PEGASUS
AIRLINES

AIR CARRIER SECURITY PROGRAM

Prepared By/Written/Created By	Checked By	Approved By
Aviation Security Specialist	Aviation Security Leader DCMM Approval Team	CEO Chief Safety and Emergency Response Management Officer

TABLE OF CONTENTS

End of Section

LIST OF EFFECTIVE PAGES

Page No	Section	Rev. Date	Rev. No
Cover Page			
1		07.01.2026	10.00
Table of Contents			
2		07.01.2026	10.00
3		07.01.2026	10.00
4		07.01.2026	10.00
5		07.01.2026	10.00
6		07.01.2026	10.00
7		07.01.2026	10.00
8		07.01.2026	10.00
9		07.01.2026	10.00
10		07.01.2026	10.00
11		07.01.2026	10.00
12		07.01.2026	10.00
13		07.01.2026	10.00
14		07.01.2026	10.00
15		07.01.2026	10.00
16		07.01.2026	10.00
List of Effective Pages			
17		07.01.2026	10.00
18		07.01.2026	10.00
19		07.01.2026	10.00
20		07.01.2026	10.00
List of Tables			
21		07.01.2026	10.00
List of Figures			
22		07.01.2026	10.00
Revision Highlights			
23		07.01.2026	10.00
24		07.01.2026	10.00
25		07.01.2026	10.00
26		07.01.2026	10.00
Chapter			
27		07.01.2026	10.00
Chapter			
28		07.01.2026	10.00
Chapter 0			
29	0.1, 0.2	07.01.2026	10.00
30	0.3	04.06.2024	09.00
31		07.01.2026	10.00
32		04.06.2024	09.00
33		07.01.2026	10.00
34		04.06.2024	09.00
35		07.01.2026	10.00
36		16.10.2022	08.00
37		16.10.2022	08.00
38		16.10.2022	08.00
39		16.10.2022	08.00
40		16.10.2022	08.00
41		07.01.2026	10.00
42		16.10.2022	08.00
43		04.06.2024	09.00
44		16.10.2022	08.00
45		07.01.2026	10.00
46		07.01.2026	10.00
47		07.01.2026	10.00
48	0.4	07.01.2026	10.00
49		04.06.2024	09.00
50		16.10.2022	08.00
51		07.01.2026	10.00
52		07.01.2026	10.00
53		07.01.2026	10.00
54		04.06.2024	09.00
55		04.06.2024	09.00
56		04.06.2024	09.00
57		04.06.2024	09.00
58	0.5	07.01.2026	10.00
59		16.10.2022	08.00
60		04.06.2024	09.00
61		04.06.2024	09.00
62		04.06.2024	09.00
63		04.06.2024	09.00
64		04.06.2024	09.00
65		04.06.2024	09.00
66		04.06.2024	09.00
67		16.10.2022	08.00
68		16.10.2022	08.00
69		16.10.2022	08.00
70		04.06.2024	09.00
71		04.06.2024	09.00
72		16.10.2022	08.00
Chapter 1			
73	1.1, 1.2	04.06.2024	09.00

Page No	Section	Rev. Date	Rev. No
74		04.06.2024	09.00
75		16.10.2022	08.00
Chapter 2			
76	2.1	04.06.2024	09.00
77	2.2	04.06.2024	09.00
78		16.10.2022	08.00
79	2.3	07.01.2026	10.00
Chapter 3			
80	3.1	04.06.2024	09.00
81	3.2, 3.3	04.06.2024	09.00
82		04.06.2024	09.00
83		04.06.2024	09.00
84		04.06.2024	09.00
85		04.06.2024	09.00
86		07.01.2026	10.00
87		07.01.2026	10.00
88		07.01.2026	10.00
89		04.06.2024	09.00
90	3.4	04.06.2024	09.00
91		07.01.2026	10.00
92		07.01.2026	10.00
93	3.5	04.06.2024	09.00
94	3.6, 3.7	04.06.2024	09.00
95		04.06.2024	09.00
96		04.06.2024	09.00
Chapter 4			
97	4.1, 4.2, 4.3	16.10.2022	08.00
98		16.10.2022	08.00
99		04.06.2024	09.00
100		16.10.2022	08.00
101	4.4, 4.5	16.10.2022	08.00
102	4.6, 4.7	16.10.2022	08.00
103		16.10.2022	08.00
104		16.10.2022	08.00
105		16.10.2022	08.00
106	4.8, 4.9	16.10.2022	08.00
107	4.10	16.10.2022	08.00
108		04.06.2024	09.00
109		04.06.2024	09.00
110		04.06.2024	09.00
111		04.06.2024	09.00
112		16.10.2022	08.00
113		16.10.2022	08.00
114	4.11	07.01.2026	10.00
115		07.01.2026	10.00
116		16.10.2022	08.00
117		16.10.2022	08.00
118		04.06.2024	09.00
119		04.06.2024	09.00
120		04.06.2024	09.00
121		07.01.2026	10.00
122		07.01.2026	10.00
123	4.12	07.01.2026	10.00
124		07.01.2026	10.00
125		16.10.2022	08.00
Chapter 5			
126	5.1, 5.2	16.10.2022	08.00
127		16.10.2022	08.00
128	5.3	16.10.2022	08.00
129		16.10.2022	08.00
130		16.10.2022	08.00
131	5.4	07.01.2026	10.00
132		16.10.2022	08.00
133		16.10.2022	08.00
134		16.10.2022	08.00
135	5.5, 5.6	16.10.2022	08.00
136	5.7, 5.8	04.06.2024	09.00
137		07.01.2026	10.00
138		07.01.2026	10.00
139		04.06.2024	09.00
140		04.06.2024	09.00
141	5.9, 5.10	16.10.2022	08.00
142		16.10.2022	08.00
Chapter 6			
143	6.1, 6.2, 6.3	04.06.2024	09.00
144	6.4	16.10.2022	08.00
145	6.5, 6.6	07.01.2026	10.00
146		16.10.2022	08.00
Chapter 7			
147	7.1	16.10.2022	08.00
148		16.10.2022	08.00
149	7.2	16.10.2022	08.00
150		16.10.2022	08.00
151		16.10.2022	08.00
152		16.10.2022	08.00
153	7.3	04.06.2024	09.00
154		16.10.2022	08.00
Chapter 8			
155	8.1, 8.2	16.10.2022	08.00
156		07.01.2026	10.00
157		16.10.2022	08.00
158	8.3	07.01.2026	10.00
159		16.10.2022	08.00

Page No	Section	Rev. Date	Rev. No
160	8.4	16.10.2022	08.00
161		16.10.2022	08.00
162	8.5	16.10.2022	08.00
Chapter 9			
163		16.10.2022	08.00
164	9.1, 9.2	16.10.2022	08.00
165		16.10.2022	08.00
166	9.3	16.10.2022	08.00
167		16.10.2022	08.00
168	9.4	07.01.2026	10.00
169		07.01.2026	10.00
Chapter 10			
170	10.1, 10.2	16.10.2022	08.00
Chapter 11			
171	11.1, 11.2	07.01.2026	10.00
172		16.10.2022	08.00
173		16.10.2022	08.00
174		16.10.2022	08.00
175		16.10.2022	08.00
176		16.10.2022	08.00
177		16.10.2022	08.00
178	11.3, 11.4, 11.5	16.10.2022	08.00
179	11.6	16.10.2022	08.00
180	11.7, 11.8	16.10.2022	08.00
181		16.10.2022	08.00
182	11.9	16.10.2022	08.00
183		16.10.2022	08.00
184	11.10	07.01.2026	10.00
185		07.01.2026	10.00
186		16.10.2022	08.00
Chapter 12			
187	12.1, 12.2	07.01.2026	10.00
188	12.3	16.10.2022	08.00
189		07.01.2026	10.00
Chapter 13			
190		07.01.2026	10.00
Chapter 14			
191	14.1	04.06.2024	09.00
192		16.10.2022	08.00
193		16.10.2022	08.00
194		16.10.2022	08.00
195		16.10.2022	08.00
196		16.10.2022	08.00
197		16.10.2022	08.00
198		16.10.2022	08.00
199		16.10.2022	08.00
200		16.10.2022	08.00
201		16.10.2022	08.00
202		16.10.2022	08.00
203		07.01.2026	10.00
204		16.10.2022	08.00
205		16.10.2022	08.00
206		16.10.2022	08.00
207		16.10.2022	08.00
208		16.10.2022	08.00
209		16.10.2022	08.00
210		16.10.2022	08.00
211	14.2	16.10.2022	08.00
212		16.10.2022	08.00
213		04.06.2024	09.00
214		04.06.2024	09.00
215		04.06.2024	09.00
216		04.06.2024	09.00
217		04.06.2024	09.00
Chapter 15			
218	15.1	07.01.2026	10.00
219		16.10.2022	08.00
220		16.10.2022	08.00
221		16.10.2022	08.00
222		16.10.2022	08.00
223		16.10.2022	08.00
224		16.10.2022	08.00
225		07.01.2026	10.00
226		04.06.2024	09.00
Chapter 16			
227		07.01.2026	10.00
228	16.1	07.01.2026	10.00
229		04.06.2024	09.00
230		04.06.2024	09.00
231		16.10.2022	08.00
232		16.10.2022	08.00
233		16.10.2022	08.00
234		04.06.2024	09.00
235		04.06.2024	09.00
236		04.06.2024	09.00
237		14.01.9999	
Chapter 17			
238	17.1, 17.2	04.06.2024	09.00
Chapter 18			
239	18.1, 18.2, 18.3	16.10.2022	08.00
240	18.4	16.10.2022	08.00
241	18.5	16.10.2022	08.00

Page No	Section	Rev. Date	Rev. No
242		16.10.2022	08.00
243	18.6	16.10.2022	08.00
244	18.7	16.10.2022	08.00
245	18.8	16.10.2022	08.00
246		16.10.2022	08.00
247	18.9	16.10.2022	08.00
248		16.10.2022	08.00

Page No	Section	Rev. Date	Rev. No
Chapter 19			
249		16.10.2022	08.00
250	19.1	16.10.2022	08.00
251		04.06.2024	09.00
252		04.06.2024	09.00

End of Section

LIST OF TABLES

End of Section

LIST OF FIGURES

End of Section

REVISION HIGHLIGHTS

Red text indicates that the text had been removed
Orange text indicates that the text had been revised
Green text indicates that the text newly had been added

Record of Revisions (RoR)

Information related to Revison 10 has been added on the table.
Information related to Revison 10 has been added on the table.

0.1 Introduction 0.1

Title revised as \"Introduction\".
Title revised as \"Introduction\".

0.1.1 Air Carrier Security Program Compliance Statement 0.1.1

Compliance Statement newly added.
Compliance Statement newly added.

0.3.3 Feedback 0.3.3

Security mail addess added.
Security mail addess added.

0.3.8.1.1 Printed Documents 0.3.8.1.1

Printed Document
Chapter newly added

0.3.15 Terms and Definitions 0.3.15

Definition of \"Security Incident\" has been added.
Definition of \"Security Incident\" has been added.
Definition of \"Security Occurrence\" has been added.
Definition of \"Security Occurrence\" has been added.
Definition of \"Security Threat\" has been added.
Definition of \"Security Threat\" has been added.

0.4.2 Aviation Security Management Review 0.4.2

Newly added.
Newly added.

0.4.2.1 Safety and Security Review Board Meetings 0.4.2.1

Title changed as \"Safety and Security Review Board\".
Title changed as \"Safety and Security Review Board\".
Added
Added
Revised according to SMS Manual.
Revised according to SMS Manual.

0.4.4 Security Culture 0.4.4

Wording change.
The word \"thanks\" changed as \"appreciation\".

2.3 The National Aviation Security Programme of the Host State 2.3

Revised to add objectives of SSPs.
Revised to add objectives of SSPs.

3.3.2.2 Duties and Responsibilities 3.3.2.2

Added in accordance with ISM Ed. 18.
Added in accordance with ISM Ed. 18.

3.3.3.1 Role Definition 3.3.3.1

SHT 17.2 reference removed.
SHT 17.2 reference removed.

3.3.3.2 Duties and Responsibilities 3.3.3.2

Security Leader Job Description has been revised in order to add reference to SSP
To ensure the preparation, implementation and maintenance of the Air Carrier Security Program (ACSP) and its associated Supplementary Station Procedures (SSPs) in accordance with International regulations and National (NCASP) and its TR-DGCA approval.
SHT 17.2 reference removed.
SHT 17.2 reference removed.

3.4.1 Sensitive Aviation Security Information 3.4.1

Reference to Corporate Manual ha sbeen added.
Reference to Corporate Manual ha sbeen added.

3.4.2 Emergency Contact Numbers 3.4.2

Revised.
Revised.

4.11 Policy for Unruly Passengers 4.11

In line with the approval received from the Directorate General of Civil Aviation (TR-DGCA), the obligation to issue a written or verbal warning for smoking incidents has been removed, as the act is considered completed at the time of detection. The Irregularity Warning Card (PG-GU-FR-008) shall therefore no longer be used for smoking or tobacco-related violations.
Revised as \"Smoking is strictly prohibited on all Pegasus Airlines flights. Passengers are informed of this regulation through pre-flight cabin announcements. Cabin crew shall immediately report any smoking incident to the Pilot-in-Command, who will decide on further operational actions, such as the offloading of the passenger and/or calling of the police if required. Such incidents shall be reported via IQSMS and by completing the Passenger Irregularity Report (PG-GU-FR-009), which shall be forwarded to the Security Department for evaluation and follow-up.\"

4.11.4.1 Passenger Restraint 4.11.4.1

location changed content
location changed content
Newly added sentence \"In case where a restraint kit is used during flight, the used kit shall be replaced at the first return of the aircraft to a designated base station. \"
Newly added sentence \"In case where a restraint kit is used during flight, the used kit shall be replaced at the first return of the aircraft to a designated base station. \"

4.11.5.1 Irregularity Warning Card 4.11.5.1

\"Smoking\" has been deleted.
\"Smoking\" has been deleted.

4.12.3 List of Prohibited Articles 4.12.3

\"Excluding\" has been changed as \"including\" for compliance with Turkish NCASP.
\"Excluding\" has been changed as \"including\" for compliance with Turkish NCASP.

5.4 Procedures for Screening and Hand-Searching of Originating Checked Baggage and Courier 5.4

Title changed as \"Procedures for Screening and Hand-Searching of Originating Checked Baggage and Courier\"
Title changed as \"Procedures for Screening and Hand-Searching of Originating Checked Baggage and Courier\"

5.8.2.1.2 In Departure from International Airports — 5.8.2.1.2

\"In some airports\" has been added, and the sentence has been moved to the 2nd paragraph for more readible procedure.
\"Weapons shall be put in a locked case in the aircraft front cargo compartment where it cannot be reached by the passenger.\" added on thi section.

6.4 Persons Other Than Passengers - List of Prohibited Articles — 6.4

\"Excluding\" has been changed as \"including\" for compliance with Turkish NCASP.
\"Excluding\" has been changed as \"including\" for compliance with Turkish NCASP.

8.2.1.1 Standard of Searches — 8.2.1.1

Airport Information Revised.
Airport Information Revised.

8.2.1.1.2.4 Areas of an Aircraft to be Examined — 8.2.1.1.2.4

new added

9.4 Checking of Catering Supplies by Cabin Crew — 9.4

The procedure has been revised for greater clarity and detail.
The procedure has been revised for greater clarity and detail.

11 Security of Cargo, Courier, Express Parcels and Mail — 11

Revised according to ISARP CGO 3.7.1.

11.10 Company Mail (Co-Mail) and Company Material (Co-Mat) — 11.10

Title changed as \"Company Mail (Co-Mail) and Company Material (Co-Mat)\"
Company Mail (Co-Mail) and Company Material (Co-Mat)

11.10.2 Company Material (Co-Mat) — 11.10.2

new revision
Reference to PG-GU-PR-055 - Company Mail (Co-Mail) and Company Material (Co-Mat) Procedure has been added.
Reference to PG-GU-PR-055 - Company Mail (Co-Mail) and Company Material (Co-Mat) Procedure has been added.

12.1.1 Application — 12.1.1

Added according to ISARP SEC 1.5.3.
Added according to ISARP SEC 1.5.3.

12.3.5 Repeating of Background Checks — 12.3.5

SHT 17.2 reference changed as Turkish NCASP
SHT 17.2 reference changed as Turkish NCASP

13 Training of Staff — 13

Reference to SHT-17.2 has been removed.
Reference to SHT-17.2 has been removed.

14.1.3.1.5 In-Flight Search — 14.1.3.1.5

deletion of references to PG-GU-FR-002 Inflight Cockpit Bomb Search Checklist and PG-GU-FR-003 Inflight Cabin Bomb Search Checklist as they are no more in use.
deletion of references to PG-GU-FR-002 Inflight Cockpit Bomb Search Checklist and PG-GU-FR-003 Inflight Cabin Bomb Search Checklist as they are no more in use.

14.1.3.1.5.1 In-Flight Cockpit Bomb Search — 14.1.3.1.5.1

In Flight Cockpit Bomb Search
Chapter newly added
PG-GU-FR-002 - Inflight Cockpit Bomb Security Search Checlist references has been changed by PG-GU-BK-002 - AIRCRAFT SECURITY SEARCH INFORMATION CARD

PG-GU-FR-002 - Inflight Cockpit Bomb Security Search Checlist references has been changed by PG-GU-BK-002 - AIRCRAFT SECURITY SEARCH INFORMATION CARD

In-Flight Cabin Bomb Search

In Flight Cabin Bomb Search
Chapter newly added

15 Incident Reporting 15

Reviewed to include incident classification.
Reviewed to include incident classification.
Reference to PG-EM-PR-009 - Occurence and Hazard Reporting Procedure has been added.
Reference to PG-EM-PR-009 - Occurence and Hazard Reporting Procedure has been added.

15.1 Description of Airline Security Incident Reporting Procedures 15.1

wording change
The verb \"must\" changed as \"shall.\"

15.1.4 Analysing of Security Reported Occurrences 15.1.4

Reference to MRM has been deleted.
Reference to MRM has been deleted.
Changed as \"Safety and Security Review Board\".
Changed as \"Safety and Security Review Board\".

16 Supervision and Performance Monitoring 16

Adding of \"its associated SSPs\" according to ISARP SEC 1.10.1.
Objectives have been reviewed.
Objectives have been reviewed.

TR-DGCA APPROVAL PAGE

Ek-1

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ
DIRECTORATE GENERAL OF CIVIL AVIATION

ONAY SERTİFİKASI
APPROVAL CERTIFICATE

HAVAYOLU GÜVENLİK PROGRAMI
AIR CARRIER SECURITY PROGRAMME

PEGASUS HAVA TAŞIMACILIK A.Ş.
PEGASUS AIRLINES INC.

Revizyon Tarihi *Issue Date*	Revizyon Numarası *Revision No*
07/01/2026	10

Türk Sivil Havacılık Genel Müdürlüğü, ICAO Annex 17, ECAC Doc. 30 ve Milli Sivil Havacılık Güvenlik Programına uygun olarak hazırlanmış olan PEGASUS HAVA TAŞIMACILIK A.Ş. Güvenlik Programını onaylar.

The Turkish Directorate General of Civil Aviation has approved the security program of PEGASUS AIRLINES INC. which has been prepared in accordance with the National Civil Aviation Security Program and ICAO Annex 17 as well as ECAC Doc. 30.

Approved By:
Ramazan DURSUN
Havacılık Güvenliği Daire Başkanı
Head of Aviation Security Department

Approval Date
22/01/2026

Figure -1: PG-GU-EK-001 AIR CARRIER SECURITY PROGRAM - TR-DGCA APPROVAL PAGE

End of Section

RECORD OF REVISIONS (ROR)

Table -1: Record of Revisions (RoR) Table

Rev. No.	Insertion Date	Notes	Prepared by
0	**13.05.2005**		**N. COŞKUN**
1	06.11.2006		TAYFUN BORA
2	20.08.2008		TAYFUN BORA
3	01.04.2010		TAYFUN BORA
4	01.04.2012		COŞKUN KAR
5	24.03.2014		SAFA ORUÇ
6	01.08.2014		SAFA ORUÇ
7	04.01.2016		SAFA ORUÇ
8	23.05.2016		SAFA ORUÇ
9	17.04.2017		SAFA ORUÇ
0	17.03.2017	Migration to QDMS Documentation System	SAFA ORUÇ
1	07.06.2018	Complete revision according to ECAC Doc. 30 Template	SAFA ORUÇ
2	28.09.2018	Wording changes	SAFA ORUÇ
3	26.12.2019	Yearly review and revision according to ISM Ed.13 and organizational changes.	MÜGE KARAPINAR
4	08.09.2020	Revision according to ISM Ed.13 and organizational changes.	MÜGE KARAPINAR
5	02.04.2021	Yearly review, revision according to NCASP Rev. 13, ISM Rev. 14, organizational and procedural changes.	MÜGE KARAPINAR
6	30.09.2021	Procedural changes.	MÜGE KARAPINAR
7	31.05.2022	Revision according to ISM Ed. 14, SeMS Ed. 5 and procedural and organizational changes.	KEMAL KUTLU
8	16.10.2022	Procedural changes.	KEMAL KUTLU
9	31.05.2022	Revision according to the migration to Comply 365 Documentation System, organizational changes, IATA ISM Ed. 16 and SeMS Manual Ed. 7. Editorial and grammar checks performed.	AYÇA CAN
10		Yearly review and procedural changes.	MUHAMMED KAYA

End of Section

0 ADMINISTRATION AND CONTROL OF THE AIR CARRIER SECURITY PROGRAMME

0.1 INTRODUCTION

Pegasus Airlines is a schedule/charter airlines company authorized by the Turkish DGCA to conduct scheduled and/or unscheduled flights to/from foreign destinations provided that all diplomatic, overflight, departure and arrival clearances have been granted in advance in accordance with AOC and Ops Specifications.

All flight operations shall be conducted in accordance with the regulations of the Turkish Government and/or any applicable Foreign Government. In the event of any conflict in regulations between Türkiye and any applicable Foreign Government, the most conservative regulation shall apply outside of the territory and airspace of Türkiye.

0.1.1 Air Carrier Security Program Compliance Statement

Pegasus Airlines hereby confirms that the ACSP has been established in compliance with ICAO Annex 17, ICAO Document 8973, ECAC Document 30, TR-DGCA NCASP and directives, IOSA standards and all other relevant national and international regulations and laws with the terms, conditions, and limitations of the Air Operator Certificate.

All the material documented herein have compulsory standards and comprise all nontype related (or common to all types) operational policies, instructions and procedures for safe and secure operations.

This implies that all affected personnel shall be familiar, stay up-to-date and have easy access to the ACSP content to execute their duties.

In the case of any individual considering that all or any part of a procedure or instruction requires amendment, refer to "0.3.3 Feedback".

0.2 PURPOSE, SCOPE

The purpose of the Air Carrier Security Programme is:

- to increase Aviation Security by controlling those elements involved including baggage, passengers, cargo, protect customers, personnel and assets from any unlawful act,
- to provide directions on security measures required in compliance with regulatory requirements.

All personnel involved in servicing the aircraft and having access to the aircraft while it is on the ground are also covered by this Programme.

In addition to the specified responsibilities of other personnel holding operational security functions within Pegasus Airlines, OM-Part A, CCM, Ground Operations Manual and Cargo Manual specify security related duties and responsibilities in detail.

WARNING	The information contained in Pegasus Airlines Air Carrier Security Programme (from now ACSP) is confidential, privileged and only for the information of the intended recipient and may not be used, published or redistributed without the prior written consent of Pegasus Airlines Aviation Security Department.

Scope: ICAO Annex 17 Standard 3.3.1

“Each Contracting State shall ensure that commercial air transport operators providing service from that State have established, implemented and maintained a written operator security programme that meets the requirements of the national civil aviation security programme of that State.”

Pegasus Airlines ACSP is issued and controlled by Pegasus Airlines Aviation Security Department, the ACSP and any revision prepared are internally approved by the Accountable Manager (CEO) and finally approved by TR-DGCA.

The following documents have influence on or are affected by the contents of the Pegasus Airlines of Air Carrier Security Programme:

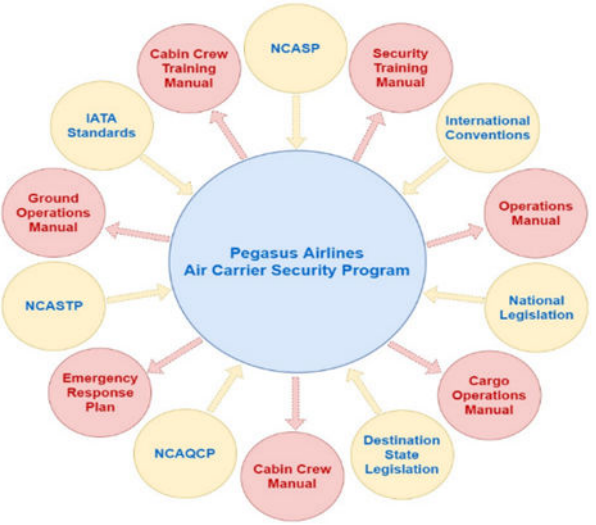


Figure 0-1: ACSP Chart

0.3 STRUCTURE AND CONTENT OF THE AIR CARRIER SECURITY PROGRAM

The ACSP is managed, revised and matched and/or is being compared with the company operation manuals in the company Comply365 Documentation System.

For further information, please refer to *PG-DU-EK-001 - Documentation System Manual*, available in Comply365.

0.3.1 Format

The Compliance Monitoring Manual is produced and distributed via Comply365 in electronic format. The content and appearance of each version is identical.

The header of each page of the Compliance Monitoring Manual contains the following information:

- Pegasus Airlines Logo
- Department Name
- Document Name
- The page number
- The document number
- The revision version of each page
- The revision date of the page

The boxes in the approval section in the approval page contain only the relevant person's duty titles, not the names.

For further information, please refer to *PG-DU-EK-001 - Documentation System Manual.*

0.3.2 Issue and Copy Identification

The master copy of the ACSP is retained in Comply365. Electronic copies of the ACSP are distributed via Comply365 and Ground Document Library.

0.3.3 Feedback

All authorized users of the ACSP is requested to provide feedback on information provided in the Manual that may be incorrect or inaccurate. Any suggestion for improvement of the ACSP or advice as regards obsolescence is appreciated.

Errors and/or discrepancies within the ACSP, or between other manuals and/or regulations shall be reported to the Aviation Security Department (security@flypgs.com) immediately.

Recommendations for changes to the ACSP can also be made by the “Suggest Revision process on Comply365”.

0.3.4 System of Amendments and Revision

Pegasus Airlines ACSP, its distribution, amendments and revisions are published and issued by the Aviation Security Department digitally.

The Aviation Security Leader (RP) is responsible for ensuring that external service providers receive information regarding security directives and instructions within 3 days and in a manner that meets the requirements of Pegasus Airlines ACSP.

CAUTION	Pegasus Airlines ACSP is a restricted document and shall be protected from unauthorized access. The document shall be available in part or in whole only to those with a bona fide need to know its contents. All entities and individuals provided with copies or portions of an ACSP shall be charged with protecting the information in their possession.
COPYRIGHT	The contents of this document are the property of Pegasus Hava Taşımacılığı A.Ş. and shall not be copied, reproduced or disclosed to a third party without the written consent of the proprietor.

Pegasus Airlines ACSP will be reviewed, yearly updated and revised to ensure validity of its contents and documentation. Pegasus Airlines ACSP amendments and revisions are made as necessary by the Aviation Security Leader (RP). Any immediate changes on regulations and practices are published as a Bulletin or Read and Sign during that period.

The Aviation Security Leader (RP) is responsible for its contents and for keeping the instructions and information up to date. S/he shall supply the TR-DGCA with the intended amendments and revisions in advance of the effective date.

0.3.5 Security Records

All Pegasus Airlines personnel shall prepare/ use/ classify the documents in accordance with *PG-BG-TL-001 - Data Management Instruction*, available in Comply365.

Sensitive or restricted documents, while not classified, could be detrimental to aviation security if released publicly.

When not in the physical possession of an authorized person, paper or physical records of restricted documents and/or security sensitive information are specially defined and stored in a locked file cabinet or drawer.

They also ensure that the retrieval of archived documents, applicable hardware and/or software is retained after it has been replaced. This type of document is reviewed once a year to identify records that are no longer valid and to ensure such records are destroyed in a manner that precludes recognition or reconstruction of the information.

For further information, refer to *PG-DU-EK-001 - Documentation System Manual*, available in Comply365.

0.3.6 Manual Holders’ Responsibility

Any holder receiving an amendment in soft copy format shall study the revised texts upon receipt not later than the effective date. The soft copies of the previous revisions shall be deleted when a new revision is published. Previous amendment letters and obsolete pages shall be destroyed from the hard copies, if any.

0.3.7 Form of Revisions

All revisions to this manual shall undergo a compliance check prior to publication. Where a revision or amendment requires TR-DGCA approval, such shall be obtained prior to publication of the amendment or revision.

All revisions will be published in the form of Comply365 system. Handwritten amendments and revisions are not permitted. When an amendment concerns any provision or procedure that must be approved by the TR-DGCA, such approval shall be obtained before the amendment becomes effective.

Only when immediate amendments or revisions are required in the interest of security or safety may they be published and applied immediately, provided that the changes have been submitted to the TR-DGCA.

New or revised information is updated in the Comply365 System.

The revision will be issued with effective pages in order that the user can follow the revisions and updated pages.

0.3.7.1 Annotation of Changes

In order to identify changes, additions or deletions of new text/illustration, a bold sideline will be used to identify the changed text/illustration in PDF version.

There is no List of Effective Pages (LEP) in HTML version of the documents. Instead, the "Revision Highlights" section is used to track changes for the revisions.

Changes in HTML version documents are listed and briefly described in this section.

There is no bold sideline for the sections which are automatically updated by the Comply365 on the front matter of the book.

"Revision Highlights section will be used to identify the revised sections and briefly describe the reason for the revision. All manual holders are responsible for carefully taking note of the changes.

The revision number for documents is automatically issued by Comply365.

For further information, please refer to *PG-DU-EK-001 - Documentation System Manual*, available in Comply365.

0.3.8 Retention and Dissemination of Internal & External Sources

All Pegasus Airlines operations personnel can access the ACSP by using their personal usernames and passwords on Comply365 and/or Pegasus EFB Application.

Controlled Manual: A controlled manual allows the verification of the completeness and revision status of each page, at any time of use.

Individual Printouts: Individually produced printouts of the ACSP are only for information and are accepted as uncontrolled documents. These printouts must be cross-checked with the Pegasus Comply365/EFB Application version for validity.

Pegasus Airlines ACSP, its applicable parts and the amendments shall be distributed as expeditiously as possible. Revised pages/chapters shall be distributed to the relevant departments in accordance with the distribution list within 15 days of TR-DGCA approval date via Comply365.

The revision become effective when the amendment is received by the holder published on the Comply365 irrespective of the proposed date of issue shown. Aviation Security Department personnel, other Pegasus Airlines relevant personnel and handling companies will receive notification for the published amendment via e-mail and shall download the same from Pegasus Airlines official website (intranet).

Table 0-1: Retention and Dissemination of the ACSP

Personnel	Website	Access
Pegasus Airlines	"https://pegasus.comply365.net/"	Easy access by using their username and password.
Ground Handling Service Providers Catering Suppliers Security Service Suppliers	"https://document.flypgs.com"	For more details, please refer to PG-DO-EK-001 - Ground Operations Manual, available in Comply365.

To download Pegasus Airlines ACSP's current edition is the responsibility of individual contracted Handling Contractors Companies and shall be monitored by the Aviation Security Department.

Aviation Security Department will make sure that all downloaded information is properly entered by keeping a record of the confirmation reply from the handling agents or concerned parties. For all downloading confirmations, please send an e-mail to our Aviation Security Department e-mail address "security@flypgs.com".

0.3.8.1 Internal Document/Data Control

Internally generated documents and data in Pegasus Airlines such as policy statements, procedures, charts, checklists, manuals, memorandums, software and plans may be on various media whether in hard copy or electronic format, digital, analogue, photographic or written. Internal operational documents are subject to management and control.

For further information, please refer to *PG-DU-EK-001 - Documentation System Manual*, available in Comply365.

0.3.8.1.1 Printed Documents

Security documents such as forms and information cards (etc.), managed as printed copies, are produced by contracted companies for large-scale printing.

Once the document approval process is completed in Comply365, the Security Department issues a purchase request within 7 days, and the controlled copy of the document is sent to the contracted printing house via e-mail.

Business printers may be used for small-scale printing needs.

Before initiating the printing process, the printing house sends a sample to the Security Department for review. After receiving approval, the printing house proceeds with printing the documents/forms.

The sample must be checked and approved by the Security Department before the full printing process can begin.

After the printing process is completed, the printed documents shall be distributed to the relevant departments by the Security Department within 45 days.

For further information, please refer to the PG-DU-EK-001 - Documentation System Manual, available in Comply365.

0.3.8.2 External Document/Data Control

Internally generated documents and data in Pegasus Airlines such as policy statements, procedures, charts, checklists, manuals, memorandums, software and plans may be on various media whether in hard copy or electronic format, digital, analogue, photographic or written. Internal operational documents are subject to management and control.

For further information, please refer to *PG-DU-EK-001 - Documentation System Manual*, available in Comply365.

0.3.8.3 Paper Documentation

The Air Carrier Security program managed by the Aviation Security Department is created using a standard template which complies with Comply365 in a structured authoring application. All human factors guidance for documentation points towards "predictability". The manual has the same design for front matter (TOC, LEP, Revision Highlights etc.) which allows the end user to predict how a manual is navigated and the process of finding and assimilating information becomes intuitive.

Pegasus Airlines supports reducing dependence on paper-based documentation and as such the font / size / colour of text in a manual are all designed to enhance the online experience of using these manuals while still being capable of producing a fully usable printed paper version.

Individually produced printouts from any electronic version of the ACSP are accepted as uncontrolled documents. Such printouts must be cross-checked with the Comply365 version for validity.

0.3.9 Disposal of Obsolete Documentation

When an amendment or revision is issued to the ACSP, the revision number changes. If the revision number of the ACSP is different than the soft copies on Comply365, Pegasus EFB Application or Ground Documentation Library, then the document is deemed as obsolete.

In order to prevent the unintended use of obsolete documents, and to apply suitable identification of out-ofdate documents or older versions of revised documents, the disposal of obsolete documents becomes valid when the amendment is received by the holder of the manual. The copies of obsolete documents shall be deleted by the users immediately after replacement.

For further information about the Disposal of Obsolete Documentation, refer to *PG-DU-EK-001 Documentation System Manual* and *PG-KU-EK-001 - Compliance Monitoring Manual* Chapter 4 - Documentations, Records, Back Up Management and Communication, available in Comply365.

0.3.10 Deletion and Control of Records

Please refer to *PG-DU-EK-001 - Documentation System Manual* and *PG-KU-EK-001 - Compliance Monitoring Manual* Chapter 4 - Documentations, Records, Back Up Management and Communication, available in Comply365.

0.3.11 Backup

Backup of documents and data are performed on a regular basis. For further information, refer to *PG-DU-EK-001 - Documentation System Manual,* available in Comply365.

0.3.12 Company Property

0.3.13 Currency / Conflicting Information

Manuals within the Pegasus Airlines documentation system may not be revised concurrently, to avoid creating the possibility of conflicting information in different manuals.

The Aviation Security Department ensures the review and revision as necessary to maintain the currency of information contained in documents. In case of conflicting information in different Pegasus Airlines operational manuals, the information contained in the higher document in the hierarchical order can be assumed to be valid.

When the documentation listed above is contradictory to rules and regulations established and mandated by State Authorities, the more restrictive shall be applicable and international/national laws remain valid until revisions can be implemented in the appropriate documentation.

0.3.14 Distribution List

The ACSP shall be distributed to all personnel via Comply365 System as listed in this chapter. When a new document is created, and/or revised, the system sends a read duty e-mail to users.

The Aviation Security Leader (RP) is responsible to ensure that such information is received by third-party services. The distribution must be performed by the Aviation Security Department in accordance with the Distribution List below.

Table 0-2: ACSP Distribution List

ACSP Manual Recipients		Version
PG-GU-EK-001	Chief Safety and Security Office	Approved Master Copy Displayed via Comply365 Document Management System
Electronic Copies	Turkish DGCA	Comply365 Document Management System

Electronic Copies	Host State DGCA	Comply365 Document Management System or Controlled Comply365 PDF Soft Copy by e-mail
	Aviation Security File Master	TR-DGCA Approved Soft Copy Downloaded from Comply365
	Accountable Manager	Comply365 Document Management System
	All Pegasus Airlines Personnel	
	Delegated Auditors	
	Subsidiary Company (if required)	
	All Pilots	Comply365 Document Management System & EFB System
	Contracted Handling	Controlled Comply365 PDF Soft Copy by Ground Doc.Lib
	Security Service Providers	
	Catering Suppliers	
	Company Legal Consultant (if required)	Controlled Comply365 PDF Soft Copy by e-mail

0.3.15 Terms and Definitions

Table 0-3: Terms and Definitions

Accompanied hold baggage	Baggage which is accepted for carriage in the hold of an aircraft and which is checked in by the passenger who is on board.
Accountable Manager	The manager who has corporate authority for ensuring operations and maintenance activities are provided with the necessary resources and conducted in accordance with the standards of the Operator and the requirements of the State.
Acts of unlawful interference	(Definition given for guidance purposes). These are acts or attempted acts such as to jeopardize the safety of civil aviation, including but not limited to: • unlawful seizure of aircraft; • destruction of an aircraft in service; • hostage-taking on board the aircraft or on aerodromes; • forcible intrusion on board an aircraft, at an airport or on the premises of an aeronautical facility; • introduction on board an aircraft or at an airport of a weapon or hazardous device or material intended for criminal purposes; • use of an aircraft in service for the purpose of causing death, serious bodily injury, or serious damage to property or the environment; and • communication of false information such as to jeopardize the safety of an aircraft in flight or on the ground, of passengers, crew, ground personnel or the general public, at an airport or on the premises of a civil aviation facility.

Aerial work	An aircraft operation in which an aircraft is used for specialized services such as agriculture, construction, photography, surveying, observation and patrol, search and rescue, and aerial advertisement.
Aircraft	Any machine that can derive support in the atmosphere from the reactions of the air other than the reactions of the air against the earth's surface.
Aircraft in flight	An aircraft from the moment when all its external doors are closed following embarkation until the moment when such doors are opened for disembarkation
Aircraft in service	A parked aircraft which is under surveillance sufficient to detect unauthorized access.
Aircraft maintenance area	All the ground space and facilities provided for aircraft maintenance. This includes aprons, hangars, buildings and workshops, vehicle parks and roads associated therewith. Such an area is normally designated as a security restricted area.
Aircraft material	A material (including a fluid) for use in the manufacture, maintenance, servicing or operation of an aircraft or of an aircraft component but does not include an aircraft component.
Aircraft not in service	An aircraft that is either parked for a period of more than 12 hours or is not under surveillance sufficient to detect unauthorized access.
Aircraft operators' documents	Air waybills and consignment notes, passenger tickets and boarding passes, bank and agent settlement plan documents, excess baggage tickets, miscellaneous charges orders, damage and irregularity reports, baggage and cargo labels, timetables, and weight and balance documents, for use by aircraft operators.
Aircraft security check	An inspection of the interior of an aircraft to which passengers may have had access and an inspection of the hold for the purpose of discovering suspicious objects, weapons or other dangerous devices, articles and substances.
Aircraft security search	A thorough inspection of the interior and the exterior of the aircraft for the purpose of discovering suspicious objects, weapons or other dangerous devices, articles and substances.
Aircraft stand.	A designated area on an apron intended to be used for parking an aircraft.
Airport	Any area in an ICAO Member State which is open for commercial aircraft operations
Airport Operations Area (AOA)	All restricted ground areas of an airport, including taxiways, runways, loading ramps and parking areas
Airside	The movement area of an airport, adjacent terrain and buildings, or portions thereof, access to which is controlled.
Appropriate authority for aviation security	The authority designated by a State within its administration to be responsible for the development, implementation and maintenance of the national civil aviation security programme.
Apron	A defined area, on a land aerodrome, intended to accommodate aircraft for the purposes of loading or unloading passengers, mail or cargo, fuelling, parking or maintenance.

Apron passenger vehicle	Any vehicle used to convey passengers between aircraft and passenger buildings.
Authority	The term ‘‘Authority’’ as used in this manual means Turkish National Aviation Authority (TR-DGCA)
Background check	A check of a person’s identity and previous experience, including where legally permissible, any criminal history, as part of the assessment of an individual’s suitability to implement a security control and/or for unescorted access to a security restricted area
Baggage	Personal property of passengers or crew carried in the cabin or in the hold of an aircraft by agreement with the operator
Baggage container	A receptacle in which baggage is loaded for conveyance in an aircraft.
Baggage sorting area	Space in which departure baggage is sorted into flight loads.
Baggage storage area	Space in which checked/hold baggage is stored pending transport to the aircraft and space in which mishandled baggage may be held until forwarded, claimed or otherwise disposed of.
Behaviour detection	Within an aviation security environment, the application of techniques involving the recognition of behavioural characteristics, including but not limited to physiological or gestural signs indicative of anomalous behaviour, to identify persons who may pose a threat to civil aviation.
Bomb alert	A status of alert put in place by competent authorities to activate an intervention plan intended to counter the possible consequences arising from a communicated threat, anonymous or otherwise, or arising from the discovery of a suspect device or other suspect item on an aircraft, at an airport or in any civil aviation facilities.
Bomb threat	A communicated threat, anonymous or otherwise, which suggests, or infers, whether true or false, that the safety of an aircraft in flight or on the ground, or any airport or civil aviation facility or any person may be in danger from an explosive or other item or device.
Cabin baggage	Baggage that is retained in the custody of passenger to bring on an aircraft. Equivalent Terms: Hand Baggage, Unchecked Baggage, Carry-on Baggage.
Cabin crew member	A crew member who performs, in the interest of the safety of passengers, duties assigned by the Operator or the Pilot in- Command of the aircraft, but who shall not act as a flight crew member. Equivalent Terms: Flight Attendant, Cabin Attendant.
Cargo	Any property carried on an aircraft other than mail, stores and accompanied or mishandled baggage.
Cargo area	All the ground space and facilities provided for cargo handlings. It includes aprons, cargo buildings and warehouses, vehicle parks and roads associated therewith.
Cargo building	A building through which cargo passes between air and ground transport and in which processing facilities are located, or in which cargo is stored pending transfer to air or ground transport.

Cargo compartment	An area of an aircraft designed and configured primarily for the transport of cargo, which has the systems and equipment necessary for the handling and restraint of cargo. There are different classifications of cargo compartments and, depending on the aircraft type and/or configuration; some cargo compartments are accessible by the flight crew in flight, while others are not. Compartments used to carry cargo, baggage and/or other items, which are located below the passenger's cabin or main deck of an aircraft, maybe referred to as the hold.
Catering stores	All items, other than catering supplies, associated with passenger in-flight services, for example newspapers, magazines, headphones, audio and video tapes, pillows and blankets, and amenity kits.
Catering supplies	Food, beverages, other dry stores and associated equipment used on board an aircraft.
Certification	A formal evaluation and confirmation by or on behalf of the appropriate authority for aviation security that a person possesses the necessary competencies to perform assigned functions to an acceptable level as defined by the appropriate authority.
Checked baggage	Passenger baggage that has been taken into custody by the Operator, and for which a baggage claim check has been issued to the passenger. Equivalent Terms: Registered Baggage, Registered Luggage.
Check-in	The process of reporting to an aircraft operator for acceptance on a particular flight.
Check-in position	The location of facilities at which check-in is carried out.
Co-Mail	Abbreviation of air carrier company mail shipped within its network of stations.
Co-Mat	Abbreviation of air carrier company materials shipped within its network of stations.
Commercial air transport operation	An aircraft operation involving the transport of passengers, cargo or mail for remuneration or hire. (For the purposes of this manual, the term aircraft operator will be used instead of commercial air transport operator.)
Commercial air transport	The carriage of passengers, cargo or mail for remuneration or hire.
Commercial flight	A scheduled or non-scheduled flight or flight activity rendered for hire to the general public or private groups for valuable consideration.
Consignment	One or more packages of cargo accepted by an Operator from one shipper at one time and at one address, received in one lot and moving to one consignee at one destination address. Equivalent Terms: Shipment.
Contingency	An event that may but is not certain to occur in the future. Equivalent Terms: Eventuality.
Contingency plan	A proactive plan to include measures and procedures addressing various threat levels, risk assessments and the associated security measures to be implemented, designed to anticipate and mitigate events as well as prepare all concerned parties having roles and responsibilities in the event of an actual act of unlawful interference. A contingency plan sets forth incremental security measures that may be elevated as the threat increases. It may be a stand-alone plan or included as part of a Crisis Management Plan.

Continuous random checks	Checks conducted during the entire period of activity, with those checks conducted on a random basis.
Contracting State	A state that is party to the Convention on International Civil Aviation (Chicago Convention). Equivalent Terms: Member State.
Corporate aviation	The non-commercial operation or use of aircraft by a company for the carriage of passengers or goods as an aid to the conduct of company business, flown by a professional pilot employed to fly the aircraft. (Note that corporate aviation is a subset of general aviation.)
Courier baggage	Shipments tendered by one or more shippers that are transported as the baggage of a courier passenger on board the aircraft under normal passenger hold baggage documentation.
Courier service	An operation whereby shipments tendered by one or more consignors are transported as the baggage of a courier passenger on board a scheduled aircraft operator service under normal passenger hold baggage documentation.
Crew member	A person assigned by an operator to duty on an aircraft during a flight duty period.
Crisis	An unstable or crucial situation that has reached a critical phase and presents the distinct possibility of an undesirable outcome.
Crisis management	Contingency measures implemented in response to increased threat levels as well as implementation of measures and procedures in response to the emergencies to include acts of unlawful interference.
Critical parts of security restricted areas	At least those parts of an airport, where more than 60 persons hold airport identification cards giving access to security restricted areas, to which screened departing passengers have access and those parts through which screened departing hold baggage may pass or in which it may be held, unless it concerns secured baggage.
Dangerous goods	Articles or substances which are capable of posing a risk to health, safety, property or the environment and which are shown in the list of dangerous goods in the Technical Instructions or which are classified according to those Instructions.
Deportee	A person who had legally been admitted to a State by its authorities or who had entered a State illegally, and who at some later time is formally ordered by the competent authorities to leave that State.
Designated land areas	Land areas that have been designated by the State concerned as areas in which search and rescue would be especially difficult.
Designated representative	A person specifically approved by an authority to act on its behalf for specific approval purposes.
Diplomatic pouch/bag	A shipping container having diplomatic immunity from search or seizure when accompanied by the required official documentation.
Direct transit area	A special area established in an international airport, approved by the public authorities concerned and under their direct supervision or control, where passengers can stay during transit or transfer without applying for entry to the State.

Disruptive passenger	A passenger who fails to respect the rules of conduct at an airport or on board an aircraft or to follow the instructions of the airport staff or crew members and thereby disturbs the good order and discipline at an airport or on board the aircraft.
Emergency plan	A plan setting forth the procedures for coordinating the response of different aerodrome agencies or services and of those agencies in the surrounding community that could be of assistance in responding to an emergency.
Equivalent terms	For example: Examination, Testing, Checking, Assessment
Evaluation	The process of determining whether an item, individual or activity meets specified criteria; when used in conjunction with training, refers to the process by which an evaluator or instructor determines how well a student's performance fulfils the course competencies; processes may include a demonstration of knowledge, proficiency and/or competency as appropriate.
Evaluation Programme	A continuous programme that the distributor applies to evaluate its own compliance with its quality system. Equivalent Terms: Self-Audit, Self-Evaluation, Audit Programme, Audit Schedule, and Audit Plan.
Evaluator	A person, who assesses, examines or judges the performance of crewmembers, instructors, other evaluators, or other operations personnel. Equivalent: Examiner.
Explosive detection system	A technology system or combination of different technologies which has the ability to detect, and so to indicate by means of an alarm, explosive material contained in baggage or other articles, irrespective of the material from which the bag is made.
Explosive device detection system	A technology system or combination of different technologies which has the ability to detect, and so to indicate by means of an alarm, an explosive device by detecting one or more components of such a device contained in baggage or other articles, irrespective of the material from which the bag or article is made.
Explosive substance	A solid or liquid substance (or a mixture of substances) which is in itself capable, by chemical reaction, of producing gas at such a temperature and pressure and at such a speed as to cause damage to the surroundings. Included are pyrotechnic substances even when they do not evolve gases. A substance which is not itself an explosive, but which can form an explosive atmosphere of gas, vapor or dust is not included.
Facilitation	The efficient management of the necessary control process, with the objective of expediting the clearance of persons or goods and preventing unnecessary operational delays.
Flight Crew	The flight crew members essential to the operation of an aircraft, the number and composition of which shall not be less than that specified in the operations manual and shall including flight crew members in addition to the minimum numbers specified in the flight manual or other documents associated with the certificate of airworthiness, when necessitated by considerations related to the type of aircraft used, the type of operation involved and duration of flight between points where flight crews are changed.
Freight	See Cargo

General aviation	An aircraft operation other than a commercial air transport operation or an aerial work operation.
Ground Handling	Services necessary for an aircraft's arrival at, departure from, an airport, other than air traffic services.
High-risk cargo or mail	Cargo or mail presented by an unknown entity or showing signs of tampering shall be considered high risk if, in addition, it meets one of the following criteria: a. Specific intelligence indicates that the cargo or mail poses a threat to civil aviation; or b. The cargo or mail shows anomalies that give rise to suspicion; or c. The nature of the cargo or mail is such that baseline security measures alone are unlikely to detect prohibited items that could endanger the aircraft. Regardless of whether the cargo or mail comes from a known or unknown entity, a State's specific intelligence about a consignment may render it as high risk.
Hold baggage	Any baggage that is carried in the hold of passenger aircraft.
Human Factors Principles	Principles which apply to design, certification, training, operations and maintenance and which seek safe interface between the human and other system components by proper consideration to human performance.
Human performance	Human capabilities and limitations which have an impact on the safety, security and efficiency of aeronautical operations.
ICAO Annexes	Additional sections to the ICAO Convention, which are guidelines, provided for the various national aviation authorities for use in developing the civil aviation rules and regulations that govern flight operations in their respective states. Equivalent Terms: Annexes
IDX	IATA Incident Data Exchange
Inadmissible person	A person who is or will be refused admission to a State by its authorities. Note — Such a person normally has to be transported back to their State of departure, or to any other State where the persons are admissible, by the aircraft operator on which they arrived.
In-flight security officer	A person who is authorized by the government of the State of the Operator and the government of the State of Registration to be deployed on an aircraft with the purpose of protecting that aircraft and its occupants against acts of unlawful interference. This excludes persons employed to provide exclusive personal protection for one or more specific people travelling on the aircraft, such as personal bodyguards.
In-flight supplies	All items intended to be taken on board an aircraft for use, consumption or purchase by passengers or crew during the flight, which typically include catering and cleaning stores and supplies.
Integrated/ consolidated cargo	A consignment of multiple packages which has been originated by more than one person, each of whom has made an agreement for carriage by air with another person other than a scheduled aircraft operator.
Interline baggage	The baggage of passengers subjected to transfer from the aircraft of one operator to the aircraft of another operator in the course of their journey.

International airport	Any airport designated by the Member State in whose territory it is situated as an airport of entry and departure for international air traffic, where the formalities related to customs, immigration, public health, animal and plant quarantine and similar procedures are carried out.
International Operations	Flights conducted from an airport in the territory of one state to an airport in the territory of another state. Equivalent Terms: International Flights.
Known Cargo	A consignment of cargo accepted by a regulated agent or operator directly from a regulated agent, operator or known shipper/consignor, to which appropriate security controls have already been applied, and which is thereafter protected from unlawful interference. Alternatively it refers to a consignment of unknown cargo that has been subjected to appropriate security controls, made ‘‘known’’ and which is thereafter protected from unlawful interference.
Known consignor	A consignor who originates cargo or mail for its own account and whose procedures meet common security rules and standards sufficient to allow the carriage of cargo or mail on any aircraft.
Known Shipper	An originator of shipments for transportation by air who has established business with a regulated agent or an Operator on the basis of having demonstrated satisfaction of specific requirements for safe transportation of cargo. Equivalent Terms: Known Consignor.
Landside	Those parts of an airport, adjacent terrain and buildings or portions thereof that are not airside, as identified by States and relevant entities in their security programmes.
Mail	All postal items tendered by and intended for delivery to designated postal operators to operate the postal service in accordance with the Universal Postal Union Acts.
Management System	The collective body of managers and other associated managerial elements that provide for direction, oversight and control of an organization
Mishandled baggage	Baggage involuntarily, or inadvertently, separated from passengers or crew.
Movement area	That part of an aerodrome to be used for the take-off, landing and taxiing of aircraft, consisting of the manoeuvring area and the apron(s).
Narcotics Control	Measures to control the illicit movement of narcotics and psychotropic substances by air.
National Civil Aviation Security Programme	The documented programme of a State for safeguarding civil aviation operations against acts of unlawful interference through regulations, practices and procedures that take into account the safety, regularity and efficiency of flights.
Non-restricted area	Area of an airport to which the public has access or to which access is otherwise unrestricted.
NOTOC (Notification to Pilot-in-Command)	Accurate and legible written or printed information provided to the Pilot in-Command concerning dangerous goods shipments or other special cargo that is to be carried on board the aircraft. Equivalent Terms: NOTAC (Notification to Aircraft Pilot-in-Command), NOPIC (Notification to Pilot in Command).
Off-airport processing facilities	A passenger or cargo transport link terminal at an urban population centre at which processing facilities are provided.

Onboard Library	The collection of documents required to be available on board an aircraft and accessible for use by the flight crew during flight preparation and in flight.

One-Stop Security	A concept whereby a passenger and accompanied baggage are subjected to only one security check during departure, even if the journey involves multiple transfers. The concept requires mutual acceptance of key security procedures used to verify that passengers, baggage, cargo consignments, the aircraft and any other item loaded on an aircraft for transport are free of dangerous items, thus not requiring duplication of such security procedures at transfer, transit and destination points. One-stop security is normally achieved through harmonized or mutually accepted: Technical requirements for equipment used in key security measures:
	• Vetting and training requirements for security personnel engaged in the implementation of key security measures;
	• Methods of implementation of key security measures;
	• Procedures for assessing compliance.
	• Operational Security Personnel: Employees of an operator or other personnel under the control of an operator trained and/or certified by the appropriate authority for security and authorized to perform the application of security controls on goods and persons, the application of preventive security measures and the management of a response to acts of unlawful interference, to include:
	  • Personnel who implement security controls;
	  • Crew members and front line ground handling personnel;
	  • Other applicable operational personnel.

Integrated Operations Control Centre (IOCC)	An office or department within the organizational structure of an operator that is assigned responsibility for operational control of ongoing operations with authority to originate, delay, divert and cancel flights. Functions located within an IOCC typically include management representatives, flight dispatch, flight planning, crew scheduling, maintenance experts, meteorology personnel, ATS specialists, and customer service specialists. An IOCC is equipped with communications equipment, technology tools and support materials necessary to accomplish required functions; serves as a ‘‘nerve centre’’ for an operator, with multiple communications links (e.g. to en-route flights, system stations, government agencies, as well as load control, security, technical and medical functions). The size and location of an IOCC is commensurate with the type and magnitude of operations; may consist of few or many personnel and may have one or more locations; all functions located in one central location is desirable for better communication and coordination. Equivalent Terms: System Operations Centre (SOC)
Operations Manual (OM)	The general section of the Operations Manual (OM) that contains flight crew policies and procedures that are not related to a specific type of aircraft.
Passenger area	All the ground space and facilities provided for passenger processing, including aprons, passenger buildings, vehicle parks and roads.

Permit system	A system consisting of cards or other documentation issued to individual persons employed at airports or who otherwise have a need for authorized access to an airport, airside or security restricted area. Its purpose is to identify the individuals and facilitate access. Vehicle permits are issued and used for similar purposes to allow vehicular access. Permits are sometimes referred to as airport identification cards or passes.
Person with disabilities	Any person whose mobility is reduced due to a physical incapacity (sensory or locomotive), an intellectual deficiency, age, illness or any other cause or disability when using air transport and whose situation needs special attention and the adaptation to the person's needs of the services made available to all passengers.
Pilot in Command	The pilot designated by the operator, or in the case of general aviation, the owner, as being in command and charged with the safe conduct of a flight.
Prohibited article	An object which can be used to commit an act of unlawful interference and that has not been properly declared and subjected to the applicable laws and regulations.
Regulated agent	An agent, freight forwarder or any other entity who conducts business with an operator and provides security controls that are accepted or required by the appropriate authority in respect of cargo or mail.
Responsiblity	The obligation or willingness to accept responsibility for the execution or performance of an assigned function, duty, task or action; implies being answerable (i.e. responsible) to a higher authority for ensuring such responsibility is executed or performed.
Restricted articles	Articles which are, in the specific context of aviation security, defined as those articles, devices or substances which may be used to commit an act of unlawful interference against civil aviation or which may endanger the safety of the aircraft and its occupants, or installations, or the public.
Sabotage	An act or omission, intended to cause malicious or wanton destruction of property, endangering or resulting in unlawful interference with civil aviation and its facilities.
Screening	The application of technical or other means which are intended to identify and/or detect weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference.
Security	Safeguarding civil aviation against acts of unlawful interference. This objective is achieved by a combination of measures and human and material resources.
Security audit	An in-depth compliance examination of all aspects of the implementation of the national civil aviation security programme.
Security checks for LAGs and STEBs	Visual checks or security controls, performed by security staff, for signs of interference; in particular tampering with seals, theft and the introduction of potentially dangerous devices, articles or substances. The checks shall be made at the first point of entry on the airside and shall be made on all supplies of LAGs and STEBs to establish that they have been protected, that there is no evidence or suspicion of tampering, and that the necessary documentation is in order.

Security control	A means by which the introduction of weapons, explosives or other dangerous devices, articles or substances which may be used to commit an act of unlawful interference can be prevented.
Security equipment	Devices of a specialized nature for use, individually or as part of a system, in the prevention or detection of acts of unlawful interference with civil aviation and its facilities.
Security exercise	A full-scale security exercise is a simulated act of unlawful interference with the objective of ensuring the adequacy of a contingency plan to cope with different types of emergencies. A partial security exercise is a simulated act of unlawful interference with the objective of ensuring the adequacy of the response to individual participating agencies and components of the contingency plan, such as the communications system.
Security incident	A designation given to a security occurrence which affects or could affect the safety of passengers, crew, ground personnel and the general public. Security incidents are designated by a security official or manager to a reported security occurrence based on an analysis of the occurrence and a determination that additionnal action is required. A security incident may also result in an act of unlawful interference that would require additional reporting by the States to ICAO.
Security inspection	An examination of the implementation of relevant National Civil Aviation Security Programme requirements by an aircraft operator, airport or other entity involved in security.
Security investigation	An inquiry into any act or attempted act of unlawful interference against civil aviation and/or any alleged or suspected instance of non-compliance with a State's National Civil Aviation Security Programme or other legal and/or regulatory requirements pertaining to civil aviation security.
Security occurrence	Any security-related event that may result in a reduced security outcome, may increase the operational risks or endangers the safety of passengers, crew, ground personnel and the general public, or is a potential compliance breach. This included the identification or observation of a vulnerability in the protection of civil aviation against acts of unlawful interference.
Security programme	Written measures adopted to safeguard international civil aviation against acts of unlawful interference.
Security restricted area	Those areas of the airside of an airport which are identified as priority risk areas where, in addition to access control, other security controls are applied. Such areas will normally include, inter alia, all commercial aviation passenger departure areas between the screening checkpoint and the aircraft, the ramp, baggage make-up areas, including those where aircraft are being brought into service and screened baggage and cargo are present, cargo sheds, mail centres, airside catering and aircraft cleaning premises.
Security survey	An evaluation of security needs including the identification of vulnerabilities which could be exploited to carry out an act of unlawful interference, and the recommendation of corrective actions.
Security tamper-evident bags (STEBs)	Specially designed bags that shall only be used for the sale of LAGs by airport outlets or on board an aircraft.

Security test	A covert or overt trial of an aviation security measure which simulates an attempt to commit an unlawful act.
Security threat	A measure of the probability of an attack being committed or attempted against civil aviation operations or installations with the potential to harm life, systems, information, environment and/or property.
Sensitive aviation security information	Information that, if accessed by or disclosed to unauthorized persons, could create or be used to exploit a vulnerability or facilitate an act of unlawful interference against civil aviation.
Service panel	Aircraft external access point used for providing aircraft services including water, lavatories and ground electrical outlets, and other service compartments that have external clip-down panels.
Small arms	A general description applied to all hand-held firearms.
State of registry	The State on whose register the aircraft is entered.
State of the operator	The State in which the operator's principal place of business is located or, if there is no such place of business, the operator's permanent residence.
Sterile area	The area between any passenger inspection or screening checkpoint and the aircraft, into which access is strictly controlled (see also security restricted area.)
Stores (Supplies)	— For consumption. Goods, whether or not sold, intended for consumption by the passengers and the crew on board an aircraft, and goods necessary for the operation and maintenance of the aircraft, including fuel and lubricants. — To be taken away. Goods for sale to passengers and crew of an aircraft with a view to being landed.
Supernumerary	A person in addition to the flight crew that is not a cabin crew member but is on board either a cargo or passenger aircraft during commercial or non-commercial operations and is not classified as a passenger by the operator or the Authority.
Terminal	The main building or group of buildings where the processing of commercial passengers and cargo, and the boarding of the aircraft occurs.
Threat image projection	A software programme approved by the appropriate authority that can be installed on certain X-ray equipment, which projects virtual images of threat articles such as guns, knives, and improvised explosive devices within the X-ray image of a real bag under examination or complete virtual images of bags containing threat articles and provides immediate feedback to the X-ray equipment operators of their ability to detect such images.
Trace detection equipment	A technology system or combination of different technologies which has the ability to detect very small amounts of explosive materials, and so to indicate, by means of an alarm, any such materials contained in baggage or other articles subjected for analysis.
Transfer cargo and mail	Cargo and mail departing on an aircraft other than that on which it arrived.
Transfer passengers and baggage	Passengers and baggage making direct connections between two different flights.
Transit cargo and mail	Cargo and mail departing on the same aircraft as that on which it arrived.

Transit passengers	Passengers departing from an airport on the same flight as that on which they arrived.
Travel document	A passport or other official document of identity issued by a State or organization which may be used by the rightful holder for international travel.
Unaccompanied baggage	Baggage that is transported as cargo and may or may not be carried on the same aircraft with the person to whom it belongs.
Unclaimed baggage	Baggage that arrives at an airport and is not picked up or claimed by a passenger.
Unidentified baggage	Baggage at an airport, with or without a baggage tag, which is not picked up by or identified with a passenger.
Unpredictability	The implementation of security measures in order to increase their deterrent effect and their efficiency, by applying them at irregular frequencies, different locations and/or with varying means, in accordance with a defined framework.
Unclaimed baggage	Baggage that arrives at an airport and is not picked up or claimed by a passenger.
Unidentified baggage	Baggage at an airport, with or without a baggage tag, which is not picked up by or identified with a passenger.
Unpredictability	The implementation of security measures in order to increase their deterrent effect and their efficiency, by applying them at irregular frequencies, different locations and/or with varying means, in accordance with a defined framework.
Vulnerable point	Any facility on or connected with an airport, which, if damaged or destroyed, would seriously impair the functioning of the airport.

0.3.16 Acronyms and Abbreviations

Table 0-4: Acronyms and Abbreviations

ABP	Able-Bodied Person	LEDS	Liquid Explosives Detection System
ACI	Airports Council International	MANPADS	Man-Portable Air Defence Systems
ACRAF	Aircraft Cyber Risk Assessment Framework	MoU	Memorandum of Understanding
ACSP	Air Carrier Security Programme	MRP	Machine Readable Passport
AFS	Aeronautical Fixed Service	MRTD	Machine Readable Travel Document
AIT	Advance Image Technology	NCASC	National Civil Aviation Security Committee
ASC	Airport Security Committee	NCASP	National Civil Aviation Security Programme
ASP	Airport Security Programme	NCASTP	National Civil Aviation Security Training Programme
ASTP	Aviation Security Training Package	NCASQCP	National Civil Aviation Security Quality Control Programme

ATC	Air Traffic Control	PIDS	Perimeter Intrusion Detection System
ATS	Air Traffic Services	PoC	Point Of Contact
AW	Aerial Work	PTI	Positive Target Indicator
BD	Bomb Disposal	RA	Risk Assessment
BSP	Bomb Search Procedure	RCS	Risk Context Statement
CAA	Civil Aviation Authority	RFID	Radio Frequency Identification
CBT	Computer-Based Training	RPAS	Remotely Piloted Aircraft System
CCTV	Closed-Circuit Television	SARPs	Standards and Recommended Practices
CMT	Crisis Management Team	SCCM	Senior Cabin Crew Member
CPSRA	Critical Parts of Security Restricted Areas	SeMS	Security Management Systems
CIS	Crew Information Sheet	SMS	Safety Management System
CSS	Checkpoint Security Supervisor	SRA	Security Restricted Areas
CSIAD	Critical Systems, Information, Assets and Data	SRA	Safety Risk Assessment
CSSO	Chief Safety and Security Officer	STEB	Security Tamper-Evident Bag
DGCA	Directorate General Of Civil Aviation	TIP	Threat Image Projection
DEM	Duty Executive Manager	UN	United Nations
EOC	Emergency Operations Centre	UPU	Universal Postal Union
EOD	Explosive Ordnance Disposal	USAP	Universal Security Audit Programme
EDDS	Explosive Device Detection System	VIP	Very Important Person
EDS	Explosive Detection System	WTMD	Walk-Through Metal Detector

0.4 SECURITY MANAGEMENT SYSTEMS

Pegasus Airlines ACSP and all other documents pertaining to security requirements, guidelines and operating procedures are available to all staff members affected by the document. Clearly, not all air carrier employees will need to have access to all security procedures and documents drafted by Pegasus Airlines.

As the contents of the documents are typically of a sensitive nature, some control over who has access is to be outlined by the Aviation Security Department. The document sensitivity is set out during the preparation process on the Comply365 system.

Contractors shall also be in possession of the Pegasus Airlines ACSP or procedures deriving from it, either in its entirety or, at a minimum, of the sections that affect their service to Pegasus Airlines.

This process is to be implemented to amend or modify any security documentation that can certify that all interested and affected parties are in possession of the latest version of the specific security document.

Processes to be managed by Pegasus Airlines Aviation Security Department are described in this part of the security manual..

The Security Management System (SeMS) provides an organisation with a structured approach to managing security as an integral part of its overall business. A SeMS serves as a tool for systematically integrating security risk management into an organisation's day-to-day operations in close alignment with other risk management systems.

Implementation of the SeMS in Pegasus Airlines contributes to the development of proactive security practices in place of more traditional reactive procedures. SeMS is built on existing procedures and practices with the goal of adopting "best practice" standards. Consequently, SeMS serves to:

(a) strengthen the security culture;

(b) promote a threat-based managed approach to security;

(c) focus on performance, results and impacts; and

(d) promote effective internal and external partnership, collaboration and cooperation.

Development and implementation of a SeMS is also guided by the principles of interoperability (with other risk management systems), flexibility and adaptability. Cost effectiveness and appropriateness are also important considerations for an organization.

For optimum effectiveness, the security aspects of daily business activities, operational decisions and planning must always be consciously considered at every level of an organization. Aspects of a SeMS is integrated into the organization's structure in terms of coordinated activities, responsibilities, practices, procedures, processes and resources. At the same time, a strong security culture must prevail.

A SeMS is designed to be integrated with or connected to other structured management systems such as a Safety Management System (SMS) and Quality Management System, while also incorporating relevant parts of any informal management systems in Pegasus Airlines. Other management systems serve as a foundation for SeMS, thus minimizing duplication and expense while contributing to an organization's business capability and credibility.

SeMS leads to a threat-based risk-managed approach under which an organization can assess and best manage its own unique security risks, threats and impacts. It provides a framework that guides risk-based decision making at all levels of an organization by Pegasus Airlines. When documented, the rationale for arriving at such decisions strengthens corporate accountably and demonstrates due diligence.

Given the, SeMS may be defined as a formal, risk-driven method of integrating security into an organization's daily business operations and its management systems. It is used to implement an organization's security policy and to fulfil any regulatory requirements while optimally managing security risks, threats and impacts in the context of an enterprise's risk management framework.

Examples of items typically not covered by national authority regulation/requirement are listed below:

- Security objectives/measurements/KPIs
- SeMS review and improvement process
- Management of the security component within subcontracted functions and purchased products
- Specific oversight measures of security subcontractors
- Risk assessment of new destinations
- Continuous threat assessment and risk management of routes, destinations and en-route alternate airports
- Security measures for crew members during layovers

As per Standard 3.2.4 of ICAO's Annex 17, the ACSP shall be developed in written form and shared with the State's Appropriate Authority for formal approval. That formal approval shall be recognized as legal coverage for airlines implementing security measures at airports.

“Aircraft operator security programmes are generally drafted to meet the requirements of a National Civil Aviation Security Programme and other regulations of the aircraft operator's home State. To address the need for aircraft operator security programme variations required by other States and perhaps an aircraft operator's special circumstances, aircraft operators shall develop a supplementary station procedures program that may be appended to the aircraft operator security programme”.

0.4.1 Risk Management and Prioritization

The principle considerations in a risk-based approach are:

(a) risk is not zero and can never be zero;

(b) risk policy should be transparent, predictable and controllable;

(c) risk policy should focus on the largest risk; and

(d) risk policy should be equitable.

It is not possible to eliminate risk entirely. Regulating risk on this basis requires knowledge of the magnitude of the risk and a limit to how much risk is acceptable. In developing criteria for acceptable risk, it is important not to adopt a black and white approach. On the contrary, any set of criteria needs to allow room for negotiation and deliberation. Risk, then, can be considered to occur on three levels, namely:

(a) a level of risk that is so large it has to be deemed unacceptable regardless of the advantages that could be gained by taking the risk;

(b) a level of risk where a reduction should at least be considered, even if it could be tolerated; and

(c) a level of risk that is so small it can always be accepted.

A risk-based security will involve identifying and reporting on:

(a) security issues and concerns, including those associated with human factors, third parties and significant changes to operations, equipment, organizational structure, technology, suppliers or contractors;

(b) procedures to evaluate and classify the threats, risks and impacts; and

(c) formal threats and the probability of their occurrence, vulnerability, and the criticality of people, property, environment and the organization itself.

Several steps are required to implement an integrated risk management system. The main steps are outlined below:

(a) ***Establish a risk management framework.*** Senior management must endorse the integrated risk management approach and designate a risk management committee to establish the general and section-specific risk tolerance levels based on the overall corporate strategy of the organization;

(b) ***Identify risk exposures.*** In the case of security risk, the identification of risk will aim to determine where and how security incidents may occur. The aim of risk identification is to address causality by looking at both immediate and root causes. For example, in the case of a knife brought into a passenger cabin, screener error would be cited as the immediate cause, but the root cause may be inadequate training in the identification of threatening X-ray images. In any event, the only way to reduce the likelihood of a recurring incident is through remediation of the root cause;

(c) ***Perform risk assessment.*** Assess each risk exposure with regard to frequency (i.e. likelihood of occurrence) and criticality (i.e. probable impact). Such an assessment will lead to a quantification of risk;

(d) ***Determine priorities.*** Following risk quantification, identify which risk exposures are the most critical. This process helps address risks in order of importance by ensuring the implementation of appropriate procedures for key risk exposures. Risk “mapping” and a prioritization matrix are useful tools;

(e)

Analyse controls. Identify what controls are in place or have been implemented and, especially, establish a system capable of measuring whether current procedures are actually reducing risk;

(f) ***Develop an action plan.*** For each risk exposure, an action plan needs to be developed that pinpoints the following:

- exposure area;
- description of the issue;
- suggested remedial action;
- identity of the executive or entity that will champion the management activity; and • a timeline;

(g) ***Report.*** It is important to periodically report progress by assessing whether or not appropriate measures have been implemented. If there is evidence that some issues exist, corrective actions or a revised actions plan shall be implemented immediately; and

(h) ***Monitor.*** Overall risk exposure management and efforts to reduce risk need to be monitored closely by senior management and the risk management committee. Risk management shall be a standing agenda item addressed at all senior management or corporate board meetings.

0.4.2 Aviation Security Management Review

Pegasus Airlines have security review meetings for the purpose of ensuring:

(i) Senior management oversight of security in operations;

(ii) Continual improvement of the SeMS;

(iii) Security threats are being identified and controlled;

(iv) The promotion of security awareness.

Following regular meetings are held to make a review of the security performance in the operations, address security concerns, provide the feedback and instructions to the operating units and set the priorities for sub-teams on security issues.

0.4.2.1 Safety and Security Review Board Meetings

Table 0-5: Safety and Security Review Board Meetings

Safety and Security Review Board

Participants	• CEO (Accountable Executive) • Chief Safety & Security Officer • Chief Flight Operations Officer • EVP Technical • EVP Ground Operation • Chief Financial Officer • Compliance Monitoring Group Manager • Chief Commercial Officer • EVP Cabin Operations • Group Head of Internal Audit & Integrated Management Systems and Business Excellence • Chief Flight Academy Officer • Chief Human Resources Officer • Chief Information Technologies Officer • Aviation Security Leader (RP) • Relevant managers and consultants
Purpose	SRB ensures that appropriate resources are allocated to achieve the established safety and security performances of the Company and provide strategic direction to Safety Action Group.
Frequency	Four times a year
Conduct	Chief Safety & Security Officer
Chaired	CEO (Accountable Executive)

Agenda	• Safety & Security Policies Review
	• Organizational structure
	• Reporting lines, authorities, responsibilities
	• Action Items
	  • SRB, SAG, ERP, Audit Corrective Actions and Corporate Safety Strategy Actions.
	• Departmental Executive Summary
	  ○ Current Safety & Security Issues
	  ○ Safety & Security Events
	  ○ Departmental Resources
	  ○ Operational Feedback
	• Findings from operational Inspection and Results of audits
	• External/Internal Incidents/Accidents Investigations
	• Review and Analysis of Risk Picture (only under Chief Safety and Security Office)
	• Safety Performance Indicators and Targets
	• Safety Significant Events
	• Service Providers Activity Performance Statement
	• Progress Updates
	  ○ New Regulations, Legislation and Latest Safety & Security Promotions
	• Identification of Training Needs
	• Any other business (AOB)

Minutes	The meeting minutes are shared with all the participants. The decisions specified in the meeting minutes are assigned to responsible persons/departments via e-mail. In the next meeting, the previous meeting decisions are followed up on the Previous Meeting Decision page of the presentation.

For further details, please refer to PG-EM-EK-001 - Safety Management System Manual, available in Comply365.

0.4.2.2 Safety Action Group Meeting

Table 0-6: Safety Action Group Meeting

Discipline	**Safety Action Group Meeting**

Chief Safety and Security Office	Participants	Departments SAG Members from: • Safety, • Aviation Security, • Technical, • Chief Flight Operations Office, • Ground Operations, • Cabin Operations, • Cargo, • OCC, • Flight Academy, • Representatives (when necessary) from: ○ Human Resources, ○ Internal Audit ○ Performance ○ OHS ○ Compliance Monitoring ○ IOCC Vice President Please refer to PG-EM-BK-007 - SAG Members List, available in Comply365.
	Purpose	Monitor operational safety performance within their functional areas of the organization and ensure that appropriate SRM activities are carried out, Review available safety&security data and identify the implementation of appropriate safety&security risk control strategies and ensure employee feedback is provided, Assess the safety impact related to the introduction of operational changes or new technologies, Coordinate the implementation of any actions related to safety&security risk controls and ensure that actions are taken promptly and within agreed timescales, Review the effectiveness of specific safety risk controls, Review the effectiveness of previous safety&security recommendations and safety&security promotion.
	Frequency	Every month
	Conduct	Chief Safety and Security Officer (CSSO) and/or SMS Manager

Chief Safety and Security Office	Agenda	• Review of SAG Member List
		• Previous Meeting Decisions
		• SRB Decisions
		  ○ only the items that need actions or strategic directions are brought to the agenda
		• Safety Objectives / Safety Performance Targets (SPTs) and Safety Performance Indicators:
		  ○ Departmental SPI's
		• Action Items
		• Hazard Library
		  • New hazards that have been introduced or discovered in the workplace.
		• 3rd Parties – External Service Provider Report
		• Top 3 Events
		• Audits and Incidents/Accidents Investigation
		  ○ External/Internal Investigations and Audits
		• Safety Issue Risk Assessment Studies
		• Risk Analysis Studies
		• Safety Risk Assessment Studies
		• Summary of Safety Activities Attended by SAG Members
		• New Regulation, Legislation and Publication (SHGM, ICAO, IATA, EASA)
		  ○ Changes in regulatory policy or civil aviation legislation
		• Safety&Security Promotion

	Minutes	The meeting minutes are shared with all the participants. The decisions specified in the meeting minutes are assigned to responsible persons/departments via e-mail. In the next meeting, the previous meeting decisions are followed up on the Previous Meeting Decision page of the presentation.

0.4.2.3 Security Operations Monitoring Meetings - Department Internal

Table 0-7: Security Operations Monitoring Meeting - Department Internal

Discipline	**Security Operations Monitoring Meetings - Department**	
Aviation Security Department	Participants	Aviation Security Department
	Purpose	Review routine and non-routine security operations.
	Frequency	Every week
	Conduct	Aviation Security Leader (RP)

Aviation Security Department	Agenda	• Results of audits; • Findings from operational inspections and investigations; • Operational feedback; • Incident and occurrence reports; • Status of corrective and preventative actions; • Feedback and recommendations for management system improvement; • Regulatory violations • New hazards that have been introduced or discovered in the workplace; • Review of requirements or needs: ○ Materials, forms etc. ○ Trainings ○ Instructors' approvals ○ Meetings ○ Security related delays ○ Updates of regulations
	Minutes	Aviation Security Department

0.4.2.4 Ground Operations - Safety & Security Action Group Meeting

Table 0-8: Ground Operations - Safety & Security Action Group Meeting

Discipline	**Ground Operations - Safety & Security Action Group Meeting**	
Executive Vice Presidency - Ground Operations	Participants	• All Ground Operations units • Representatives from: • Safety • Security • Compliance Monitoring Management • Ground Operations Training
	Purpose	Evaluation of Safety and Security performance level in the context of Ground Operations to enable the mitigation of risk raised by Ground Operations and to develop the Safety and Security performance
	Frequency	At least - once in a month unless otherwise authorized by EVP Ground Operations
	Conduct	Internal notice / EVP Ground Operations

Executive Vice Presidency - Ground Operations	Agenda	• Operational, financial, administrative and management systems subjects that affect the performance level of Safety & Security in the context of Ground Operations • Related Actions
	Minutes	Distributed by Safety Advisor

0.4.3 Security Objectives and Security Performance Standards

Security objectives will derive from the vison, mission and, ultimately, the purpose of establishing the SeMS within the organization. This will be a prerequisite for further development of measurements and metrics, which are of importance for executive management.

The goal of security is to keep the business' risk exposure within the threshold acceptable for the executive management.

Measurements and metrics in security, as with other governance issues, shall be applied to reliably indicate the value that security is bringing to the organization.

As a result, measurements shall constitute Key Performance Indicators and Security Performance Indicators (KPI/SPI) leading to the establishment of relevant targets.

Metrics shall be developed based on what is meaningful for those seeking information from Security. Metrics will also influence the communication content.

Metrics shall be SMART:

- **Specific** to what is required and understandable,
- **Measurable** from available data,
- **Actionable/Achievable** driving change and positive results,
- **Relevan**t to what is important, and
- **Timely** because verifiably reliable data shall be there when you need it.

Pegasus Airlines Aviation Security Department's performance are monthly measured via:

- Key Performance Indicators (KPI) defined on the Ensemble Process and Performance Management System. Each KPI is related to a specific security process, also defined in the system.
- Safety Performance Indicators and Safety Performance Targets (SPI/SPT).

For further details, please refer to PG-EM-EK-001 - Safety Management Systems Manual and PG-EY-EK-001 - Quality Management System Manual, available in Comply365.

0.4.4 Security Culture

An enhanced security culture will strengthen the regulatory collaboration that can improve data sharing and analysis, which will lead to better trust, learning, development, regulation and enforcement, collectively. The system is cost-effective for set-up, modification of programmes and maintenance; it can also reduce enforcement costs. The benefits will also lead to better cross-border data management and enhance the commitment to continuous improvement among States and airlines.

The security culture in Pegasus Airlines is a type of organizational culture that encourages optimal security performance. The organizational culture is commonly understood to be a set of norms, beliefs, values, attitudes and assumptions that are inherent in the daily operation of organizations and abided by all entities and personnel within Pegasus Airlines. Just as leaders have a critical impact on organizations and their culture, organizational cultures greatly influence leaders by guiding their decisions. Organizations shall, therefore, ensure that the full commitment at every level of leadership, from top management to supervisors, is applied at all times and in all activities, strategies, policies and objectives to continuously improve the security culture.

Management will lead by example and encourage all employees to adopt a security mindset by advocating security as an organizational and personal value and aligning their own behaviour with this value. To establish or improve the security culture in organizations, measures are developed to enhance such norms, beliefs, values, attitudes and assumptions. These enhancements shall aim to further the following principles:

- Encourage awareness and alertness to security risks by all personnel
- Promote the role that employees play in identifying, eliminating or reducing security risks
- Allow the necessary time and make the necessary effort to comply with security measures, even when under pressure
- Promote willingness to accept responsibility, be proactive and make decisions autonomously in the event of security breaches or incidents
- Challenge other employees in case of irregularities and accept being challenged
- Immediately report incidents or any suspicious activity that might be security-related
- Foster critical thinking regarding security and an interest in finding potential security vulnerabilities and solutions
- Appropriately handle security-sensitive information

The Aviation Security Department promotes a sound security culture to create an atmosphere where every employee can transmit information they have gathered on security issues.

Major tools used to promote a security culture throughout the company include, but are not limited to, the following.

Table 0-9: Tools for the implementation of a positive security culture

Tool	Objective
Security Incident Reporting	Establish a reporting system that encourages and facilitates personnel to report security incidents and threats, identify security deficiencies and raise security concerns.
Clear and consistent policy, processes, systems and procedures	Enshrine security in all corporate policy and procedures, including those areas which do not have a primary security focus and document clearly in writing. Ensure the information is easy to understand, simple to follow, and readily accessible to staff who may want to refresh their understanding.
Corporate Screen Displays	Help employees to implement security by reminding them what actions they need to take.
Safety and Security Appreciations	Strong positive impact on security culture by personally thank those who have reported suspicious activity or security breaches.
Security Training	Provide all employees with the knowledge, skills and abilities to perform security duties, including knowledge about the threats to aviation security.

0.5 SECURITY RISK MANAGEMENT

0.5.1 Security Risk Assessment

It is clear that risks cannot be totally avoided or eliminated, it is equally clear the concept of risk assessment is not new.

Everyone in their personal and professional lives is constantly looking to evaluate and assess the data that is available before making, hopefully, a well thought out and considered decision that fits with the individual

or company 'risk appetite'. The goal being to reduce, as far as practicable, the possibility of something going wrong–and the potentially negative consequences that may arise as a result.

There will always be factors beyond our control or beyond our knowledge–such as new, evolving and/or as yet unknown, terrorist attack methodologies. We should also be aware that effective, efficient and timely risk mitigation strategies can be far less time-consuming and far less costly than post-event consequence management and recovery, but that just a threat continue to evolve so do mitigation considerations – thus the risk assessment and risk management process should ideally be subject to regular review and where necessary revision.

As a result, everyone faces the inevitable challenge of balancing all the risk management variables (including, at times, some with very little information or visibility) to make maximum use of limited time, resources, personnel and funding. In effect, the goal is to ensure that organizational capabilities and resources are utilized to the maximum effect, while at the same time seeking to prioritize activities in a proportionate, sustainable and carefully considered manner. This is particularly true when the damage (consequences) can be difficult to initially quantify and potentially even harder to recover – such as reputation.

Risk initially stems from the result of a threat (real or perceived) and is a combination of two factors:

- Intent—the desire someone may have to mount an attack
- Capability—their ability to commit the act they wish to undertake

The threat, when combined with a vulnerability, that is a weakness that an attacker may be able to exploit such as poor perimeter security, coupled with unanticipated or reasonably expected consequences that may result should a successful attack occur (e.g., in financial, human, reputational or operational terms), equates to risk.

From this calculation, one is required to factor in the degree of existing mitigation currently in place in terms of:

- Policy—The degree to which security activities and requirements are documented (e.g., via Standard Operating Procedures (SOPs), national regulatory requirements (NCASP), company specific procedural specifications, etc.)
- Practice—The degree to which security activities and functions are operationally delivered in line with documented requirements or standards in an effective and consistent fashion

While little can be done by individual entities (e.g., carriers, airports, cargo operators, ground handlers, caterers) to directly reduce any given threat (the intent and capability of potential perpetrators), reducing vulnerabilities or increasing mitigations will contribute to a reduction in risk and potentially minimize the consequences of attacks on the operations.

This section looks at the concepts of risk management and includes various subsections devoted to the individual elements within a risk assessment calculation (e.g., threat identification, vulnerability analysis and consequence assessment). In addition, it explores the importance of mitigation (both mitigation policy and mitigation practice) and the concept of residual risk (that element of risk that will continue to remain after existing mitigation factors have been considered and enacted).

Risk assessment is a fundamental component of risk management, which should form part of an organization's overall governance, values and culture. The effective and timely assessment of risk better enables appropriate authorities, airlines, airports and all other aviation entities and stakeholders wishing to improve their aviation security posture to more effectively evaluate security performance against the measures contained in airline and airport security programmes in a timely, effective and proportionate fashion.

ICAO prescribes the application of the risk assessment by national authorities. Standard 3.1.3 in ICAO Annex 17 states that:

"Each Contracting State should keep under constant review the level of threat to civil aviation within its territory and establish and implement policies and procedures to adjust relevant elements of its national

civil aviation security programme, accordingly, based upon a security risk assessment carried out by the relevant national authorities."

Moreover, the latest Annex 17 amendments expand this provision by introducing the recommendation 3.1.4 on periodic vulnerability assessments:

"Each Contracting State should ensure that periodic vulnerability assessments are conducted at its airports engaged in international operations, ensuring coordination among relevant departments, agencies, including appropriate law enforcement and intelligence authorities, and other entities. Such vulnerability assessments should be used to inform risk assessments and security improvements."

Airlines and other entities in aviation should perform security risk assessments in an effective and documented fashion to identify and address risks in a timely, consistent and transparent manner, to:

- Better protect their customers, staff, assets, brand, reputation and revenues
- Better prioritize the use and deployment of limited resources, including funds, technology, personnel, time and associated protective security activities
- Act as an early warning system
- Provide an effective audit trail for risk management decision-making
- Build and enhance the security culture within the organization

In the aviation security context, risk assessments are also a fundamental part of the Security Management System (SeMS), as they allow practitioners to evaluate, record and monitor their risks utilizing a standardized evidence-based methodology.

Risk assessments are a core element within a SeMS package and should be conducted periodically. For each organization, the meaning of "periodically" will vary depending on the organization's nature, size, configuration, etc. Every six months can be considered an adequate starting point for Security Departments, even though conducting the assessments more frequently, even in real time, is ideal. Some aspects (e.g., those with higher threat or residual risk levels), may require review far more frequently. The timing of the review(s) should also be a factor when considering and documenting a risk assessment process. A risk assessment is only one element of a SeMS package–discussion, communication, consultation and appropriate decision-making—are also key elements of an effective risk management strategy.

The minimum baseline for all airlines (indeed all regulated entities) should be to ensure consistent levels of compliance with all applicable international, regional, national and local aviation security regulations and standards. As such, an airline security risk assessment should focus on identifying gaps and determining the need for additional, or ad hoc, security measures to mitigate against risk–whether at the global or local (station) level. All applicable regulations and legislation should be identified and reviewed when performing a risk assessment–usually as part of existing compliance and/or mitigation reviews.

Ideally, airlines should have been involved in the risk assessments that led to the regulations being created or imposed. To ensure consistency, it is also recommended that the airline and the regulatory authority share the same understanding of the terminology used for assigning probability, likelihood and risk ratings–though the key issue is to conduct, evidence and document risk assessments in a timely and effective fashion, rather than to become potentially distracted by debating specific methodologies or processes. Ultimately, what is required is a clear and unambiguous understanding by the entity carrying the residual risk of where the issues sit and how best to effectively mitigate them to an acceptable level.

After sharing information horizontally across a company, the risk analysis and results are reported up the management chain and consolidated in a report for the Senior Management.

Note	Pegasus Airlines Aviation Security Department uses the risk assessment process established by the Safety Management Department. All details about risk assessments are described in the *PG-EM-EK-001 - Safety Management Systems Manual*, available in Comply365.

0.5.2 Threat Identification and Assessment

Threat assessment is based on a general analysis of the likelihood of an attack—composed of intent and capability. While threats cannot be eliminated, appropriate and timely measures can reduce the overall residual risk. The perceived threat level associated with aviation operations is influenced by the political situation, historical occurrences, media reports, open-source commentary and potential or real threats, among others.

Threat assessment is not a perfect science. Those deciding on a threat score will need to make a considered value judgment–considering all of the 'intelligence' that is available at the time of the evaluation. One approach could be to create, following a threat analysis, a matrix where different scores are assigned to individually identified threats. Many States employ a threat level chart to determine their national threat level and, in some cases, these are openly published.

Many factors and/or information outlets should be considered when allocating a threat score. Examples include, but are not limited to:

- **Government**—Official sources of threat level information exist in many States. The government or Civil Aviation Authority may operate and declare an overall threat level (e.g., 'High') for the State and/or various regions and/or cities and/or individual sectors (such as aviation) as well as include detail with respect to the particular attack methodology that may be used (e.g., 'ground-based armed attacks').
- **Police—State** or local police may also share/broadcast threat levels and/or anticipated attack methodologies. These advisories are not restricted to terrorism. They may advise on the threat of or risk from crime, sabotage, disruptive activities as well as the risk of an individual company, sector of society and/or location being targeted (e.g., via protestors).
- **Media**—Information that is useful in assessing a threat score can often be found/provided via media outlets and other open-source information channels, including local or national news channels. These can be of interest with respect to immediate events that may take time to result in a change in 'official' threat levels (e.g., the events of 9/11). Various attacks on airports, hotels and tourists are often widely communicated by the media/internet long before 'official' threat levels, declarations and/or additional advice, guidance or regulatory requirements are issued or altered.
- **Internal sources** — An organization's Board of Directors, management, security staff and internal audit/ quality control mechanisms can also educate a Security department's view of the threat score. For example, they may highlight/report incidents/events (locally, nationally or internationally) that cause them concern and could directly or indirectly influence the threat score evaluation.
- **Outsourced services** — Pegasus Airlines solicits services of companies/agencies providing constant flow of security threat information gathered from open and, whenever possible, restricted sources, in a close to real-time period regarding risk and threat analysis to the airline.

When the risk or a threat is immediate (according to Security Incident Risk Table available in Chapter 15.1.2), the CSSO or the Aviation Security Leader (RP) will inform the General Manager and other members of Emergency Response Plan by phone and initiate an appropriate response to the risk, as defined in Chapter 14. The effectivennes of taken actions is reviewed during review meetings.

For non-immediate risks and threats, the Aviation Security Department will bring them up to review meetings they attend such as Safety Review Board, Safety Action Group, Ground Handling Safety & Security Action Group Meetings.

Although there is a desire to harmonize threat assessment protocols, mechanisms and procedures globally (e.g., to have one acceptable template), many States have their own threat matrix devised with different threat levels and/or terminologies.

States that are signatories to the Chicago Convention have an obligation to gather intelligence and, therefore, if the process of delegation through a National Aviation Security Programme is correctly implemented, airlines and airports have a duty to progress the search for information.

Airlines and airports should be involved in lateral thinking. The nature of their business is one of global involvement in travelling to and from foreign airports and the transportation of people and property from

place to place. Some governments will not have knowledge or interest in a threat emerging on the other side of the world, especially when it does not have an impact on foreign policy. Airlines should impress on their States the importance of intelligence for carriers that have people and property entering a zone that is under threat.

Pegasus Airlines security risk assessment responsible managers:

(i) Have a high level of security clearance

(ii) Have a good working relationship with national intelligence-gathering agencies

(iii) Have regular meetings with intelligence agencies

(iv) Reach agreement about what intelligence is required and for what purpose

(v) Deliver to the intelligence agencies all information known to the airport/airline

It is also important in the aviation industry to cooperate towards building strong relationships to facilitate and develop the means of enhancing information exchange between airline operators and between the industry and governments. Within that context, States should continue to use proper channels to inform the industry on threats.

0.5.3 Risk Management Process

Figure 0-2: The Risk Management Process

Source: IATA SeMS Manual Revision 7

Step 1: Communication and Consultation

Communication and consultation with external and internal stakeholders take place during all stages of the risk assessment process. Depending on the nature of the risk, consideration is given to forming a consultative team to ensure that stakeholders understand the basis on which decisions are made and the reasons why particular actions are required. Given that security threats are not necessarily confined to a specific business or geographical area, an extensive internal and external security network is established and maintained to share information and recommended practices. This network includes government agencies, other entities of the organization, other industry organizations and the commercial security sector.

Recording should be done at each step. A system should be in place to keep track of assessments and decisions taken, to which the management and consultative team have access.

Step 2: Establishing the Context

By establishing the context, Pegasus Airlines Aviation Security Group Department articulates its objectives, defines the external and internal parameters to be considered when managing risk, and sets the scope and risk criteria for the remaining process.

What to do at this step:

- Define objectives
- Identify stakeholders and resources
- Allocate responsibilities
- Record the process in IQSMS Risk Module.

Step 3: Identifying the Risks and Possible Target Areas

Risks and possible target areas should be identified, and consideration given to areas of impact, events (including changes in circumstances), causal factors and the potential consequences. The list should be as comprehensive as possible and include identification of what might affect the achievement of objectives, where and when the impact might be observed, why the potential risk would happen, and how it could happen.

In Step 3, identify the threats:

- What can happen? (e.g., hijacking, airport bombing, sabotage, unruly passenger, hostage taking, chemical/biological/radioactive/nuclear threat)
- Where? (e.g., aircraft, airport terminal, apron, cargo terminal, fuel farm, air traffic control, runway)
- When? (e.g., check-in, taxiing, take-off, in flight, landing, immigration, day, night, anytime) • How? (e.g., firearms, explosives, knives, Man-Portable Air Defence Systems (MANPADS), chemical/ biological, dirty bombs, fake bombs, fists)
- Who? (e.g., organized terrorist group or individual ‘lone wolf’)
- Why? (e.g., political tensions, certain nationalities travel on the airline)

Sources of relevant, up-to-date information include, but are not limited to, national intelligence services, specialized companies’ security briefings and in-house dedicated personnel.

In the aviation security field, examples of threats include, but are not limited to:

- International, regional, national and local political events or industrial unrest that may affect aviation, airline operations or airline staff
- Terrorist activities
- Criminal activities

And, as always, record this process in the IQSMS Risk Module.

Step 4: Analysing the Risks

This step looks at the vulnerabilities:

- How widely known and understood is the vulnerability? (not very to very)
- How quickly and easily could the vulnerability be exploited? (not very to very)

Much of the information that will educate deliberations in this area is already available within the organization, but in many cases, may not be captured, reviewed or utilized to best advantage in a holistic fashion. It is also fair to acknowledge that vulnerability can be caused by lack of mitigation, and thus, may be assessed and evaluated when considering the degree of mitigation policy or practice that may already exist.

In some cases a feeling of ‘vulnerability’ may be based on a hunch that may be educated by years of experience and knowledge of the organization, but that is not a documented and evidence-based rationale. In many cases, a Security Manager will know where a potential vulnerability exists as a result of internal or external compliance and quality assurance audits–conducted by own security staff or assigned quality

auditors, external auditors or local Civil Aviation Authority compliance inspectors. Equally, an Aviation Security Leader may conduct a specific 'vulnerability assessment' that seeks to identify and quantify where and to what degree vulnerabilities may exist.

Those deciding on a consequence score (the effect of a successful attack or incident) will need to make a considered value judgment that realistically looks to make a credible and potentially 'worst case' scenario considering all the 'intelligence' that is available at the time of the evaluation. Many factors are considered when allocating a consequence score, including human, financial, operational and reputational damage.

It is also important to consider the degree to which mitigation plays a role in potentially reducing these factors (threat, vulnerability and consequence). Mitigations have two components:

- The documented security policies and mitigation practices in place (national, regional or local).
- The degree to which they are effectively implemented and practised in a timely and consistent fashion

The mitigation (policy) score will be assigned based on a value judgment that realistically looks to evaluate the policies that are currently in place. This should ideally include all existing internal security policies together with State documentation that must be adopted/adhered to (e.g., Local/National Aviation Security Programmes). In addition, policies should be viewed broadly as all documentation that clearly articulates the requirements of the organization. These could include, but are not limited to:

- Recruitment and retention policies/requirements
- Training policies and procedures
- CONOPs (Concept of Operations) and SOPs (Standard Operating Procedures) in relation to a wide variety of aviation related activities, including:
  - Cargo/passenger/hold baggage and in-flight supplies acceptance and screening o Cargo/passenger/hold baggage and airside protection
  - Perimeter/air-side protection
  - High-risk cargo
- Post orders
- Documented security audit and compliance procedures
- Equipment purchase, servicing, maintenance and testing requirements

Mitigation (practice) scorings are be based on the evaluation of the performance being delivered as adjudged by internal or external compliance/inspection regimes, quality assurance mechanisms, covert testing and/or relevant company compliance/delivery KPIs. These include, but are not limited to:

- Appropriate Authority Audit and Inspection findings (e.g., access controls, training records)
- Internal Audit, Inspection and Quality Compliance findings (e.g., TIP data, covert test information)
- Supervisory checks and oversight (e.g., x-ray testing logs/records, CSD documentation)

Calculating, documenting and evidencing individual scores with respect to threat, vulnerability, consequences and mitigations (policies and practices) will allow the risk manager/assessor to determine the overall residual risk score for each aspect or area evaluated–and will create a base for the prioritization of risk management decisions moving forward.

And, as always, record this process in the IQSMS Risk Module.

Step 5: Evaluating the Residual Risk and Setting Priorities

The residual risk evaluation stage aims to prioritize risks and assist decision-making as to the order in which the risks should be treated. To do so, Pegasus Airlines considers organization's risk tolerance/appetite levels (ensuring alignment with regulatory and/or other requirements for which tolerance levels may differ and/or be mandated), which assists in determining what action is required in the next step of the risk assessment process. Risks that are not within an organization's tolerance levels require the development

and implementation of a treatment plan; whereas risks that fall within the tolerance levels are deemed acceptable by the organization–such that no additional treatment plan is required.

What should be done under this step?

- Determine tolerance:
  - What risks may be accepted without further action?
  - What risks require action?
- Set priorities

And, as always, record this process in the IQSMS Risk Module.

Step 6: Treating the Residual Risk

Risk treatment involves identifying one or more options to mitigate or control the risks to a tolerable/ acceptable level and implementing the option(s). Selecting the most appropriate risk treatment option involves balancing the costs and efforts of implementation against the benefits derived as well as legal, regulatory and other requirements. In doing so, where possible, the root causes of the risk must be treated, and the mitigating actions and controls tailored to the cause (where possible). It should be noted that a decision may be taken to accept the risk 'as is' and not implement any controls to modify it. In all cases, these judgements–and the rationale behind them–should be evidenced, documented, recorded and periodically reviewed.

Mitigation of certain risks may sometimes not fall under Pegasus Airlines responsibility. In situations where, for example, another stakeholder has control over the mitigation measures or where there are certain legal impediments that do not permit optimal mitigation measures to be deployed, we are expected to apply our best efforts and work with the stakeholders to improve the situation–or, at the very least, to document, share and discuss concerns and associated recommendations.

The following actions should be considered once the risk assessment is performed and before assigning operational mitigations for each risk:

- Determine the duration for heightened threat conditions
- Become familiar with the operational environment
- Conduct an inventory of available security staff and equipment
- Review the current security measures in place

What should be done under this step?

- Identify one or more mitigating options for treating risk
- Prepare risk treatment and control action plans, including responsibilities, timeframes, expected outcomes, budgets and performance measures

And, as always, record this process in the IQSMS Risk Module.

Step 7: Monitoring and Review

Monitoringand periodic review should be a planned part of the risk management process, with the aim of monitoring the risk and the progress of any mitigating actions. Responsibility for this function is formally assigned and determination made as to how it will occur (e.g., periodic or ad hoc checking or surveillance).

In addition to a regular review, a change in the environment or organization might warrant an ad hoc review of the risks—if the change is likely to modify the overall risk profile.

What should be done under this step?

- Assigning responsibilities
- Reviewing risk ratings for every risk area
- Identifying any new or additional mitigating actions

And, as always, record this process in the IQSMS Risk Module.

Note	Pegasus Airlines Aviation Security Department has an integrated risk management process together with the Safety Management Department. All details about risk management are described under the PG-EM-EK-001 Safety Management Systems Manual, (available in Comply365). Any changes requiring an MOC study must be completed according to the *PG-EM-PR-001 - Management of Change Procedure*, available in Comply365.

0.5.3.1 IQSMS Risk Module

Registered risks in IQSMS Risk Module are reviewed to validate the effectiveness of safety risk controls regularly according to review date by the owner of the risks. When the reminder warning about risk review date is taken by risk owner via IQSMS.

Please review the *PG-EM-PR-010 - Risk Management Procedure* on how to conduct risk analysis studies.

For further information, please refer to PG-EM-EK-001 – SMS Manual, available in Comply365.

0.5.3.2 Threat and Risk Assessment Process Map

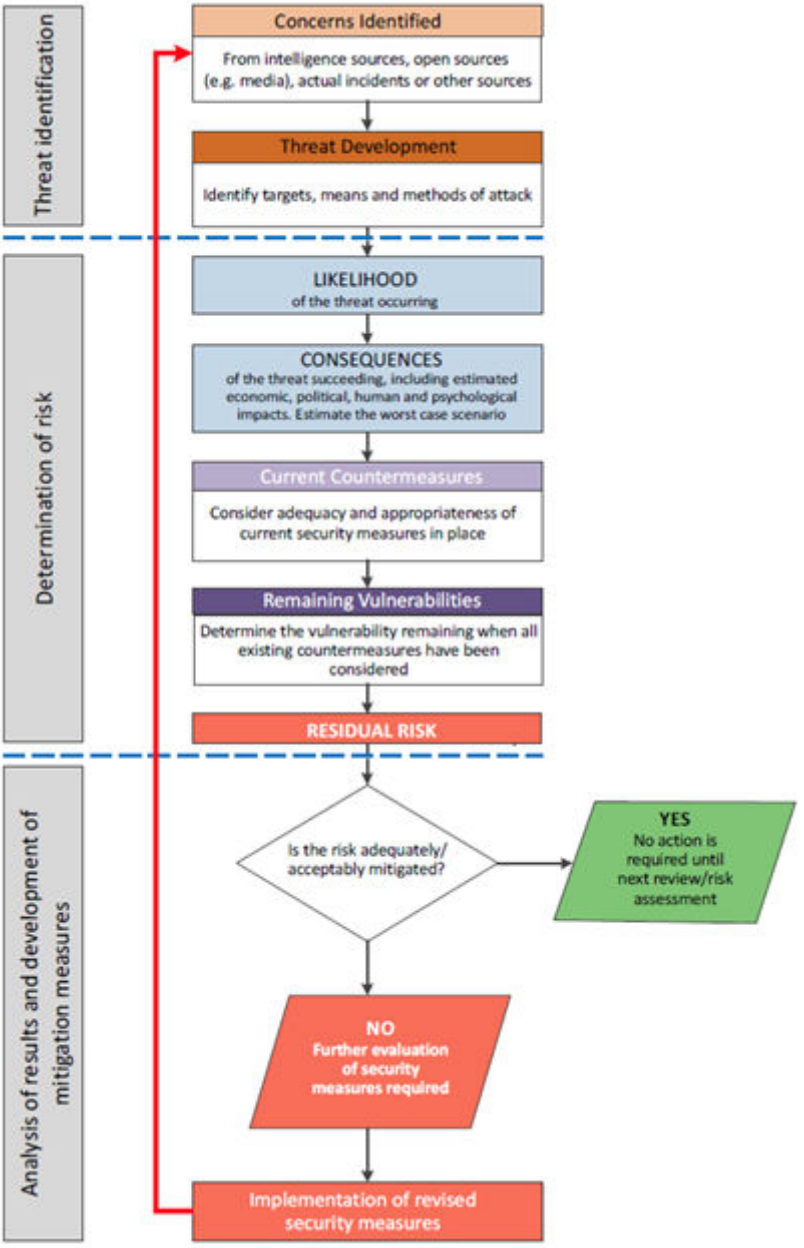


Figure 0-3: Threat and Risk Assessment Process Map

0.5.4 Insider Threats

An insider is a person who exploits, or has intention to exploit, their role or knowledge for unauthorized purposes. They may be full or part-time permanent employees, contractors, consultants, agency staff or temporary staff.

0.5.4.1 Insider Threat Description

There is a growing concern in today's world that an isolated few of the personnel employed within the operations could turn out to be the very people who target the aviation industry. The reality is that these are potentially the very people who leave the industry vulnerable to an attack. Addressing the insider threat is no easy task due to the risks posed by insiders.

Recent known cases of insider activity in the aviation industry demonstrate that the issue is not limited to terrorism, radicalization, nor to private industry:

Recent Known Cases of Insider Activity in the Aviation Industry		
Date	**Country**	**Case**
February 2016	Somalia	On 2 February 2016, an explosion occurred on board the aircraft after it took off from Mogadishu (Daallo Airlines Flight 159). Investigation revealed airport employees were part of the plot.
September 2015	Philippines	25 employees of the Office of Transport Security were suspended for extortion
July 2015	USA	46 airport-based employees were indicted in Dallas-Fort Worth International Airport for smuggling drugs.
June 2015	Uganda	Five members of the staff at Entebbe Airport were arrested for their involvement in facilitating the smuggling of more than 600 kg of ivory onto a flight to Singapore.
May 2015	Austria	In Vienna, a group of airport employees, including two employed in aviation security activities were involved in smuggling illegal migrants to the UK.
May 2015	Venezuela	24 criminal gangs were identified to be operating at Simon Bolivar International Airport, resulting in the arrest of 42 airport-based employees.
February 2015	USA	Two airport security screeners, contracted by the TSA at San Francisco International Airport, were arrested and charged with bribery and drug trafficking.

Source: AAPA

Figure 0-4: Recent Known Cases of Insider Threat in the Aviation Industry

The existence of threats from within an organization is a widely recognized phenomenon. There have been numerous analyses conducted to explain the mechanisms through which an insider threat may grow. A simplified process is outlined below:

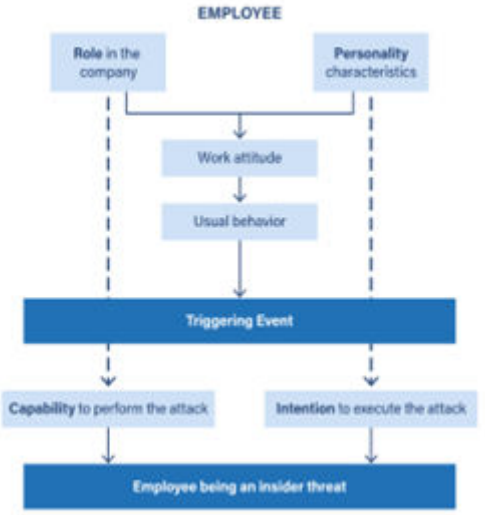


Figure 0-5: Growing Insider Threat Process

The triggering event that turns an employee into a threat may be one or more of the following: home-life conflicts, work stress, regional or global tensions as well as direct approach (e.g., financial inducement); currently most attention is given to the topic of radicalization.

One description of radicalization is a situation where an individual feeling unfairly treated, deprived, marginalized or aggrieved takes violent action for what S/he believes is justice.

While, like terrorism, radicalization has many definitions, it is a process an individual goes through. According to scientific research, such an individual may be spotted due to changes in his/her behaviour or personality.

Identifying these changes might be an opportunity to spot a potential insider threat growing within the organization, and either initiate a process for de-radicalization or address the issue to mitigate the risk.

Examples of indicators related to deviant behaviour being a basis to suspect an insider threat include:

- Perceived injustices
- Openly speaking out against the leadership or the company
- Signs of depression
- Asking for access to sensitive information without business need
- Unjustified work pattern

- Repeated violation of organizational policies
- Chronic expression of under-recognition
- Attempts to bypass security controls
- Unusually high interest in security measures
- Unusually high number of security violations
- Deliberate omission or falsification of company materials
- Obvious changes in financial status with no rational explanation
- Decreased quantity and quality of work
- Unusual questioning of co-workers about information/areas to which S/he does not have access

Each of these indicators on its own may not necessarily be an indication of insider activity, so proper investigation is necessary to assess if alternative explanations are likely.

0.5.4.2 Insider Threat Policy

Pegasus Airlines insider threat policy is to ensure that there are appropriate procedures and processes in place that are described in point 12. of this ACSP to effectively manage the insider threat.

Our policy is to be focused on terror-related activity and covers a range of activities that could damage the company finances or reputation (e.g., involvement in significant fraud).

The policy is to consider the development of a risk assessment for relevant staff roles where exposure to risk from an insider threat perspective has the potential to create significant damage to Pegasus Airlines.

We also consider assessing the nature and magnitude of the risk and implementing appropriate measures to manage the risk (please refer to point 12.). Our process clearly shows the company tolerability with this process and the measures implemented, depending on the risk provided by the role.

At the stage where it will be appropriate to consider the handling of insider cases, once a concern has been raised by a member of staff, an authority, or an individual from outside the operator, all further actions are taken in accordance with the PG-YO-YN-002 Disciplinary Regulation (Stop and Spot Measures) available in Comply365.

For staff, this awareness can be part of their vigilance when conducting everyday routines and ensuring that company processes are applied consistently to prevent, or at least restrict, actions by insiders; internal communications are set as an important part in supporting the security culture, and the insider threat is included in the communication/reporting systems of Pegasus Airlines.

All persons performing their duties in security restricted areas of airports, are subjected to additional criminal background checks by the relevant authorities and this issue is regarded by Pegasus Airlines as an additional barrier for insider threat assessment.

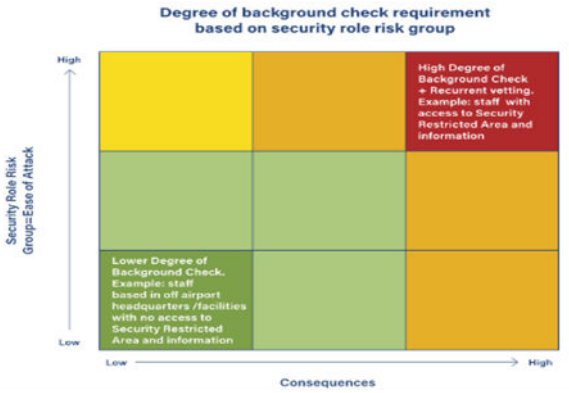


Figure 0-6: Degree of background check requirement based on security role risk group

Within the SeMS, reports on suspected or actual insider activity are reviewed by Security in conjunction with Human Resources, with the discussion aimed at evaluating the risk to the company following an insider security occurrence. This could help to mitigate the potential for future unidentified risks.

0.5.5 In-Flight Theft

The primary targets for in-flight theft are believed to be the substantial amounts of cash, jewellery and personal electronic devices carried in cabin baggage. Due to the international nature of our operations, there may be a lack of clarity on enforcement in the case of in-flight theft, especially regarding the following:

- Applicability of jurisdiction (aircraft State of registry? State of arrival? State of departure? AOC-issuing State?)
- Law enforcement agency appropriate to report the incident to
- Threshold level for reporting the theft as a criminal offence
- Documentary requirements for the purposes of prosecution

Therefore, the guidance provided below cannot always be successful in deterrence or mitigation of the risk of in-flight theft. Still, Pegasus Airlines considers implementation of the measures mentioned below.

0.5.5.1 On the Ground

- Flagging certain reservations - If the information is available, the cabin crew should be made aware (e.g., during the briefing) of a passenger or a group (e.g., under the same PNR and with a return flight on the same day) requesting separate seating in the aircraft cabin.
- Training for cabin crew may include:
  - Attention to passengers who intentionally stow personal belongings or cabin baggage at a distance from one's assigned seat
  - Attention to passengers requesting a seat change (for no stated reason) and to be seated next to someone the passenger does not know (especially when the requested seat is on the aisle)
  - Reporting in-flight theft through the operational reporting system (e.g., Cabin Safety Reports) in order to implement the *PG-GU-PR-003 - Unruly Passenger Procedure,* available in Comply365.
- Providing crew members with organizational and legal assistance in case they are called to act as a witness for the prosecution.

0.5.5.2 In the Air

- Providing advice to passengers to protect and avoid exposing carried valuable items
- Observe passengers exercising certain (above-mentioned) behaviours
- Ensure proper cooperation and coordination between the cabin and cockpit crews to agree on the course of action upon landing (e.g., requesting law enforcement at the aircraft door upon reaching the parking position if necessary)

0.5.6 Aviation Cyber Security Management

0.5.6.1 Application of ISMS to Cyber Management Framework

Pegasus Airlines is certified with the standard of ISO/IEC 27001:2017 Information Security Management Systems.

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization’s information risk management processes.

According to its documentation, ISO 27001 is developed to "provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system."

ISO 27001 uses a top down, risk-based approach and is technology-neutral. The specification defines a six-part planning process:

- Define an Information Security Policy.
- Define the scope of the ISMS.
- Conduct a risk assessment.
- Manage identified risks.
- Select objectives and controls to be implemented.
- Prepare a statement of applicability.

The specification includes details for documentation, management responsibility, internal audits, continual improvement, and corrective and preventive action. The standard requires cooperation among all sections of an organization.

According to the Ministry of Transport and Infrastructure Corporate SOME Installation and Administration Guidance (PG-BG-KD-00001, available in Comply365), monthly SOME (intervention team for cyber events) meeting are carried out about the review of the Cyber Security Risk assessments, news, sharing of information.

For further details please contact the Information Security Management Department via itsecurity@flypgs.com and refer to PG-EY-PR-008 Information Risk and Opportunity Management Procedure (available in Comply365).

0.5.6.2 Governance, Management and Responsibilities

Pegasus Airlines' Head of Information Security Risk and Compliance is responsible for ensuring the security of Pegasus Airlines' information systems and communication networks and protecting them against internal and external threats.

For more details, please refer to *PG-BG-GT-006 – Head of - Information Security Risk and Compliance Job Description*, available in Comply365.

0.5.6.3 Cyber-Security Culture, Awareness and Training

Much like a physical security culture, the aviation industry needs to have a well-established cyber security culture that encompasses all elements of the sector, reaching from operations into the supply chain and from the most senior levels down to the most junior.

As a crucial element of the entire industry, the cyber security culture should be included together with business innovation, procurement, recruitment and flight operations.

It is important that cyber security plays a key role in the organization and is part of the personnel training. This will allow the personnel to understand their roles and responsibilities to keep the organization safe, secure and resilient to cyber threats.

Every employee with access to company computers receives an initial on-line cyber/information briefing at the beginning (first month) of employment and repeated once every year in accordance with *PG-EG-PR-001 - Training Procedure* article 5.3.2.3 Information Security Training. Those without computer access receive in class training.

0.5.6.4 Cyber-Security Risk Management

"Pegasus Airlines Security Management has an integrated risk management process together with the Information Security Management. All details about cyber-security incident reporting and risk management are described under the *PG-BG-PR-002 - Information Security Management System Procedure* and *PG-BG-PR-024 Information Security Incident Procedure* available in Comply365."

Any occurring cyber-security incident should be reported to Information Security Management via the Incident-Reporting Module, integrated in Comply365.

0.5.6.5 Incident Management Response

Reporting Security incidents and concerns is a component of Pegasus Airlines' Security culture embedded in its SeMS principles.

In terms of cyber-security, reporting is similarly essential as a preventive security control contributing to reinforcing cyber resilience. This reporting should come from both IT Teams and end-users (Pegasus Airlines employees), and should include any unusual performance of affected systems, data and processes that include a cyber component.

Incident reporting that leads to an analysis of vulnerabilities not only enables an increased level of security but also a major component of raising situational awareness.

End of Section

1 INTERNATIONAL OBLIGATIONS AND ORGANIZATIONS

“States are mandated to require aircraft operators to submit and receive approval of their ACSP according to their national rules to ensure applicable requirements of their National Civil Aviation Security Programme (NCASP) are adhered to. At the same time, States must ensure relevant information is available to the aircraft operators as per ICAO Annex 17 Standard 3.1.9.3.”

1.1 THE STRUCTURE AND ROLES OF ICAO AND ECAC

International Civil Aviation Organization (ICAO): International Civil Aviation Organization is the central (government) civil aviation organization, a specialized organization of the UN. It derives the right of existence from part II, Articles 43-66 of the Chicago Convention. The ICAO is entrusted with the unification of rules in international civil aviation transport, inter alias, by drawing up annexes that have been appended to the Chicago Convention.

European Union (EU): The European Union is involved in the European organization in the field of civil aviation security. Based on the Regulation of 16 December 2002, the European Commission has powers to further develop the common rules.

European Civil Aviation Conference (ECAC): The European Civil Aviation Conference is an organization in the field of aviation and it has been set up to coordinate European aviation and to supervise the development of European aviation, as well as to help to resolve the problems that arise.

1.2 THE PURPOSE OF THE VARIOUS CONVENTIONS, ICAO ANNEXES AND ECAC DOC. 30

Chicago Convention 1944

The Convention expresses three basic principles:

- the idea that States must be able to participate in air transport on the basis of equality;
- the acknowledgement of the complete and exclusive sovereignty of States above their own territory;
- the development of civil aviation in a safe and orderly manner.

Article 38 of the Convention provides that any State which finds it impracticable to comply with the standards and/or recommendations laid down in the Convention and Annexes must give notice of this to the ICAO whilst stating the articles it has failed to comply with and the reason for non-compliance.

Tokyo Convention 1963: Convention on Offences and Certain Other Acts Committed on Board Aircraft

The Convention has the following objectives:

- to establish which penal law applies where the action is conducted in a lawless area;
- to establish what the rights and obligations of the aircraft Pilot-in-Command are;
- to establish what the rights and obligations are of the States where the aircraft, which has on board a person guilty of a punishable conduct, lands.

The Hague Convention 1970: Convention for the Suppression of Unlawful Seizure of Aircraft

The Convention applies where:

- the unlawful seizure and ancillary acts must occur during the flight;
- there must have been some (threat of) use of violence;
- the acts must result in the unlawful seizure of an aircraft, or at least be regarded as an attempt to do so.

Montreal Convention 1971: Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation

The Convention applies as long as the aircraft is in service, which may be defined as the moment at which the activities with respect to a specific flight commence until 24 hrs after landing.

Protocol supplementing the Montreal Convention 1988: Concerns a supplement to Article 1 of the Montreal Convention.

Any person commits a criminal offence if he:

- unlawfully and intentionally commits an act, whether or not using any device, substance or weapon;
- commits an act of violence against a person on an airport serving international civil aviation, where this causes or is likely to cause serious injury or death;
- destroys or seriously damages the facilities of an airport serving international civil aviation or aircraft not in service located thereon ordisrupts the services of the airport;
- commits an act which endangers or is likely to endanger security on the airport.

Convention on the Marking of Plastic Explosives for the Purpose of Identification

This Convention obliges States to take measures to prohibit and prevent the fabrication of unmarked explosives (plastic explosives containing no means/substance of recognition) on their territory, and in addition to take preventive and/or prohibitive measures to counteract the import and export of unmarked explosives from and to their own country.

ICAO Annex 17 provides that every Member State must have a National Civil Aviation Security Programme.

ECAC Document 30 incorporates the most recent recommendations in the field of security.

1.2.1 Relevant EU Security Regulations

Table 1-1: Relevant EU Security Regulations

Council Regulation (EC) 300/2008 of the European Parliament and of the Council	On common rules in the field of civil aviation security and repealing Regulation (EC) No 2320/2002
Commission Regulation (EU) 18/2010	Amending Regulation (EC) No 300/2008 of the European Parliament and of the Council as far as specifications for national quality control programmes in the field of civil aviation security are concerned
Commission Regulation (EC) 272/2009	Supplementing the common basic standards on civil aviation security laid down in the Annex to Regulation (EC) No 300/2008 of the European Parliament and of the Council.
Commission Regulation (EU) 297/2010	Amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security.
Commission Regulation (EU) 720/2011	Amending Regulation (EC) No 272/2009 supplementing the common basic standards on civil aviation security as regards the phasing-in of the screening of liquids, aerosols and gels at EU airports.
Commission Regulation (EU) No. 1141/2011	Amending Regulation (EC) No. 272/2009 laying down measures for the implementation of the common basic standards on aviation security in respect of security scanners.
Commission Regulation (EU) No. 245/2013	Amending Regulation (EC) No 272/2009 as regards the screening of liquids, aerosols and gels at EU airports
Commission Regulation (EU) No. 1254/2009	Setting criteria to allow Member States to derogate from the common basic standards on civil aviation security and to adopt alternative security measures
Commission Regulation (EU) No. 72/2010	Laying down procedures for conducting Commission inspections in the field of aviation security
Commission Implementing Regulation (EU) No. 2015/1998	Laying down detailed measures for the implementation of the common basic standards on aviation security

Commission Implementing Regulation (EU) No. 2017/815	Amending Implementing Regulation (EU) 2015/1998 as regards clarification, harmonisation and simplification of certain specific aviation security measures
NOT FOR PUBLICATION – Implementing Decisions under Regulation 300/2008	
Commission Decision C(2015) 8005	Laying down detailed measures for the implementation of the common basic standards on aviation security containing information as referred to in point (a) of Article 18 of Regulation (EC) No 300/2008.
Commission Decision C(2017) 3030	Amending Commission Decision C(2015)/8005

1.2.2 Powers of the Aircraft Pilot-in-Command

In accordance with Turkish National Civil Aviation Law 2920 (articles 100-103), International Civil Aviation regulations (Tokyo Convention, ICAO Annex 17, ECAC Document 30, Regulation (EU) No. 965/2012), an aircraft Pilot-in-Command is authorized to:

(a) protect the safety of the aircraft and the persons and property on board;

(b) maintain good order and discipline on board;

(c) restrain persons on board who may be a threat to safety;

(d) disembark or deliver to the competent authority's persons who may be a threat to safety;

(e) notify the authorities of a State as soon as practicable and preferably before landing in the territory of that State that a person on board is under restraint;

(f) furnish authorities of the State with evidence and information regarding the incident that necessitated the disembarkation and/or handover of a passenger;

(g) attempt to land as soon as practicable at the nearest suitable aerodrome or at a dedicated aerodrome assigned by the appropriate authority unless considerations aboard the aircraft dictate otherwise;

(h) refuse transportation of inadmissible passengers, deportees or persons in custody if their carriage increases the risk to the safety of the aircraft or its occupants.

End of Section

2 NATIONAL OBLIGATIONS AND RESPONSIBILITIES

The Turkish National Security Programme has been prepared and conducted in accordance with the National Legislation below, and Pegasus Airlines ACSP has been prepared and is conducted accordingly.

Table 2-1: National Legislation

Law Number	Name
2920	Turkish National Civil Aviation Law
5442	Administrative District Law
2559	Police Duties & Responsibilities Law
2803	Gendarme Duties & Responsibilities Law
5188	Special Security Service Law
4749	Public Finance and Debt Management Law
4926	Preventative Smuggling Law
4458	Turkish Custom Law
6698	Personal Data Protection Law
Directive	Maintain Security at Civilian Airports, Borders & Ports Regulation
Directive	Airport Special Security Organization Protection Services Directive
Directive	Regulation on Procedures and Principles Regarding the Obligations of Airline Carriers
Decree	Organization of Affiliated, Related, Associated Institutions and Organizations with Ministries and Other Institutions and Organizations
SHT-17.3	Civil Aviation Security Management and Organization Directive
SHT-17.6	Air Cargo and Mail Security Directive
MSHGP (NCASP)	Turkish Civil Aviation Security Programme

2.1 THE RELEVANT AUTHORITY FOR THE STATE OF THE REGISTRATION

Turkish Directorate General Civil Aviation (TR-DGCA) is the authority for the State of Registration. The Headquarter of the TR-DGCA is located in Ankara and the complete address is given below:

Table 2-2: Turkish Directorate General Civil Aviation (TR-DGCA)

Name	DIRECTORATE GENERAL OF CIVIL AVIATION
Address	GAZİ MUSTAFA KEMAL BULVARI NO: 128/A 06570 MALTEPE
City	ANKARA
Country	Türkiye
Office Phone	+90 312 203 60 00
Fax	+90 312 212 46 84
E-Mail	security@shgm.gov.tr

2.2 THE RELEVANT APPROPRIATE AUTHORITY FOR THE HOST STATE OF OPERATION

The following is a list of the countries and their respective Civil Aviation Authorities' contact details where Pegasus Airlines operates. These informations are regularly controlled via official websites by the Aviation Security Department.

Table 2-3: Foreign Civil Aviation

Afghanistan	+93 20 2311954	farhad@motca.gov.af	**Latvia**	+371 67830940	maris.gorodcovs@caa.gov.lv
Albania	+355 4 2251220	info@acaa.gov.al	**Lebanon**	+961 1 628195/6/7	dgca@beirutairport.gov.lb
Algeria	+213 21 920921	azzi@ministere-transports.gov.dz	**Liberia**	+231 776 998800	rwilliams.dirgen@liberiacaa.com
Argentina	+54 11 5941 3000 / 7	info@anac.gov.ar	**Libya**	+218 91 731 2343	n.shaebelain@caa.gov.ly
Armenia	+374 10 28 20 66	sergey.avetisyan@aviation.am	**Lithuania**	+370 5 273 9260	caa@caa.lt
Austria	+43 1 71162 659800	elisabeth.landrichter@bmvit.gv.at	**Luxembourg**	+352 247 74900	info@dac.public.lu
Azerbaijan	+994 12 598 5191	hq@caa.gov.az	**Mali**	+223 20 20 80 56	anac-mali@anac-mali.org
Bahrain	+973 1732 1112	m.alkaabi@mtt.gov.bh	**Malta**	+356 2555 5642	info.tm@transport.gov.mt
Bangladesh	+880 2 8901400	chairman@caab.gov.bd	**Monaco**	+377 9898 8024	aviation-civile@gouv.mc
Belarus	+375 17 222 53 92	gka@caa.gov.by	**Montenegro**	+382 20 625 506/7	acv@caa.me
Belgium	+32 2 277 43 00	civilair@mobilit.fgov.be	**Morocco**	+212 66 3732192	k_cherkaoui@mtpnet.gov.ma
Bosnia and Herzegovina	+387 51 92 12 12	bhdca@bhdca.gov.ba	**Myanmar**	+95 1 533015	dgdca@dca.gov.mm
Bulgaria	+359 2 937 1000	directorgeneral@caa.bg	**Netherlands**	+31 70 456 1656	rob.huyser@minienm.nl
China	+86 10 6409 1247	jr_yang@caac.gov.cn	**Niger**	+227 20 72 32 67	aayaha@yahoo.fr
Croatia	+385 1 6169060	uprava@caacro.hr	**Nigeria**	+234 1 279 0421	
Czechia	+420 225 131 390	sekretariat.220@mdcr.cz	**Norway**	+47 75 58 50 00	postmottak@caa.no
Denmark	+45 36 18 60 00	info@trafikstyrelsen.dk	**Oman**	+968 24354442	info@paca.gov.om

Egypt	+202 2267 7617	ecaa@civilaviation.gov.eg	**Pakistan**	+92 21 9924 2002	dgcaa@caapakistan.com.pk
Equatorial Guinea	+240 333 15 82 x 200	miko.angue@caage.org	**Poland**	+48 22 520 75 20	sekretariat@ulc.gov.pl
Estonia	+372 610 3589	kristjan.telve@ecaa.ee	**Qatar**	+974 4455 7100	chairman@caa.gov.qa
Finland	+358 29 534 5000	airtransportpolicy@trafi.fi	**Republic of Moldova**	+373 22 52 40 64	info@caa.gov.md
France	+33 1 58 09 36 94	patrick.gandil@aviation-civile.gouv.fr	**Romania**	+40 21 319 62 09	dgavc@mt.ro
Georgia	+995 32 294 80 02	office@gcaa.ge	**Russian Federation**	+7 495 645 85 55	rusavia@scaa.ru
Germany	+49 228 300 4500	al-lf@bmvi.bund.de	**Saudi Arabia**	+966 2 684 7007	aalbadir@gaca.gov.sa
Ghana	+233 30 2776171	info@gcaa.com.gh	**Serbia**	+381 11 292 71 12	dgca@cad.gov.rs
Greece	+30 210 89 16 507	governor@hcaa.gr	**Slovakia**	+421 2 5949 4744	dgca@mindop.sk
Guinea	+224 628 22 00 36	kabaviation49@yahoo.fr	**Slovenia**	+386 1 47 88 201	mzip.letalstvo@gov.si
Hungary	+36 1 795 6836	dgca@nfm.gov.hu	**South Africa**	+27 11 545 1017	khozap@caa.co.za
India	+91 11 24620784	dgoffice@dgca.nic.in	**Spain**	+34 91 597 53 55	ofri.dgac@fomento.es
Iran, Islamic Republic of	+98 21 66025230	abedzadeh@cao.ir	**Sweden**	+46 11 415 21 02	luftfart@transportstyrelsen.se
Iraq	+964 79016 7505	dg@iraqcaa.com	**Switzerland**	+41 58 465 80 39	security@bazl.admin.ch
Ireland	+353 1 6041510	fintantowey@dttas.ie	**Republic of Macedonia**	+389 2 3181 601/3	gjandreoski@caa.gov.mk
Israel	+972 3 977 4555	feldschuhj@mot.gov.il	**Tunisia**	+216 71 906 563	kamel.miled@mt.gov.tn
Italy	+39 06 44 596 1	a.quaranta@enac.gov.it	**Türkiye**	+90 312 203 60 10	info@shgm.gov.tr
Jordan	+962 6 489 2282-3400	c.commissioner@carc.gov.jo	**Turkmenistan**	+993 12 35 10 52	aviahead@online.tm
Kazakhstan	+7 7172 754 802	b.seidakhmetov@mid.gov.kz	**Ukraine**	+380 44 351 53 45	vdz@avia.gov.ua
Kenya	+254 20 827470-5	info@kcaa.or.ke	**United Arab Emirates**	+971 2405 4489	dg@gcaa.gov.ae

Kuwait	+965 2 431 5600	president@dgca.gov.kw	**United Kingdom**	+44 207 944 2400	dan.micklethwaite@dft.gsi.gov.uk
Kyrgyzstan	+996 312 25 16 19	mail@caa.kg	**Uzbekistan**	+998 71 120 00 60	caa@uzcaa.uz

2.3 THE NATIONAL AVIATION SECURITY PROGRAMME OF THE HOST STATE

Pegasus Airlines Security Programme is drafted to meet the requirements of the Turkish National Civil Aviation Security Programme and other regulations.

To address the need for Pegasus Airlines Security Programme variations required by other States, and to accommodate airport-specific or operator-specific circumstances, Pegasus Airlines has developed Supplementary Station Security Procedures (SSPs). Where required by the competent authority, these SSPs may be appended to this Air Carrier Security Programme (ACSP). The objectives of the SSPs are to protect passengers, personnel, assets, aircraft, and customer property against acts of unlawful interference; to ensure compliance with national and local regulatory requirements of the States of operation aimed at safeguarding passengers, crew, ground personnel, and the general public against security threats; to address airport-specific security requirements, infrastructure limitations, and operational constraints imposed by airport operators or local authorities; and to ensure the consistent implementation of Pegasus Airlines' security standards across all stations while allowing justified local variations based on risk and regulatory requirements.

The SSPs are prepared, controlled, and managed within the Comply365 Documentation System in accordance with PG-DU-EK-001 – Documentation System Manual.

For details of the Security Programme of the host states please refer to the Local Security Instructions *PG-GU-EK-Doc.No* (available in Comply365, reference number changing according to the country) or contact security@flypgs.com.

End of Section

3 AIRLINE SECURITY POLICY AND ORGANIZATION

3.1 AIRLINE SECURITY POLICY

(PG-GU-PO-001, available in Comply365)

The security policy of Pegasus Airlines is to ensure the security and control of all Pegasus operations while taking into account the rules and regulations stipulated by national and international authorities, and also company procedures. To ensure that efficient procedures are implemented and staff are trained so that in the event of a major security event the incident may be controlled in the most effective manner.

The overall responsibility for standards of security within Pegasus Airlines lies with the responsible Manager, however he gives the operational running of these responsibilities to the Aviation Security Leader (RP). However, all department managers are responsible to implement, improve and report the security related cases as regards their own department's security.

For a continual improvement, the Security Policy is reviewed twice a year by the Senior Management during Compliance Monitoring Management Review Meetings (please refer to PG-YO-EK-001 Corporate Manual, available in Comply365).

In all of its operations, Pegasus Airlines hereby commits:

- **Operational Security**

Pegasus Airlines guarantees to ensure the security of operations, employees, passengers and service providers. For this purpose, the company ensures that it will implement an effective Security Management System (SeMS) by clearly determining the lines of implementation as well as security duties and responsibilities the employees throughout the organization.

- **Compliance with Regulations**

In all its activities, Pegasus Airlines ensures that security processes are performed in compliance with applicable National and International Civil Aviation regulations and standards and adopts the industry's best practices.

- **Continual Improvement**

For a continual improvement of the Security Management System, all necessary security practices and processes are supported and periodically reviewed by Senior Management. Pegasus Airlines Security Policy is then periodically reviewed at least twice a year during Management Review Meetings and revised if necessary to ensure a continuous relevance to the organization's requirements and applicable national and international regulations and standards.

- **Resources Provision**

In order to ensure a successful implementation of the Security Management System, Pegasus Airlines ensures that Senior Management provides financial, human, material, equipment, training and all other necessary resources.

- **Promotion of a Corporate Security Culture**

Pegasus Airlines ensures that security is a fundamental operational priority and an integral part of the Corporate Commitment. "Corporate Security Culture" is promoted by Aviation Security by increasing the security awareness of employees and service providers with training, bulletins and all necessary arrangements.

- **Threat Assessment and Risk Management**

Pegasus Airlines' objective is to prevent unlawful acts threatening the security of its operations, employees, passengers, facilities and stakeholders. To achieve this goal, it is ensured that operational security threats are identified, evaluated and mitigated by means of close to real-time monitoring via open and restricted sources and a risk-based approach of security activities.

- **Security Training**

Pegasus Airlines ensures and requires that the qualifications and trainings of its employees and sub-contractor employees who perform security functions are in compliance with the requirements of applicable national, international and Pegasus Airlines regulations and standards.

- **Highest Level of Communication**

Pegasus Airlines ensures an objective information sharing and communication between senior management, the employees and its services providers in order to support all activities in a secure framework. Communication shall be executed in a secure and timely manner throughout an effective sharing of security-related information to all relevant parts.

- **Incident Reporting System**

Pegasus Airlines ensures that communication between Senior Management and employees is monitored in a non-punitive approach, and in a way that protects the confidentiality of the reporter. This system is aimed to encourage all employees to report any security-related issue. This is a fundamental part of an effective Security Management System and all employees shall be aware of its importance and participate.

- **Performance Monitoring**

Pegasus Airlines Security objectives are determined by Senior Management. In order to achieve these objectives, security performance standards are set, monitored and actions are taken if necessary.

3.2 CHIEF SAFETY AND SECURITY OFFICE ORGANIZATION CHART

The Chief Safety and Security Office Organization Chart is described as below in the document referenced *PG-IK-BK-002*, available in Comply365.

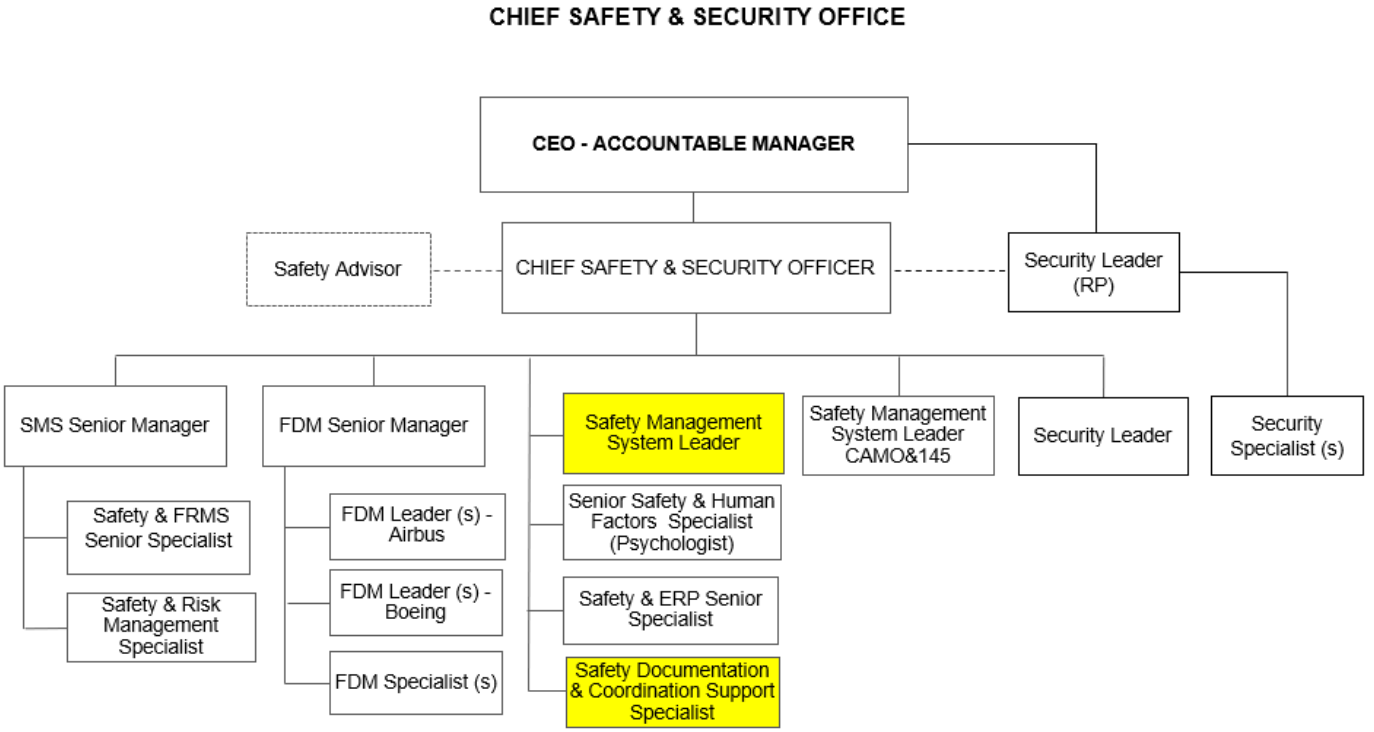


Figure 3-1: Chief Safety and Security Office Organization Chart

3.3 THE ROLES AND RESPONSIBILITIES FOR AVIATION SECURITY IN THE AIRLINE

The roles, requirements and responsibilities for Aviation Security in Pegasus Airlines organization are described in the job description documents (*PG-YN-GT-001 - CEO*, *PG-EK-GT-001 - Chief Safety and Security*

Officer, PG-GU-GT-001 - Aviation Security Leader (RP), PG-GU-GT-002 - Security Leader , PG-GU-GT-003 - Security Specialist , available in Comply365).

3.3.1 Accountable Manager - CEO

3.3.1.1 Role Definition

The Accountable Manager has by virtue of position the corporate authority and responsibility, and thus is accountable for ensuring within all operational areas:

- Irrespective of other functions, establishing, implementing, and maintaining safety, security, compliance monitoring and quality management systems.
- The allocation of resources necessary to manage safety risks and security threats to aircraft operations and their required maintenance activities.

Operations are conducted in accordance with conditions and restrictions of the Air Operator Certificate and in compliance with applicable regulations and standards required by DGCA-TR and other authorities (i.e. foreign authorities, environmental protection etc.).

Lead Pegasus for sustainable profitable growth with a transformational change while ensuring the safety standards for both customers and employees and has the corporate authority for ensuring that all operations and maintenance activities can be financed and carried out to the required standards by the DGCA-TR. Liaison (on behalf of the Company) with regulatory authorities, original equipment manufacturers (OEM) and other operational internal/external entities.

3.3.1.2 Authorities, Accountabilities and Responsibilities

- To be responsible that Pegasus operates in accordance with AOC, Operations Specifications, CAMO, ATO, AMO, AMTO Approvals, Authorizations, Certifications and statutory, regulatory requirements and standards where operations are carried out.
- To be responsible for leading the development and execution of the Company’s long-term strategy with a view to create shareholder value.
- To lead overall organization with strong coordination role.
- To oversee alignment between strategic priorities and resource allocation, and ensure consistent, transparent and well-supported decision-making when considering new or difficult programming and operational opportunities, and expenditures.
- To oversee budget, income statement, balance sheet and cash flow statement.
- To define and execute strategic initiatives; deliver on key elements of business, operation and financial strategy.
- To maintain an effective and transparent dialogue with Board and investors.
- To lead organizational transformation and consolidate leadership team
- To simplify organization and governance structure
- To review and revise compensation and performance management systems
- To prioritize attracting/retaining/investing in top talent and developing people
- To create a high-performance culture at Pegasus
- To manage senior level government and regulative body relations
- To be responsible for presenting the information in the financial information set in timely, wholly and accurate manner.
- To determine the lines of safety and security accountability throughout the organization
- To have direct accountability for safety and/or security throughout the organization

- To have the authority to ensure all necessary financial and human resources are available to meet and maintain the required regulatory and safety standards.
- To encourage the personnel in increasing voluntary and mandatory safety reporting and in writing Hazard reports, promoting safety policy and implementing principles of Just Culture and the nonpunitive policies
- To determine the tolerability of the safety risks in all areas of operations in accordance to the PGEM-EK-001 Chapter 4.10 Organizational Implementation of the Process and accepted standards.
- To manage appropriate company risk profile and ensure compatibility with safety and compliance requirements.
- To be responsible for ensuring appropriate actions are taken to address safety issues and safety risks.
- To be responsible for ensuring the Safety Management System is properly implemented and performed to requirements in all areas of Pegasus Airlines.
- To manage the safety risks and security threats to aircraft operations,
- To have authority for conducting over operations under the certificate, authorization or approval of the organization, including the authority to stop the operation or activity.
- To have accountability for establishing and promoting the safety policy and the non-punitive policy, setting of the acceptable safety risk limits and resourcing of necessary controls, promoting a positive safety culture, seeing the continuous improvement of the SMS.
- To be responsible for the active implementation of the peer support program and the establishment of an organizational structure in line with the standards. CSEO will take active part in the implementation and compliance monitoring on behalf of the CEO for this responsibility.

Related regulations:

- Commission Regulation (EU) 965/12 as amended by Regulation (EU) 2018/1042 covering:
  - AMC1 – AMC2 – AMC 3 – AMC4 CAT.GEN.MPA.215
  - CAT.GEN.MPA.215
  - GM1 CAT.GEN.MPA.215 through GM8 CAT.GEN.MPA.215
- SHT-PSP (Article 11 Requirements Specific to the Accountable Executive)

- To act as the chairman at Safety Review Board Meetings and providing the necessary resources for safety issues.
- To establishing and defining desired Safety and Security Objectives which are consistent with Pegasus safety and security policies and to set Performance Indicators in all areas of operations by supporting Safety, Compliance Monitoring and Security Departments in managing an effective SMS, FRMS, SEMs and meeting the safety, security objectives of the organization as per accepted procedure and standards.
- To ensure that for monitoring and auditing compliance with all applicable regulatory requirements in order to ensure the adequacy and processes of Pegasus Airlines' compliance monitoring activities and safe and efficient operations and training activities as well as the requirements and provisions of all standards adopted by Pegasus Airlines.
- To ensure Company remains compliant with applicable regulatory, company and safety requirements.
- To ensure that all necessary resources which are needed for effective implementation of corrective actions are available and the related actions are taken as necessary.
- To periodically review the compliance monitoring function is effectively established, implemented, and maintained.

- To ensure that all necessary resources which are needed in all areas of operations are available to meet and maintain the required regulatory and standards.
- To ensure personnel who perform functions relevant to the safety or security of aircraft operations are maintained competence based on continued education and training and for the specified positions, continued to satisfy any mandatory technical competency requirements.
- To Act in accordance with role and responsibility for management systems instruction *PG-EY-TL-002*.

3.3.1.3 Job Requirements

The corporate needs defined by the board of directors as well as requirements of the competent authority (TR-DGCA) will be fulfilled as per SHY-6A.

- University Graduate
- Excellent command of English
- Experience in a senior management position
- Integrate the business to deliver results.
- Collaborate and thrive in cross functional working environment.
- Act fact based - action oriented.
- Demonstrate strong communication, persuasion and negotiation skills.

3.3.1.4 Acting

- Chief Operations Officer
- Chief Flight Operations Officer
- Chief Financial Officer
- Chief Commercial Officer

3.3.2 Chief Safety and Security Officer

3.3.2.1 Role Definition

S/he is nominated to implement the Safety Management System (SMS) and Security Management System (SeMS). S/he has the responsibility to monitor compliance with SHT OPS, SHT-UYUMLULUK İZLEME, EC 965/2012 Part ARO/ORO. GEN. 200, Part ARA/ORA, SUBPART ATO, SHY-CA, Part 145/SHT 145, Part CAMO/SHY CA/SHT CAM, Part 147/ SHT 147, IOSA, SHY-SMS, ICAO Doc.9859, ICAO Annex-13, ICAO Annex 19, SHT-FDM, SHY 6A, IMS, NCASP, ECAC Doc. 30, ICAO Annex-17 and Pegasus Airlines Company requirements.

S/he promotes and supervises operational safety as representative for all safety related matters of the Company. S/he is the focal point for the development and maintenance of an effective Safety Management System. S/he is appointed to manage and oversee the day-to-day operation of the SMS operation throughout the Company on behalf of the Accountable Executive and senior management.

S/he is also likely to be the main point of contact with the regulatory authority for safety issues. S/he has the authority and independence and responsible for the performance of the Safety Management System and and Security Management System and for ensuring communication and coordination with appropriate operational managers.

Pegasus Airlines has an independent corporate safety structure, which may provide the flight accident prevention function with direct lines of reporting to senior corporate officials. This type of structure allows an effective and fully integrated system of prevention across all relevant operational disciplines.

The CSSO also has the responsibility to ensure the implementation of an effective Security Management Systems (SeMS) within the scope of National Civil Aviation Security Program (NCASP) and its Annexes,

namely TR-DGCA Training Directive, and SHT-17.3 - Security Management Systems Directive, as well as relevant National and International Aviation Security publications throughout Pegasus Airlines operations.

S/he carries university degree and has Captain License with at least 5 years of operational experience and minimum five years of management experience in commercial aviation industry. S/he has a good command of English and computer literacy, good knowledge of T-DGCA procedures and ICAO, AIR-OPS Regulations. S/he fulfils all requisitions covered in SHY 6A, and requirements of Pegasus AOC.

3.3.2.2 Duties and Responsibilities

- Establishment, development, management, documentation and day to day administration of SMS, FRMS and ERP throughout the organization on behalf of the Accountable Executive and senior management,
- Oversight of SMS, FRMS and ERP ensuring compliance with TR-DGCA and all other applicable regulations, company and customer standards, and airworthy aircraft,
- Promotion and periodic review of safety policy, security policy, fatigue risk management policy and nonpunitive policy to ensure their continued relevance as well as the deployment of the relevant policies throughout the organization,
- Management of continuous improvement by ensuring that corrective actions are taken by the relevant post holders and department heads within Pegasus Airlines,
- Administration of Safety Review Board, Safety Action Group, Fatigue Safety Action Group and Flight Operations Safety Review and FDM Meetings,
- The performance of the flight safety analysis program,
- The dissemination of information to management and non-management operational personnel as appropriate to ensure an organizational awareness of relevant flight safety issues,
- Maintaining open communication and coordination with all the relevant nominated persons, responsible managers / supervisors, department heads, and personnel in the identification, assessment and mitigation of operational risks,
- Maintaining a continued feedback system to the Accountable Executive about progress and adequacy of Safety Management, Fatigue Risk Management and ERP ensuring that deficiencies and non-compliances are identified, root causes are analyzed, risks are assessed and the appropriate corrective/preventive actions are applied,
- Communicating and coordinating with regulatory authorities and other external entities with regards to safety issues on a regular basis ensuring coordination with departments,
- Liaison (on behalf of the Accountable Executive) with Regulatory Authorities, Original Equipment Manufacturers (OEM) and other operational internal/external entities.
- Ensuring safety related trainings are taken by all necessary personnel,
- Ensuring SMS, FRMS and ERP requirements are implemented in the Company and by third parties,
- Taking active part in the implementation and compliance monitoring on behalf of the Accountable Executive which involves establishing an organizational structure which allows for peer support program are following all standards specified in the legislation. CSSO is also an active member of the Oversight Committee.
- Assuring that all personnel are trained to handle organization emergencies based on their role in the organization and to control and observe the emergency management activities,
- Ensuring safety audits of any aspects of the operation are conducted according to Compliance Monitoring Program,
- Administration of Flight Data Monitoring program as team leader, ensuring system security and guaranteeing confidentiality,

- Ensuring safety-related information, including organizational goals and objectives, is made available to all personnel through established communication processes,
- Ensuring the SMS and SeMS effectiveness of the operational activities,
- Providing periodic reports on safety performance,
- To determine the lines of safety and security accountability throughout the organization within his/her respective defined area,
- To have accountability for safety and/or security throughout the organization within his/her respective defined area,
- To be responsible for ensuring implementation and maintenance of the AOSP, and its associated SSPs,
- To encourage the personnel in increasing voluntary and mandatory safety reporting, promoting safety policy and implementing principles of Just Culture and non-punitive policies.
- To determine the tolerability of the safety risks in related area of operations in accordance the *PG-EM-EK- 001 Chapter 4.10 Organizational Implementation of the Process.*
- Facilitating hazard/risk identification and risk analysis and management
- Monitor the implementation of actions taken to mitigate risks, as listed in the safety action plan,
- Ensure initiation and follow up of internal occurrence/accident investigatiions,
- To have the responsibility for ensuring, in his/her respective defined area:
  - To manage the safety risks and security threats,
  - To conduct the operations in accordance with conditions and restrictions of the Air Operator Certificate (AOC), and in compliance with applicable regulations and Pegasus standards,
  - To take into account requirements originating from applicable external sources, including regulatory authorities and original equipment manufacturers,
- To establish and define desired Safety and Security Objectives and to set Performance Indicators in his/her respective area of operations by supporting Safety and Security Departments in managing an effective SMS, SeMS and meeting the safety, security objectives of the organization as per accepted procedure and standards,
- To ensure that all necessary resources which are needed in his/her respective area of operations are approved by Accountable Executive to meet and maintain the required regulations and standards,
- To distribute information to management and non-management operational personnel by using company communication methods (e-mail, bulletin, reports, training, meeting etc.) to ensure an organizational awareness of relevant quality assurance issues and results,
- To ensure that Aviation Security is a core element of the Corporate Commitment and is integrated throughout all company activities,
- To guarantee the timely implementation of required security measures to maintain Aviation Security continuity,
- To ensure the adequacy of security procedures and compliance with these procedures.
- To ensure that a system of investigation, reporting, development, recording, risk analysis and threat assessment for Aviation Security incidents and deficiencies is established, and that necessary preventive/corrective actions are taken.
- Act in accordance with role and responsibility for management systems instruction *PG-EY-TL-002.*

3.3.2.3 Job Requirements

- Undergraduate degree and Captain License with at least 5 years of operational experience
- Minimum five years of management experience in commercial aviation industry,
- Good Command of English,
- Good Computer Literacy,
- Good knowledge of TR-DGCA procedures and ICAO, AIR OPS Regulations
- To fulfil all requisitions covered in SHY 6A, and requirements of Pegasus AOC,

S/he has the below core competencies;

- The promotion of a positive safety culture.
- Interpersonal, influencing and leadership skills.
- Oral and written communication skills.
- Data management, analytical and problem-solving skills.
- Professional integrity.
- Relevant and documented work experience, preferably in a comparable position, in:
  - Management systems including compliance monitoring systems and safety management;
  - Risk management.

Acceptable Training Requirements

- ISO 9001 Quality Management System and internal Auditor Training,
- Safety Management Systems,
- Security Management Systems (SeMS)
- Risk Management,
- Accident Incident Investigation
- Human Factors courses and other formal required trainings must be completed.

3.3.2.4 Acting

- SMS Senior Manager
- FDM Senior Manager
- Safety Management System Leader CAMO&145.

3.3.3 Aviation Security Leader (RP)

3.3.3.1 Role Definition

The Security Leader (RP) is the Responsible Person to implement the security principles and adherence to all security regulations. S/he has the responsibility to monitor compliance with the requirements outlined in the National Civil Aviation Security Program (NCASP) and its Annexes, namely TR-DGCA Relevant Training Directive, and SHT-17.3 - Security Management Systems Directive, as well as relevant National and International Aviation Security publications within Pegasus Airlines operations.

As the Responsible Person for Aviation Security within the company, the Security Leader (RP) is the key element in establishing and maintaining an effective Security Management System (SeMS). S/he oversees daily SeMS procedures, ensuring their proper implementation, and actively promotes operational security.

The Security Leader (RP) is responsible for facilitating coordination and communication with both National and International Aviation Security Authorities and representatives regarding matters of Aviation Security. S/he is following up National and International Aviation Security publications.

The Security Leader (RP) also bears responsibility for ensuring compliance with Integrated Management Systems and Pegasus Airlines' internal security requirements within the Aviation Security Department.

3.3.3.2 Duties and Responsibilities

- To establish and develop Pegasus Airlines Security Policy by including elements ensuring the implementation and the continuity of applicable regulations issued by the NCASP, Turkish DGCA's instructions and directives as well as International Civil Aviation Security Standards defined on ICAO Annex 17 Security, ECAC Doc. 30 Part 2 Security, IATA SeMS and IOSA requirements,
- To ensure that Aviation Security is considered as a core element of the Corporate Commitment and that it is implemented in all activities of the company, and to make sure that the necessary security measures are taken in a timely manner to ensure the continuity of Aviation Security,
- To ensure the preparation, implementation and maintenance of the Air Carrier Security Program (ACSP) and its associated Supplementary Station Procedures (SSPs) in accordance with the requirements of relevant national and international regulations,
- To monitor the adequacy of the procedures and compliance with these procedures, ensure that current regulations (SeMS) are carried out,
- To determine the lines of Safety and Security accountability throughout the organization within his/her respective defined operational area,
- To monitor the performance of Safety, Security and compliance functions and to implement the procedures in accordance with external sources, applicable National and International regulations, original equipment manufacturers, standards of Pegasus Airlines, defined and desired operational safety and security objectives, Pegasus safety and security policies,
- To have accountability for Safety and Aviation Security throughout the organization within his/her respective defined operational area,
- To implement new regulations and applications concerning Aviation Security according to the operator's activities by following all National and International Aviation Security regulations,
- To be responsible for liaison with Civil Aviation Security and Airport Security Authorities,
- To manage Safety risks and Security threats to flight operations,
- To be responsible for Aviation Security matters in the Head Quarter, company representative offices, Approved Maintenance Organisations and ACC3 Stations,
- To distribute security-related information to management and non-management operational personnel by using company communication methods (e-mail, bulletin, reports, training, meeting etc.) to ensure an effective communication throughout the company and all areas where operations are conducted,
- To ensure the preparation of Security Training Program and materials in accordance with TR-DGCA Training Directive, relevant national and international regulations.
- To ensure the preparation of Airport Security Plans in accordance with the NCASP and to ensure their written approval by relevant Local Governors,
- To follow up and ensure the continuity of the approval process of Aviation Security Training Centre and Aviation Security Instructors in the scope of TR-DGCA Training Directive,
- To ensure that Security Audits of internal and external services received for the company are carried out according to Compliance Monitoring Program and that corrective actions are taken, if necessary,

- To ensure that a system of investigation, reporting, development, recording, risk analysis and threat assessment for Aviation Security incidents and deficiencies is established, and that necessary preventive/corrective actions are taken,
- To ensure that the internal audits are carried out within the Compliance Monitoring System, and that necessary corrective actions and/or correction are taken,
- To encourage the personnel in increasing voluntary and mandatory safety reporting and in writing Hazard reports, promoting safety policy and implementing principles of Just Culture and the nonpunitive policies,
- To ensure the review, analysis, follow-up, and record of security reports in the reporting system,
- To establish and define desired Safety and Security Objectives which are consistent with Pegasus Safety and Security policies and to set Performance Indicators in its respective area of operations by supporting Safety and Quality Compliance and Security Departments in managing an effective SMS, SeMS and meeting the safety, security objectives of the organization as per accepted procedure and standards,
- To conduct research and to ensure that all necessary resources which are needed for Aviation Security in order to meet and maintain the required regulations and standards,
- To provide periodic reports on security performance to the Senior Management,
- To determine the tolerability of the safety risks in related area of operations in accordance with *PG-EM-EK-001 Chapter 4.10 - Organizational Implementation* of the process and accepted standards,
- To assist DGCA, IOSA (etc.) Aviation Security Auditors during audit activities, and to report on corrective action(s) regarding any non-conformities arising during these audits, to represent the department in all third-party Security Audits,
- To ensure that findings / deficiencies related to Aviation Security are corrected and corrective or preventive actions within the scope of Security operations are taken, reported and analysed for the necessary measures regarding nonconformities,
- To ensure that all activities are conducted in compliance with Pegasus Airlines Integrated Management System (SMS, ISO9001, ISO14001, ISO18001, ISO27001 etc..), and to ensure that all its stakeholders are working in the same standards,
- To ensure a continuous monitoring and evaluation of Security & Safety performance,
- To act in accordance with *PG-EY-TL-002 - Role and Responsibility for Management Systems Instruction*.

3.3.3.3 Job Requirements

- Being certified as “Accountable Authorized Security Manager” (Form 4) according to Turkish Civil Aviation SHT-17.3 Security Management Systems Directive,
- To be fluent in English, preferably a second foreign language,
- College graduate,
- Knowledge about computer office programs,
- Good communication skills, strong negotiating skills and ability to analyse / synthesize,
- Being team-oriented and responsive,
- Having at least 4 years of experience in Aviation Security operations,
- Having a good knowledge about EU regulations, DGCA legislation, IATA and ICAO, regulations, Integrated Management Systems in aviation operations.

3.3.3.4 Acting

In the absence of the Aviation Security Leader (RP), the Chief Safety and Security Officer will be in charge of all responsibilities, duties and rights for the maintenance of Security.

The details of the delegation process are described in *PG-YO-YN-011 - Delegation Procedure*, available in Comply365.

3.3.4 Responsibilities of Pegasus Airlines Personnel

According to the directive of the Security Management Systems (SeMS), the roles, requirements and responsibilities for aviation security of Senior Management and management personnel with the authority to make decisions that affect operational security and also non-management personnel are defined in the Job Descriptions Documents.

Every employee of Pegasus Airlines regardless of being management or non-management is responsible for implementing airlines security policy, security programmes, procedures and directives, in accordance with their job descriptions.

Pegasus Airlines ensure the management system includes planning processes for operations which:

- Define desired operational safety and security objectives.
- Address operational resource allocation requirements.
- Consider requirements originating from applicable external sources, including regulatory authorities and original equipment manufacturers.

For further details, please refer to *PG-YO-EK-001 – Corporate Manual*, available in Comply365.

3.4 SECURITY COMMUNICATION

Aviation Security Department of Pegasus Airlines uses e-mail & hard copy letters for communication, especially with TR-DGCA and other relevant authorities; info.security@flypgs.com and security@flypgs.com are e-mail groups into which all Aviation Security Department staff is assigned, and where important alerts or information are sent from TR-DGCA and other related authorities.

- Airport security committees are in communication with Pegasus Airlines Aviation Security Department via representative ground handling agents.
- In order to distribute all security information in all relevant areas such as flight crew, cabin crew and operational personnel, Aviation Security Department prepares and issues Security Bulletins via Comply365. Security Bulletins are disseminated by Comply365 as priority to related personnel, and then transferred to EFB if relevant.
- Security Procedures, Risk and Threat Assessment and other security-related publications can also be published by e-mail, EFB or the Comply365 system.
- The communication with subcontractors is provided by e-mail and/or Ground Document Library (document.flypgs.com) which is an online document library for subcontractors.
- Other communication tools such as Smart Ops, EGITA, IQSMS, Pegasus Intranet Website (PIN), Corporate Screen, Pegasus Website (flypgs.com) and Pegasus Academy Online Training Platform may be used internally for security communication.
- Security information intended for passengers is also available in the inflight magazines.
- Periodic executive operations meetings are held to ensure the sharing of operational security information between relevant operational departments.

For further details, please refer to *PG-YO-EK-001 - Corporate Manual*, available in Comply365.

Table 3-1: Pegasus Airlines Postal Address

Name	Pegasus Hava Taşımacılığı A.Ş. – Pegasus Airlines (Aeropark)

Address	Yenişehir Mahallesi Osmanlı Bulvarı No:11/A Kurtköy-Pendik / 34912
City	Istanbul
Country	Türkiye

Table 3-2: Accountable Executive - CEO

General Manager	Güliz ÖZTÜRK
Office Phone	+90 216 560 0000 Ext.7555
Fax	+90 216 560 7070
E-mail	guliz.ozturk@flypgs.com

Table 3-3: Key Corporate Officials

Chief Safety and Security Officer	Murat TÜNAY	**Aviation Security Leader (RP)**	Müge KARAPINAR
Mobile Phone	+90 531 250 20 81	**Mobile Phone**	+90 534 014 54 79
E-mail	murat.tunay@flypgs.com	**E-mail**	muge.karapinar@flypgs.com

3.4.1 Sensitive Aviation Security Information

Sensitive aviation security information will be restricted to those persons who require such information in the performance of their duties and are therefore authorized to have access thereto. This is known as the need-to know principle.

Sensitive aviation security information will be securely stored when not in use to prevent unauthorized access. For example, the use of security cabinets, locked rooms or safes may be considered ways of affording greater protection by the Aviation Security Department Office if considered necessary.

Electronic copies of sensitive aviation security information documents will be equivalently protected in accordance with the Information Security Management Systems.

Operational security sensitive information is distributed to the level of need to know via Comply365 documentation system; the access or printing levels are clearly defined according to each document.

Pegasus Airlines has adopted measures to ensure that authorized persons with access to sensitive aviation security information do not disclose such information to any unauthorized persons. All authorized staff with access to such information sign the “non-disclosure agreement” before being allowed access to such information.

Periodic executive operations meetings are convened to ensure the sharing of operational security information among relevant departments. Additionally, all contact information for department heads within the company is detailed in Chapter 3.4.2 of the corporate manual. Any changes to this information must be updated within 15 days from the date of the change and reported to TR-DGCA and any other relevant authority.

For further details, please refer to PG-YO-EK-001 - Corporate Manual, available in Comply365.

3.4.2 Emergency Contact Numbers

Table 3-4: Emergency Contact Numbers

Name	Title	Mobile Phone	E-mail
Güliz ÖZTÜRK	CEO	+90 216 560 75 55	guliz.ozturk@flypgs.com

Name	Title	Mobile Phone	E-mail
Murat TÜNAY	Chief Safety and Security Officer	+90 531 250 20 81	murat.tunay@flypgs.com
Müge KARAPINAR	Aviation Security Leader (RP)	+90 534 014 54 79	muge.karapinar@flypgs.com
Serkan KILIÇ	IOCC Vice President	+90 533 318 74 20	serkan.kilic@flypgs.com
Semih DEDEBAŞ	OCC Group Manager	+90 216 560 75 26	semih.dedebas@flypgs.com
Ergün DEMİRCİ	Chief Operations Officer	+90 533 137 07 48	ergun.demirci@flypgs.com
Gencer KARATEPE	Chief Flight Operations Officer	+90 533 708 50 62	gencer.karatepe@flypgs.com
Ersel GEYİK	EVP - Cabin Operations	+90 216 560 75 06	ersel.geyik@flypgs.com
Boğaç UĞURLUTEĞİN	EVP - Ground Operations	+90 216 560 75 22	bogac.ugurlutegin@flypgs.com
Mustafa YAVAŞOĞLU	Deputy Vice President - Ground Operations	+90 216 560 75 23	mustafa.yavasoglu@flypgs.com
Tahsin ISTANBULLU	EVP - Technical	+90 533 739 70 84	tahsin.istanbullu@flypgs.com
Barbaros KUBATOĞLU	Chief Financial Officer	+90 216 560 75 66	barbaros.kubatoglu@flypgs.com
Dilara OĞUR	Chief Human Resources Officer	+90 216 560 75 02	dilara.ogur@flypgs.com
Barış FINDIK	Chief Information Technologies Officer	+90 216 560 75 46	baris.findik@flypgs.com
Ali UZUN	General Counsel and Group Head of Sustainability	+90 532 634 56 63	ali.uzun@flypgs.com
Hasan ÖZDEMİR	Cargo Manager	+90 549 744 17 62	hasan.ozdemir@flypgs.com
Güller GÜNGÖRDÜ	Head of - Information Security Risk and Compliance	+90 532 210 19 35	guller.gungordu@flypgs.com
Kemal KUTLU	Security Leader	+90 532 768 62 23	kemal.kutlu@flypgs.com
Ayça CAN	Security Specialist	+90 532 454 72 92	ayca.can@flypgs.com
Muhammed KAYA	Security Specialist	+90 533 394 69 05	muhammed.kaya@flypgs.com
Berkay DEMİRCİ	Security Specialist	+90 534 860 86 74	Berkay.demirci@flypgs.com

Table 3-5: 24/H Contacts

Unit	Integrated Operations Control Centre (IOCC)	Unit	Guest Control Centre (GCC)

Duty Manager	+90 216 560 7264	**Duty Manager**	+90 216 560 7222
Office Phone	+90 216 560 7260/61/62/63	**Office Phone**	+90 216 560 7223
Fax	+90 216 560 7083	**Fax**	+90 216 560 7076
E-mail	ioccdutyleader@flypgs.com	**E-mail**	guestcontrol@flypgs.com

Table 3-6: Cargo Operations Centre

Unit	Cargo Operation Centre
Duty Manager	+90 549 744 64 18 +90 549 742 76 36
Office Phone	+90 216 585 59 83
E-mail	pegasuscargo@flypgs.com

3.5 DESCRIPTION OF AIRLINE'S OPERATIONS

Pegasus Airlines' principal place of business and company offices are registered in Türkiye. As approved by the TR-DGCA, Pegasus Airlines commercially operates:

- Passenger and Cargo International Charter Flights,
- Passenger and Cargo Domestic and International Scheduled Flights

And also, where applicable:

- Wetlease and Codeshare operations

For more details, please refer to PG-KU-KT-00002 - Operation Specifications, available in Comply365.

3.5.1 General Protection

Pegasus Airlines do not control any security sterile area, nor does it perform any screening processes by its own personnel.

3.6 BOARD ORGANIZATION CHART

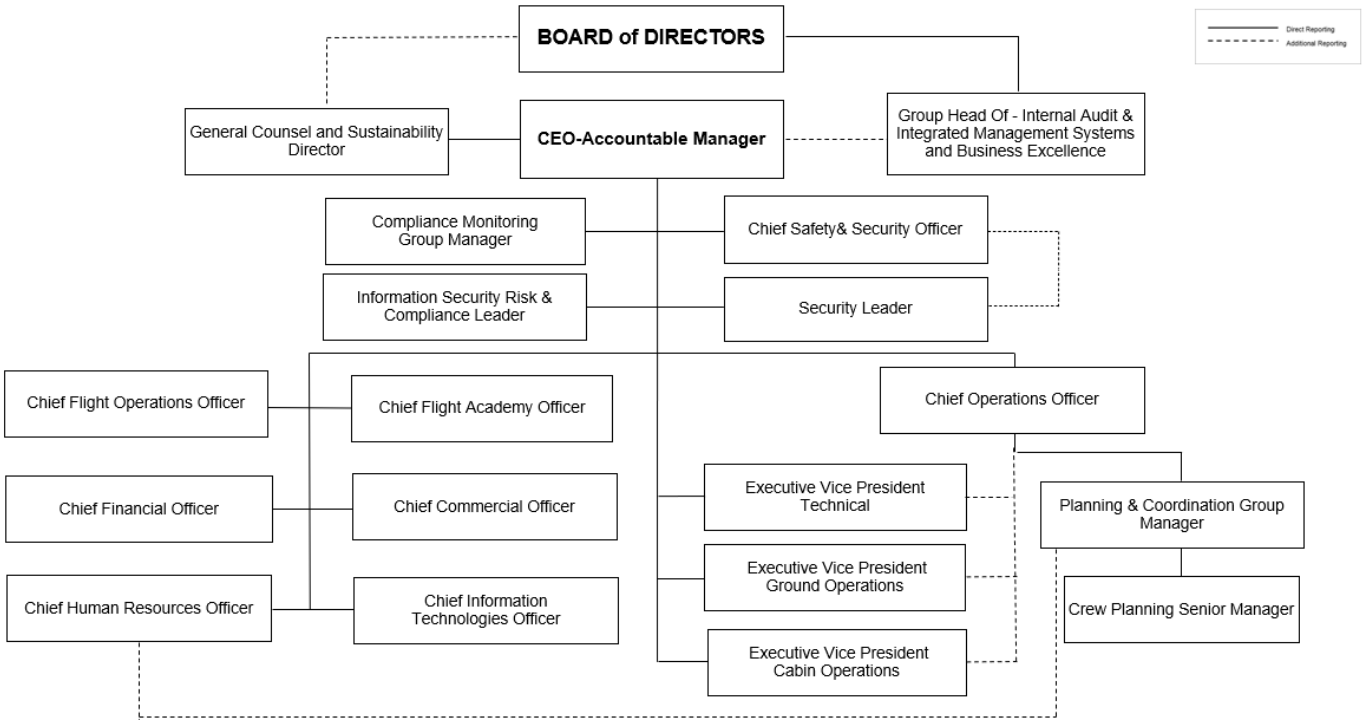


Figure 3-2: PG-IK-BK-001 - Board Organization Chart

For further details, please refer to *PG-YO-EK-001 - Corporate* and *PG-IK-BK-001 - Board Organization Chart*, available in Comply365.

3.7 PEGASUS AIRLINES POLICIES

3.7.1 Corporate Commitment

Refer to *PG-KU-PO-001 - Management Corporate Commitment*, available in Comply365.

In all of its activities Pegasus Airlines is committed to:

A culture that has safety, security and compliance monitoring as fundamental operational priorities, to promote this Pegasus Airlines shall act in full compliance with the current national and international rules and laws regulating the company's field of activity in conjunction with environmental protection and occupational health and safety requirements,

Working towards the continuous improvement of;

- Compliance, safety and security elements in all departments depending on the Company performance.
- Ability to maintain and improve the performance results in all aspects while implementing national and international rules and regulation, Company Procedures and the provisions of relevant statutory and regulatory requirements, any other standards.
- Follow-up of corrective actions and their effectiveness in operational performance.

Ensuring an effective management system is fully implemented and functional with a clear consistency and unity of purpose between corporate management and management of operational areas.

Defining employee accountabilities and responsibilities for delivery of safety, security and customer satisfaction,

Continually striving for improvement in matters related to safety, compliance, security and guest satisfaction, and to internalize the necessity of developing better systems by working to learn from mistakes and reduce human errors,

Encouraging uninhibited reporting of all incidents and occurrences that compromise safety and security to enhance safety and security outcomes and for appropriate human error management,

Ensuring externally supplied systems and services are selected based upon continuous compliance with Aviation Safety, Compliance Monitoring, Security, Information Security and Environment, Health and Safety performance standards to support business activities,

Prohibiting the offering, giving, solicitation or the acceptance of any bribe or corrupt inducement in any form,

Ensuring sufficient skilled and trained resources are available to implement Company strategies and processes,

Maintaining physical infrastructure, including buildings, plant and equipment, in a condition that ensures it is safe to use and consistent with environmental management and minimizes waste and pollution, as far as practical,

Striving to reduce our carbon emissions through technological, infrastructural, operational measures and via application of the emissions reduction principles,

Improving environmental performance continuously and to adopt the attitude of sustainability in order to reduce the impacts of activities on environment, and also to execute studies with the aim of increasing environmental awareness,

Regularly review and measure the performances of the company management systems by analyzing all data coming from audits, inspections, performance-based indicators, the company employee surveys, guest relations feedback system, employee e reporting system,

Assigning accountability and responsibility to all department heads, managers, and employees to strictly adhere to published regulations and orders of safety, security, compliance monitoring, data protection and for all processes to fulfil environmental, occupational health and safety requirements with sensitivity.

3.7.2 Quality Policy

Refer to *PG-KU-PO-002 - Quality Policy*, available in Comply365.

We are committed to continually improve our quality management system in our passenger and cargo air transportation activities by providing secure, safe flight operation and service conditions, increasing guest satisfaction, providing all needed resources and acting in compliance with compulsory aviation laws, regulations, standards and procedures, supporting our strategic and sustainable objectives together with human factors in accordance with purpose and context.

3.7.3 Safety Policy

Refer to *PG-EM-PO-001 - Safety Policy*, available in Comply365.

3.7.4 Environmental Policy

Refer to *PG-EY-PO-006 - Environmental Policy*, available in Comply365.

3.7.5 Occupational Health and Safety Policy

Refer to *PG-EY-PO-007 - Occupational Health and Safety Policy*, available in Comply365.

3.7.6 Information Security Policy

Refer to *PG-EY-PO-008 - Information Security Policy*, available in Comply365.

3.7.7 Periodic Review of Pegasus Airlines Policies

Pegasus Airlines ensures that Safety, Compliance Monitoring / Quality and Security policies are periodically reviewed. This is done through the quality assurance and compliance monitoring programme and management reviews, as necessary, as part of the continuous improvement plan to ensure the suitability, adequacy and effectiveness of the policies and operational controls in place to help meet corporate requirements and applicable national and international civil aviation regulations and standards.

The following policies are part of a periodic review:

- Corporate Commitment
- Safety Policy
- Security Policy
- Fatigue Risk Management System Policy
- Quality Policy
- Environmental Policy
- Occupational Health and Safety Policy
- Information Security Policy

In addition, other company policies and commitments may be reviewed and revised as deemed by the Executive Committee and/or by the Board of Directors at least once a year.

For further details, please refer to *PG-YO-EK-001 - Corporate Manual*, available in Comply365.

End of Section

4 SECURITY OF PASSENGERS AND CABIN BAGGAGE

The screening of all passengers and their cabin baggage is recognized as an essential element of the aviation security measures advocated by ICAO, in order to ensure that unauthorized persons and/or restricted articles do not enter a security restricted area or an aircraft.

All passengers and cabin baggage, including transfer passengers and baggage, shall undergo appropriate security screening before being allowed access to an aircraft, sterile area or security restricted area.

Supernumeraries are always considered as regular passengers. They must go through security screening as well as other passengers, along with their cabin and hold baggage.

Passenger who does not consent to search including cabin and hold baggage shall not be accepted on Pegasus Airlines flights.

4.1 PASSENGER PROFILING

Most of the actions we consider suspicious can be related to the physical and psychological status of the passenger and even cultural sensitivities. Therefore, it is not always easy to analyze passenger behavior and link it to the root cause right away which also requires expertise on the subject.

Despite that, all staff members dealing with passengers in person must be vigilant and observant to the best of their ability.

They should pay attention to passengers who are:

- Sweating,
- Acting nervously
- Having frequent contact with other passengers in distance, Monitoring the crew and the surrounding constantly,
- Avoiding eye contact with the crew,
- Improperly dressed for the destination,
- Asking security sensitive questions,
- Frequently visiting the toilets particularly ones with bags along with them.

This list can be extended to every employee's point of view. It is very critical that these employees report all actions they consider suspicious and request second view or evaluation from their immediate supervisor. No one should be criticized or discouraged for their reports no matter what the root cause turns out to be.

4.2 PURPOSE OF SCREENING AND SEARCHING

Screening and searching of passengers and their baggage is an essential part of aviation security. Pegasus Airlines has a responsibility to make sure that people and baggage boarding the aircraft will not be involved in any act of unlawful interference against civil aviation.

The effective screening of all passengers and their cabin baggage is recognized as an essential element in achieving a safe and secure operation and forms part of the passenger handling procedures contained in the Pegasus Airlines Security Programme.

Pegasus Airlines ensures that all originating, transfer and transit passengers and their cabin baggage shall be screened in order to prevent prohibited articles from being introduced into security restricted areas and on board an aircraft.

4.3 PROCEDURES FOR SCREENING AND HAND-SEARCHING OF ORIGINATING PASSENGERS

Unless otherwise stated, the authority, airport operator, Pegasus Airlines or entity responsible in accordance with the Turkish National Civil Aviation Security Programme or Doc 30, Part III, point 1.2 or ICAO DOC8973 will ensure the implementation of the measures set out in this chapter.

Passengers arriving from a country where the aircraft was in transit after having arrived from a country where the security measures were not recognised equivalent to the standard detailed in Doc 30 or Turkish NCASP, shall be considered as passengers and cabin baggage not screened will be screened to the standard detailed in Doc 30 or NCASP, unless there is a confirmation that these passengers were screened according to this standard in that country.

4.3.1 Standards of Screening and Searching

4.3.1.1 Hand Search of Passengers

When a hand search is performed, it shall be carried out in accordance with the following requirements, so as to reasonably ensure that the passenger is not carrying prohibited articles.

- A hand search shall consist of an examination of the body and clothing by running the hands over the body and clothing in a systematic manner, back and front.
- A hand search shall, where applicable, include a physical examination of:
- headgear; and
- upper body and clothing (back, collar, lapels, shoulders, pockets, arms, tie or scarf, blouse, shirt, sweater or cardigan, including pockets); and
- lower body and clothing (trousers or skirts, inner and outer waistband, belt, pockets, turn-ups, hemlines); and

It shall, where appropriate, include a physical or visual examination of:

- hair; and
- footwear

In addition, unusual or suspicious bulges shall be further examined.

When performing a hand search, special attention shall be paid to the possibility of concealed objects hidden behind collars, waistbands and belts, as well as within footwear.

4.3.1.2 Walk-Through Metal Detection (WTMD) Equipment

4.3.1.2.1 Alarm Resolution

When the WTMD equipment sets of an alarm, the cause of the alarm shall be resolved. This shall be achieved by:

(a) subjecting the passenger to a hand search in accordance with 4.2.1.1; or

(b) either screening the passenger again with the WTMD equipment or the shoe metal detection equipment (SMD) where the alarm is only indicated on the bottom zone of the WTMD equipment that is approved for use with the SMD equipment; or

(c) screening the passenger by a security scanner.

Where the option referred to in point (b) is used, between 10% and 20% of the passengers who caused an alarm shall also be subjected to a hand search, or be screened by a security scanner, EDD or ETD in order to detect prohibited articles. The hand search shall be performed in accordance with 4.2.1.1. Such passengers shall be selected on a continuous random basis.

Where the SMD is used and an alarm cannot be resolved, the footwear shall be removed and subjected to a hand search or screened by the X-ray equipment and the passenger shall be subjected to a hand search of the lower part of the leg.

4.3.1.2.2 Passengers Not Causing WTMD Alarm

Where passengers have passed through the WTMD equipment and did not cause it to alarm, between 10% and 20% of those passengers shall be subjected to screening by either:

(a) a security scanner; or

(b) ETD; or

(c) a hand search; or

(d) EDD.

If option (c) is used, in addition, at least 10% of all passengers shall be screened by the security scanner, ETD or EDD and the percentage of passengers selected for hand search may be reduced to 5%.

Hand searches shall be performed in accordance with 4.2.1.1.

Passengers shall be selected on a continuous random basis.

4.3.1.2.3 Percentages Measurement

The percentages required under points 4.2.1.2.1 and 4.2.1.2.2 shall be measured for each 100 passengers. When less than 100 passengers are expected per hour, another means of ensuring that between 10% and 20% are selected on a continuous random basis shall be chosen.

4.3.1.3 Hand-Held Metal Detection (HHMD) Equipment

Hand-held metal detection (HHMD) equipment may only be used as a supplementary means of screening. It shall not replace the requirements of a hand search.

4.3.1.4 Screening of Passengers by ETD Equipment

The screening by the explosive trace detection (ETD) equipment of passengers shall use samples taken from at least:

(a) the palms and backs of the passenger’s hands or a personal item recently handled by the person (wallet, purse, passport etc.); and

(b) at least one of the following regions on the person's body: the outer waistband of the person or the top of shoes worn.

4.3.1.5 ETD Alarm Resolution

Where an alarm is generated during the screening with the ETD equipment it shall be checked so as to reasonably ensure that the passenger does not constitute a potential threat to civil aviation. The procedure to be followed shall be included in the airport security programme or the relevant document of the entity responsible for screening. The appropriate authority may require prior approval.

4.3.1.6 ETD Equipment in Combination with HHMD Equipment

Explosive trace detection (ETD) equipment in combination with handheld metal detection (HHMD) equipment may only be used in cases where the screener considers a hand search of a given part of the person to be inefficient and/or undesirable.

Where ETD equipment is employed in combination with handheld metal detection (HHMD), for areas where a hand search is not possible or desirable, it shall be:

(a) applied directly to the area; and

(b) applied to the extremities/openings of plaster casts; and

(c) applied to any area which appears to have been tampered with or to raise concern.

4.3.1.7 Security Scanners

When a security scanner with a human reviewer is used for screening of passengers, all of the following minimum conditions shall be complied with:

Security scanners shall not store, retain, copy, print or retrieve images. However, any image generated during the screening can be kept for the time needed for the human reviewer to analyse it and shall be deleted as soon as the passenger is cleared. Any unauthorised access and use of the image is prohibited and shall be prevented;

(a) The human reviewer analysing the image shall be in a separate location so that S/he cannot see the screened passenger;

(b) Any technical devices capable of storing, copying or photographing or otherwise recording images shall not be allowed into the separate location where the image is analysed;

(c) The image shall not be linked to any data concerning the screened person and his/her identity shall be kept anonymous;

(d) A passenger may request that the image of his/her body is analysed by a human reviewer of the gender of his/her choice;

(e) The image shall be blurred or obscured to prevent the identification of the face of the passenger.

Paragraphs a) and d) shall also apply to security scanners with automatic threat detection.

Passengers shall be entitled to opt out from a security scanner. In this case the passenger shall be screened by an alternative screening method including at least a hand search in accordance with point 4.2.1.1.

Before being screened by a security scanner, the passenger shall be informed of the technology used, the conditions associated with its use and the possibility to opt out from a security scanner.

4.3.1.7.1 Alarm Resolution for Security Scanners

When a security scanner sets off an alarm, the cause of the alarm shall be resolved.

This shall be achieved by:

(a) subjecting the passenger to a targeted hand search in the areas of the body for which an alarm is raised; or

(b) re-screening the person with the security scanner; or

(c) subjecting the passenger to a hand search performed in accordance with point 4.2.1.1.

A targeted hand search shall consist of a manual check of those parts of the body where the security scanner alarms. A hand search consists of a manual check of the person's body as detailed in point 4.2.1.1.

4.3.2 Location of Screening or Searching

The basic rule is that all non-exempt passengers and all of their cabin baggage must undergo screening before being permitted to have access to an aircraft or security-restricted area. These procedures will need to be applied to all international flights and to domestic flights which connect with them.

4.3.3 Details of Screening Equipment

Passengers shall be screened by at least one of the following methods:

(a) hand search; or

(b) walk-through metal detection (WTMD) equipment; or

(c) explosive detection dogs; or

(d) explosive trace detection (ETD) equipment; or

(e) security scanners which do not use ionising radiation; or

(f) ETD equipment combined with handheld metal detection (HHMD) equipment.

4.3.4 Details of Operator or Service Provider

In Türkiye, the Ministry of Internal Affairs is responsible for screening of persons and cabin baggage.

Outside Türkiye the recognised authority may perform the screening or security agency personnel contracted by the authority may perform the screening of persons and cabin baggage.. Also depending on the regulations or risk assessment in some airports, Pegasus Airlines can contract to second and/or if necessary to third parties, via a process described under the point 17.2.

4.4 PROCEDURES FOR SCREENING AND HAND-SEARCHING OF TRANSFER PASSENGERS

Passengers arriving from a country where the aircraft was in transit after having arrived from a country where the security measures were not recognised as equivalent to the standard detailed in Doc 30 or Turkish NCASP, shall be considered as passengers and cabin baggage not screened to the standard detailed in Doc 30.

Transfer passengers and their cabin baggage may be exempt from screening if they arrive from a country where the security standards applied are recognised as equivalent to the common basic standards detailed in Doc 30 or if they arrived from a country complying with Turkish NCASP Annex 25.

WARNING	Otherwise, transfer passengers must be subjected to the same implementation as in point 4.2 for the standard of screening, location of screening, details of screening, details of screening equipment, details of service providers.

4.5 LIST OF PERSONS EXEMPT FROM SCREENING AND SEARCHING

4.5.1 Escorted Persons

The appropriate authority may, for objective reasons, allow persons other than passengers to be exempt from screening, or to be subjected to special screening procedures, provided that they are escorted by a person authorised to be an escort.

4.5.2 Screened Persons Temporarily Leaving Critical Parts

Screened persons other than passengers who temporarily leave critical parts may be exempt from screening on their return provided that they have been under constant observation by authorised persons sufficient to reasonably ensure that they do not introduce prohibited articles into those critical parts.

4.5.3 Compliance Authority Officers

The appropriate authority may, on the basis of a local risk assessment, establish a specific accreditation procedure for compliance authority officers, fire brigade staff and licensed security staff required to carry firearms in security restricted areas, to be exempt from screening, or to be subjected to special screening procedures, provided that they are on duty at that airport. Unless they are on covert surveillance duties or responding to an emergency, they shall display a valid identification card.

4.5.4 Other Exemptions from Screening in Case of Emergencies

Persons other than passengers responding to a serious emergency threat to life or property may be exempt from screening.

4.5.5 Exemptions from Screening for National Security Personnel

National Security officers and agents on duty for intelligence units working at that airport, whose identities must remain confidential due to their duties, may be exempt from screening and airport entry card application.

4.6 DENIAL OF BOARDING

Any person who refuses to undergo screening before entering an aircraft must be denied boarding.

Persons who fail to obtain clearance at a screening checkpoint must be referred to law enforcement officials and must be subject to further investigation. All operators at the airport shall be alerted of this development so that the would-be passenger cannot arrange to travel on another flight or with another aircraft operator.

If a passenger refuses to undertake the screening process for himself/herself or for his/her cabin baggage, security staff shall inform their supervisor or authorised police or authority staff. This information must also be reported as soon as possible to Pegasus Airlines' personnel or the contracted ground handling personnel for the offloading process of the passenger and, if available, his/her checked baggage.

4.7 SCREENING AND SEARCHING OF CABIN BAGGAGE

The cabin baggage of all departing passengers shall be screened prior to being allowed into security restricted areas and on board an aircraft.

4.7.1 Screening of Portable Computers and Electrical Items

Before screening, portable computers and other large electrical items shall be removed from the cabin baggage and shall be screened separately, unless the cabin baggage is to be screened with Explosive Detection Systems (EDS) equipment meeting standard C2 or higher.

4.7.2 Screening of LAGs

The appropriate entity or the Pegasus Airlines contracted service supplier at all airports shall screen, upon entry to the security restricted area (SRA), LAGs obtained at an airport or on board an aircraft that are sealed in a STEB, inside which is displayed satisfactory proof of purchase on the airside at an airport or on board an aircraft. Screening shall also cover LAGs to be used during the trip for medical purposes or as a special dietary requirement, including baby food.

Before screening, LAGs shall be removed from the cabin baggage and shall be screened separately, unless the equipment used for the screening of cabin baggage is also capable of screening multiple closed LAG containers inside the baggage.

Where LAGs have been removed from the cabin baggage, the passenger shall present: a. all LAGs in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent resealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed; and b. all other LAGs, including STEBs containing LAGs.

Appropriate authorities and airports shall provide information to passengers in respect of the screening of LAGs at their airports. Information for passengers is available on the check-in desks and on the website of Pegasus Airlines. (www.flypgs.com and https://cdnp.flypgs.com/files/pdf/sivi_brosur_shgm_ENTR.pdf)

4.7.2.1 Special Categories of Cabin Baggage

The appropriate authority may create categories of cabin baggage that, for objective reasons, shall be subject to special screening procedures or may be exempt from screening.

4.7.3 Standards of Screening and Searching

4.7.3.1 Hand Search of Cabin Baggage

Where x-ray or EDS equipment is used, each image shall be viewed by the screener or analysed by auto clear software (ACS).

4.7.3.2 Use of X-Ray or EDS Equipment

4.7.3.2.1 Image Viewing

Where x-ray or EDS equipment is used, each image shall be viewed by the screener or analysed by auto clear software (ACS).

4.7.3.2.2 Alarm Resolution

Where x-ray or EDS equipment is used, all alarms shall be resolved to the satisfaction of the screener so as to reasonably ensure that no prohibited articles are carried into the Security restricted area or on board an aircraft.

Where EDS equipment is used, and the identity of an article is unclear, the baggage shall be screened again by one or more of the following methods:

(a) hand search;

(b) x-ray equipment, whereby the same screener examines the baggage from a different angle than that used during the original screening;

(c) explosive detection dogs (EDD);

(d) ETD equipment.

Where ETD equipment or EDD are employed either the whole bag shall be screened or, if it can be clearly identified, only the item(s) causing the alarm may be screened.

Where an EDS alarm occurs on a liquid, aerosol or gel, the alarm resolution steps laid out in point 4.5.3.7.4. shall be followed.

The procedure to be followed for the resolution of EDS alarms shall be included in the airport security programme or the relevant document of the entity responsible for screening. The appropriate authority may require prior approval.

4.7.3.2.3 Dense Items

Where x-ray or EDS equipment is used, any item, whose density impairs the ability of the screener to analyse the contents of the cabin baggage, shall be taken out of the baggage. The bag shall be screened again, and the item shall be screened separately as cabin baggage.

4.7.3.2.4 Large Electronical Items

Any bag that is found to contain a large electrical item shall be screened again with the item no longer in the bag and the electrical item screened separately, unless the cabin baggage was screened with EDS equipment meeting standard C2 or higher.

4.7.3.2.5 Continuous Reviewing of Images

Persons screening cabin baggage by x-ray or EDS equipment shall normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener shall not review images for at least 10 minutes. This requirement shall only apply when there is an uninterrupted flow of images to be reviewed.

There shall be a supervisor responsible for screeners of cabin baggage in order to assure optimum team composition, quality of work, training, support and appraisal.

4.7.3.3 Screening Of Cabin Baggage By ETD Requiring Particulate Sampling

The screening by ETD equipment which requires particulate sampling of cabin bags shall use samples taken from at least the following:

(a) parts of the outside of the baggage that are frequently handled, such as zips, handles and clasps of the baggage;

(b) the inside of the baggage including, where applicable, the inner lining of the baggage or the outside of any large items contained within the baggage.

4.7.3.4 Screening Of Cabin Baggage By ETD Requiring Vapour Sampling

The screening by ETD equipment which requires vapour sampling of cabin bags shall use samples taken from at least the inside of the baggage.

4.7.3.5 ETD Alarm Resolution

Where an alarm is generated during the screening with ETD equipment it shall be investigated so as to reasonably ensure that the cabin baggage does not constitute a potential threat to civil aviation. The procedure to be followed shall be included in the airport security programme or the relevant document of the entity responsible for screening. The appropriate authority may require prior approval.

4.7.3.6 Threat Image Protection

4.7.3.6.1 Screening Requirements Related to the Use of TIP

Where x-ray equipment is used, at least one of the following measures shall also be implemented:

(a) at least 10% of the cabin baggage or the cabin baggage carried by at least 10% of the passengers, selected on a continuous and random basis, shall be screened with ETD or EDD; this percentage may be reduced to 5% where threat image projection (TIP) software is installed and employed; or

(b) at least 15% of the cabin baggage or the cabin baggage carried by at least 15% of passengers, selected on a continuous and random basis, shall be subjected to a hand search, whereby all electronic equipment larger than a pocket-sized mobile phone shall be removed from any protective cover or case and carefully examined for signs of alteration or tampering; this percentage may be reduced to 5% where TIP software is installed and employed; or

(c) based on a risk assessment approved by the appropriate authority, at least 50% of the cabin baggage, selected on a continuous and random basis, shall be screened by EDS.

4.7.3.7 Screening of Liquids, Aerosols and Gels (LAGs)

4.7.3.7.1 Application

These shall only be screened at airport security control points involving LAGs that are:

(a) sealed in a STEB as described in point 4.5.3.7.3,

(b) required for medical purposes carried in a quantity proportional to the travel time to be used during the journey,

(c) for special dietary requirement, including baby food in a quantity proportional to the travel time,

(d) transported in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent resealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably and the bag is completely closed.

Liquids, aerosols and gels (LAGs) other than those listed above shall not be permitted to be carried as cabin baggage and taken into security restricted areas. Liquids, aerosols and gels shall be permitted to be taken into security restricted areas and on board an aircraft provided they are screened or exempt from screening in accordance with the provisions of this chapter.

LAGs shall be screened as cabin baggage. In addition, screening by LEDS equipment shall only apply to:

(a) LAGs carried by at least 50% of the passengers carrying LAGs, selected on a continuous random basis, who have presented such LAGs separately from other items of cabin baggage.

(b) LAGs carried by all passengers who did not present such LAGs separately from other items of cabin baggage.

4.7.3.7.2 Exemptions From Screening

LAGs carried by passengers may be exempt from screening with LEDS equipment upon entry to the Security Restricted Area in the following cases:

(a) if the LAG is in individual containers with a capacity not greater than 100 millilitres or equivalent in one transparent resealable plastic bag of a capacity not exceeding 1 litre, whereby the contents of the plastic bag fit comfortably, and the bag is completely closed; or

(b) liquids used in the health sector and body fluids that need to be carried for analysis. If there is an inconvenience in transporting in the aircraft hold and in scanning on the X-Ray device, they can be transported in the cabin after the records of this exemption are kept, with the documents of the relevant institution or organization.

Airport personnel on duty may be exempt from liquids restrictions provided that they carry with them liquids suitable to their needs.

LAGS carried into the security restricted area or on board an aircraft by persons other than passengers may be exempt from screening with the decision of the relevant authority.

4.7.3.7.3 Dedicated STEBs

The dedicated STEBs referred to under point (b) of point 4.5.3.7.2. shall:

(a) be clearly identifiable as a STEB of that airport; and

(b) display inside proof of purchase or resealing at that airport within the preceding period of three hours; and

(c) originate from a supplier that submits a declaration to the airport operator confirming that the STEB is made available exclusively for use airside at that airport.

4.7.3.7.4 Alarm Resolution

Where an alarm is generated during the screening of LAGs with LEDS equipment, the following steps shall be taken:

(a) if the screener identified that during the initial screening with LEDS equipment the concept of operations for that equipment was not fully adhered to, the LAG may be re-screened once with the same LEDS equipment;

(b) if the screening point is equipped with LEDS equipment that offers a different principle of operation from the initial screening, the LAG may be re-screened once with such equipment using that different principle of operation;

(c) if the screening point is equipped with LEDS equipment meeting standard 3 that offers a different principle of operation from the initial screening and the re-screening in point (b), the LAG may be re-screened once with such equipment using that different principle of operation;

(d) if the alarm cannot be resolved in accordance with points (a) to (c), the passenger shall be offered screening of the LAG with LEDS equipment dedicated to be used on open LAG containers, subject to the applicable health and safety legislation at the airport concerned. This procedure shall not be permitted where point (c) is applied;

(e) if the alarm cannot be resolved in accordance with points (a) to (d), security personnel shall search the passenger and cabin baggage and interview the passenger. This procedure shall reasonably determine whether the passenger and cabin baggage, including the LAG, constitute a potential threat to civil aviation. The procedure to be followed and the qualification requirements for the security personnel involved shall be included in the airport security programme or the relevant document of the entity responsible for screening. The appropriate authority may require prior approval.

Where the process described in this point cannot resolve the alarm, the LAG shall be rejected.

4.7.4 Location of Screening and Searching

The basic rule is that all non-exempt passengers and all of their cabin baggage must undergo screening before being permitted to have access to an aircraft or security-restricted area.

These procedures will need to be applied to all international flights and to domestic flights which connect with them.

4.7.5 Details of Screening Equipment

Cabin baggage shall be screened by at least one of the following methods:

(a) a hand search; or

(b) x-ray equipment; or

(c) explosive detection systems (EDS) equipment; or

(d) explosive detection dogs in combination with point a); or

(e) ETD equipment.

Where the screener cannot determine whether or not the cabin baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

4.7.5.1 Supplementary Means of Screening

Explosive detection dogs and explosive trace detection (ETD) equipment may only be used as a supplementary means of screening.

4.7.6 Details of Operator or Service Provider

In Türkiye, the Ministry of Internal Affairs is responsible for screening of persons, checked baggage and cabin baggage.

Outside Türkiye an authority may perform the screening or security agency personnel contracted by the authority Also, depending on the regulations or risk assessment in some airports, Pegasus Airlines can contract to second and/or if necessary to third parties, via a process described under the point 17.2.

4.8 TREATMENT OF SUSPECT PASSENGERS OR CABIN BAGGAGE

If the cause of the alarm cannot be resolved using the screening methods, security personnel shall search the passenger and cabin baggage and interview the passenger. This procedure shall reasonably determine whether the passenger and cabin baggage constitute a potential threat to civil aviation. The procedure to be followed and the qualification requirements for the security personnel involved shall be included in the airport security programme or the relevant document of the entity responsible for screening. The appropriate authority may require prior approval.

4.9 CONTROL OF MOVEMENT OF PASSENGERS

Passengers and their cabin baggage shall be protected from unauthorised interference from the point at which they are screened until departure of the aircraft on which they are carried.

4.9.1 Separation of Passengers

4.9.1.1 Application

Screened departing passengers shall not mix with arriving passengers, unless they have been previously screened to the standard detailed in this ACSP as per Doc 30 or Turkish NCASP.

4.9.1.2 Procedures in Case of Mixing

In the event of detected or suspected mixing of screened departing passengers and unscreened persons, the following action shall be taken:

(a) those parts where mixing was detected or suspected shall be cleared and then a search shall be carried out to reasonably ensure that no prohibited articles have been introduced to those parts; and

(b) departing passengers and their cabin baggage present in areas where mixing was detected or suspected shall be screened again.

4.9.1.3 Exemptions

Point 4.7.1.2. shall not apply to screened departing passengers mixing with:

(a) crew members departing on the same aircraft; or

(b) transit passengers departing on the same aircraft; and/or

(c) other persons formally exempt from screening by the appropriate authority of the Member State, as detailed in the National Civil Aviation Security Programme.

Point 4.7.1.2. shall not apply if mixing took place due to factors beyond the passengers' control.

4.9.1.4 Aircraft Subject to Security Search

Point 4.7.1.2. shall be considered to be met for an aircraft that is subjected to an aircraft security search.

4.9.1.5 Details of Operator or Service Provider

Inside Türkiye, the Ministry of Internal Affairs and contracted passenger handling companies of Pegasus Airlines are responsible for ensuring :

- separation of screened and unscreened passengers and their cabin baggage.
- protection of the screened hold baggage from unauthorized access until loaded on the aircraft.

Outside Türkiye where an authority performs the implementation of security control or security agency personnel are contracted by the authority, or contracted passenger handling companies of Pegasus Airlines involved, they must ensure :

- The separation of screened and unscreened passengers and their cabin baggage.
- The protection of the screened hold baggage from unauthorized access until loaded on the aircraft.

4.10 MEASURES FOR SPECIAL CATEGORY PASSENGERS

The appropriate authority may create categories of passengers that, for objective reasons, shall be subject to special screening procedures or may be exempt from screening.

4.10.1 Diplomats and Other Privileged Persons

Subject to the provisions of the Vienna Convention on Diplomatic Relations, diplomats and other privileged persons shall be liable to screening for security purposes.

In principle, only the following persons may be exempt from normal security screening in ECAC Member States:

(a) Heads of State;

(b) Official guests invited by the Government.

4.10.2 Government Couriers and Diplomatic Bags

The appropriate authority may allow a diplomatic bag and government couriers to be exempt from screening or to be subjected to special security procedures provided that the requirements of the Vienna Convention on Diplomatic Relations are met.

Pegasus Airlines or contracted ground handling staff responsible for receiving diplomatic bags shall make sure that they have, in fact, been sent by duly appointed officials of the missions concerned. Diplomatic couriers and their personal baggage are not exempt from screening.

4.10.3 Passengers With Reduced Mobility and Medical Cases

Private screening shall not be routinely provided. However, passengers carrying high-value material, passengers with pacemakers and passengers with reduced mobility may be manually screened in an area out of view of other passengers.

4.10.3.1 Passengers With Reduced Mobility

Persons on crutches, in wheelchairs or on stretchers, or wearing prosthetic aids, etc., may be privately screened. With reason and discretion, the person conducting the screening or consent search using either a handheld metal detection device or a physical search or a combination of both, shall ensure that no weapons or dangerous objects are on or about the person being screened. The person may then be escorted through or around the screening point. Hand-carried items shall be screened in the normal manner.

4.10.3.2 Passengers With Medical Cases

Specific guidelines shall be produced, and training given to personnel, for procedures to be followed for persons with special needs.

As a minimum, this shall include instructions on what actions to take for the following classes of person:

- babies in pushchairs and children (will require consent of adult);
- pregnant women;
- disabled persons;
- passengers in wheelchairs;
- persons with medical conditions [limbs in plaster];
- passengers with religious reasons that prevent a hand search of them or their baggage;
- transsexuals;
- blind passengers and guide dogs;
- other special local criteria.

4.10.4 Inadmissible Passengers/Deportees/Escorted Prisoners

Specific security measures shall be introduced for the air transport of the following groups of potentially disruptive passengers:

Table 4-1: Potentially Disruptive Passengers Terms and Codes

Deportees	Persons who had legally been admitted to a Member State by its authorities or who had entered a Member State illegally, and who at some later time is formally ordered by the Authorities to leave that Member State.
DEPO	Industry-approved code for a deportee.
DEPA	Industry-approved code for a deportee accompanied by an authorized escort.
DEPU	Industry-approved code for a deportee not accompanied by an authorized escort.
Deporting State	The State that has arranged for a deportee's removal from its territory.
Escort	A person authorized by the deporting State who has been trained to accompany deportees on removal flights.
Inadmissible persons (INAD)	Persons whose entry to a Member State is refused by the competent authorities because he or she lacks the required visa, has an expired passport, etc. and who are being transported back to their country of departure, or to any other country where the persons are admissible.
Persons in Lawful Custody	Persons either under arrest or convicted by a court of law who have to be transported to another State for legal reasons.

Refugees	To attain refugee status, it must be established that the applicant has a well-founded fear of persecution in their home country.
Political Asylum	Under International law, it is defined as refuge afforded to a person whose extradition is sought by a foreign government.
Economic Migrants	People who are seeking to improve their lifestyle and are only trying to gain entry to another State for personal financial gain or profit.

Passengers who are refused entry to a State can be called upon to return to the port of embarkation. This removal is accompanied by a judicial order of removal.

All such persons shall be subjected to strict security controls. Although a person is involved in travel in response to a judicial or custodial order, while in flight S/he is under the control of the Pilot in Command of the aircraft.

Those responsible within the airline for the compliance with the judicial orders (airport managers) will inform the Pilot in Command and his crew at point of embarkation. Transit and destination airports will also need to be advised that such a person is being carried via SITA message or e-mail.

4.10.4.1 Carriage

Pegasus Airlines that have transported people who have been refused entry to a state can be called upon to return such person(s) to the port of embarkation. Such removal is accompanied by a judicial order of removal.

All such persons shall be subjected to strict security controls. Although a person is involved in travel in response to a judicial or custodial order, while in flight S/he is under the control of the Pilot in Command of the aircraft.

4.10.4.2 Notification to an Air Carrier by the Competent Authority

Prior notification (minimum of 24 hours) shall be given to the air carrier using PG-GU-FR-011 - Potentially Disruptive Passengers Information Form (available in Comply365) in English language.

This form must be filled by the Passenger Service Agents for INADs, Deportees, Denied Boarding (Travel Document Reasons) and Escorted Persons in Lawful Custody. By the approval of the Pilot-in-Command, one copy of this form with the other documents shall be handed over to the Senior Cabin Crew.

Verification of acceptance of the inadmissible passenger, deportee or person in lawful custody at transit points and final destination must be made by the authorities and handling companies before the removal takes place.

4.10.4.3 Content of the Written Notification

The notification shall contain the following details:

(a) identity and gender of the person; and

(b) reason for transportation; and

(c) name and title of escorts, if provided; and

(d) risk assessment by the competent authority, including reasons to escort or not; and

(e) prior seating arrangement, if required; and

(f) the nature of the available travel documents.

4.10.4.4 Availability of Information to the Pilot In Command

The contracted passenger handling service responsible personnel shall fill in the “Potentially Disruptive Passengers Information Form” and hand it over to the Senior Cabin Crew.

This information shall be available for the Pilot-in-Command and passengers are permitted to board the aircraft only after obtaining his/her approval.

4.10.4.5 Supplementary Safeguards for Potentially Disruptive Passengers

The following supplementary safeguards for potentially disruptive passengers shall be observed:

- stringent screening of them and their cabin and hold baggage;
- boarding prior to all other passengers, subject to coordination with the airline or Pilot in Command;
- no occupancy of aisle seats or seats next to emergency exits;
- no access to alcohol;
- sufficient number of escorts, if deemed necessary in the risk assessment;
- escorts shall be able to converse with the aircraft crew;
- no public disclosure of the flight schedule for transporting potentially disruptive passengers; and
- restraining devices shall be provided, if deemed necessary in the risk assessment.

4.10.4.6 Risk Assessment of Potentially Disruptive Passengers

A risk assessment must be carried out by the authorities/handling companies for each passenger intended for removal. The result shall be notified to Pegasus Airlines Aviation Security Department via e-mail and to the aircraft Pilot-in-Command. The assessment shall take account of the passenger's history, previous and current behaviour, media and/or activist activity and any other relevant factor which may indicate a security risk.

Based on the risk assessment, the authorities shall recommend whether or not an escort is needed. Persons in lawful custody must always be escorted.

If the assessment indicates a high level of risk, arrangements other than commercial aircraft shall be made.

The Potentially Disruptive Passengers Information Form (PG-GU-FR-011, available in Comply365) shall be attached to the Crew Information Sheet to determine whether an uplift of a passenger is to be refused or if an escort is necessary.

Females traveling under the provisions of a judicial order may require a female escorting officer as a member of the escort team.

Other important information includes the following:

(1) Name and sex of the person identified as the deportee,

(2) Reason for deportation (nature of crime),

(3) Willingness or unwillingness to travel by air,

(4) Whether the person has attempted to escape custody,

(5) Whether the person has any history of violence,

(6) Whether the person has a history of self-harm,

(7) Whether members of the person's family are booked on the same flight,

(8) Whether the person is likely to be target of harm during the transportation,

(9) Identity of escorts (if required),

(10) The mental/physical state of the person,

(11) Is S/he on a wanted list by any other Authority?,

(12) Is there any other information that would allow the risk of endangering the security of the flight?,

(13) Special conditions and precautions for transport of the person, if any.

4.10.4.7 Control of Numbers

According to Pegasus Airlines Security and Safety policies and conducted risk assessments, the acceptance limits of Potentially Disruptive Passengers are as below.

Table 4-2: Control of Numbers of Potentially Disruptive Passengers

	Maximum Number	Escorted
Pegasus Airlines Own INAD	Maximum 21 INAD	According to INAD's Behaviour
Other Airlines' INAD	**Not Accepted**	**Not Accepted**
DEPA **(Deportee Accompanied)**	Maximum 4 DEPA (*Aviation Security Department pre-approval is required)	Min. 2 Escorts per DEPA
DEPU **(Deportee Unaccompanied)**	**Not Accepted**	**Not Accepted**
Person in Lawful Custody	Maximum 4 Persons	Min. 2 Escorts per Person

4.10.4.8 Escorts

Where an escort is needed, the authorities shall ensure that there is a minimum of 2 escorts. Additional escorts should be provided according to the risk assessment.

- The escorts must be provided until the final destination.
- Pegasus Airlines does not accept armed escorts on their flights.
- Escorts provided for deportees should include a law enforcement officer. If persons other than law enforcement officers act as deportee escorts, these persons should:
  - have the appropriate legal authority for the task;
  - carry proper identification;
  - have received appropriate training;
  - possess the necessary physical and mental attributes for the task.
- No alcohol will be served to escorts during their duties

4.10.4.9 Carriage With Escorts

The necessity of an escort should be considered in all cases where the individual:

- is deemed a safety risk because of past or present conduct;
- is in a mental state which requires special attention;
- is in a physical condition which could be objectionable to or cause discomfort to other passengers;
- has committed a crime, or is wanted by the police in any state;
- has some form of addiction.

If the authorities and the carrier differ on the necessity of an escort, the carrier may require from the authorities a discharge of responsibility for any damage as a consequence of the lack of an escort. A carrier retains the right to refuse carriage if it believes that the safety of the aircraft, crew or passengers is deemed to be at risk as the result of carriage of such persons.

4.10.4.10 Nature of Escorts

Depending on the reasons for providing the escort, it may be necessary for the escort to have medical or other specialist qualifications. In some cases, it may be advantageous for the airline to provide the escort. There shall be no public disclosure of the itinerary of the escorted individual.

4.10.4.11 Escort Procedures

The escort shall:

- be in plain clothes;
- not be in possession of firearms or weapons;
- carry and be trained in the use of appropriate restraint devices (to be concealed to the public);
- ensure that the individual and baggage is subjected to thorough pre-embarkation security screening;
- keep the Pilot-in-Command of the aircraft fully informed of any incident during the flight;
- ensuring that no alcohol is served to the inadmissible passenger or deportee;
- be in possession of the escorted persons personal property including passport, travel documents and ticket;
- be in possession of the deportation/removal order, which shall be given to the authorities at the destination airport;
- supervise the taking of medication;
- not permit the deportee to disembark at transit stops;
- ensure that the person under escort is never left alone, including when in the lavatory.

Under no circumstances shall a female deportee be escorted on a flight without a female being part of the escort team.

4.10.4.12 Persons in Custody

Pegasus Airlines provides guidance material, as below for persons in lawful custody, persons under arrest, or convicted criminals under escort:

- a prisoner shall not be transported on board an aircraft unless escorted by a minimum of two policing authority officers;
- policing authority officers or other authorized persons shall notify a responsible representative of the airline well before the date it is proposed to transport a prisoner, or as soon as practicable in an emergency, of the identity of the person being escorted, the flight on which the transportation has been arranged, and whether or not the escorted person is considered dangerous;
- Pegasus Airlines does not accept prisoners and escort(s) as passengers unless an agreement has been obtained in advance from the States that may be involved en route and at the intended final destination. In such cases sufficient advance notification must be given to the airline so that prior agreements can be obtained;
- escorting officers shall be informed by a responsible representative of the airline of the potential danger to the safe operation of the aircraft shall they take any action during an act of unlawful interference without direction from the Pilot in Command;
- escorting officers shall ensure that a prisoner does not carry contraband, weapons, matches or other potentially dangerous items;
- escorts shall be equipped with adequate restraining devices to be used in the event that they determine that restraint is necessary. Under normal circumstances a prisoner shall not be shackled to any part of the aircraft, including seats, tables, etc.;

- escorts shall not carry mace, tear-gas or similar incapacitating gas-generating devices on board an aircraft;
- escorts shall adequately identify themselves to security personnel, policing authority officers on duty, and flight attendants, requesting that their presence on board and seat assignment be transmitted to the Pilot in Command, who shall acknowledge receipt of this information;
- any other security personnel and passengers authorized to carry firearms on board the aircraft shall be made aware of the transportation of prisoners and escorts and their location;
- escorted persons shall be boarded before all other passengers and disembarked after all other passengers have left the aircraft;
- they shall be seated as far to the rear of the passenger cabin as is possible but not in a lounge area, next to or directly across from an exit;
- they shall only be seated in a row of two or more seats and at least one escort shall sit between the escorted person and any aisle;
- they shall be accompanied always and kept under surveillance, including visits to the lavatory; • no intoxicating beverage shall be served to escorts or prisoners while on board the aircraft;
- prisoners may be served food at the discretion of the escorts but shall not be provided with metal utensils or a knife;
- Pegasus Airlines refuse to accept a prisoner if, in the judgment of a responsible representative of the airline, such acceptance may jeopardize the safety of the other passengers.

4.10.4.13 Carriage Without Escorts

When it is decided that there is no requirement for an escort, the following security procedures shall be applied:

- full security check of the individual and his/her baggage prior to embarkation;
- no public disclosure of the itinerary, especially where there is political significance;
- travel formalities for transit, transfer and entry at destination to be properly completed;
- any special requirements, permits, or authorities at transit, transfer and destination stations must be made available;
- notify the Pilot-in-Command of seat number;
- notify cabin crew members to refrain from serving alcohol to that specific passenger.

4.10.4.14 Acceptance Procedure

Seats must be allocated to the inadmissible deportee or person in lawful custody and any escorts at the rear of the aircraft, away from doors and away from wing exits.

Arrangements shall be made to board either before or after the other passengers, depending on whether or not the aircraft is on a jet way.

The authorities shall ensure that the inadmissible passenger, deportee or person in lawful custody and his/her cabin and hold baggage is thoroughly searched.

The hold luggage is to be loaded last in order to avoid delaying the aircraft's departure in the event that the passenger does not travel.

4.10.4.15 Documents

Documents of inadmissible passengers must be placed in the care of the crew.

4.10.4.16 Denial of Carriage and Pilot In Command's Authority

According to ECAC Document 30 Annex IV-4-B;

At the point of boarding, the Pilot-in-Command, in accordance with domestic law and international conventions, shall assume full authority in respect of such passengers. That authority may extend to refusing to accept an escorted person in lawful custody or an escorted or unescorted inadmissible passenger or deportee for transportation when S/he considers that action to be in the best interest of flight safety. Such refusal shall be based on objective reasons related to the passenger and his/her action or behavior being exhibited at the time of boarding or at a subsequent time.

Pegasus Airlines provides reasons in writing for any instance in which transportation is denied, including what additional requirements shall be met to enable transportation to occur, when requested by the authorities.

4.10.4.17 Use of Restraints

The use of restraining devices by the escort must be limited to actual need and must conform to the laws of the State and the applicable operating carrier's policy.

Escorts shall be trained in the safe use of, and, subject to government regulation and the operating carrier's policy, shall have access to appropriate restraining devices when accompanying an inadmissible passenger, a deportee or a person in lawful custody.

Sedatives or other drugs may be administered only when their use complies with applicable legislation and the operating carrier's policy.

States that administer sedatives or other drugs to inadmissible passengers, deportees or persons in lawful custody must ensure that a medical attendant is provided en route to the final destination, or that a suitably trained escort is provided to administer the medication during travel.

4.11 POLICY FOR UNRULY PASSENGERS

The term unruly or disruptive refers to passengers who fail to respect the rules of conduct on board the aircraft or to follow the instructions of the crew members, thereby disturbing good order and discipline on board and compromising safety.

In the interest of safety and security any potentially disruptive passenger must be denied boarding. It is an offence under National and International law for a passenger to be under the influence of drugs or alcohol on board an aircraft. It is appreciated that it is sometimes difficult to ascertain if a passenger may be under the influence of drugs or alcohol or merely in high spirits. If there is any doubt you must bring the matter to the attention of the Station Manager or his/her Deputy, to obtain authorization for carriage.

- To prevent unacceptable passengers from boarding the aircraft.
- To ensure unacceptable passengers are off-loaded before taxi or take-off.
- To land en-route, if the situation in the Pilot-in-Command's judgment is justified, to offload unacceptable passengers.
- To ensure unacceptable passengers are reported to the appropriate authorities at the destination.
- To ensure that protection is obtained on the return flight including refusal of carriage, where appropriate.
- To encourage prosecution by the appropriate authority, when applicable.

In order to preserve the legal position under which we will prosecute or defend, it is desirable to confirm the reasons in writing on a standard "Passenger Irregularity Report Form".

Pegasus Airlines will refuse carriage or cancel the reservation of any passenger when, in using reasonable discretion, it is decided:

- ground incidents preventing the boarding of potentially unruly passengers (check-in, lounge, gate);
- incidents occur during taxiing;
- in-flight incidents;

- Incidents at arrival.

POLICY REGARDING ALCOHOL

Drunk passengers are a danger to themselves and others when on board, especially in emergency situations. Pegasus Airlines is the only authority to determine the rules for alcohol service on board. All cabin crew members have the authority to decide whether to provide alcohol or not to the passengers considering their physical appearance or behavior. Pegasus Airlines gives support to ground staff who deny boarding to drunk passengers.

Passengers may only drink alcoholic beverages served to them by the cabin crew. Alcohol consumption from a bottle brought on board or from a bottle bought at the duty-free is not allowed.

4.11.1 Incident Motivators

A number of possible causes for unruly/disruptive passenger behaviour in flight have been identified:

- Intoxication (e.g., through alcohol, narcotics or medications). It shall be noted that in many cases the ingestion and consequent influence of alcohol, narcotics and/or medication starts before the passenger boarded the aircraft;
- Irritation with other passengers' actions on board (e.g., kicking seats, sharing the armrest or a lack of hygiene);
- Frustration linked with the passenger's journey: long-haul flights, inability to smoke or use personal/ portable electronic devices (e.g., mobile phones), dissatisfaction with customer service and service delivery (e.g., too slow, too long, poor quality food, inoperative equipment: IFE, lavatories, chair tables, seats);
- Mental breakdowns/episodes (e.g., acute anxiety, panic disorder or phobias);
- Mental conditions (e.g., psychosis, dementia or other mental health-related disorders);
- Personality differences among passengers or between crew members and passengers; • Emotional triggers originating outside the flight (e.g., loss of a job);
- Lack of medication or alcohol withdrawal symptoms.

Passenger disturbances are classified into four categories:

Table 4-3: Passenger Disturbances Levels

Level - 1	**Disruptive Behavior (Verbal)**	**Minor**
Behavioral indicators include, but are not limited to: • The use of unacceptable language towards a crew member (e.g., swearing or using profane language); • Unacceptable behavior towards a crew member (e.g., communicating displeasure through an aggressive voice tone or rude gesture, provoking an argument or making unreasonable demands such as refusing to give up on a denied request); • A display of suspicious behavior (e.g., agitated, numb, distant or unresponsive behavior); • Passenger not following crew instructions or challenging authority; • Violation of a safety regulation.		
Level – 2	**Physically Abusive Behavior**	**Moderate**

Behavior includes, but is not limited to:

- Physically abusive behavior towards a crew member (i.e., an openly or aggressively hostile action that includes a physical act or contact);
- Obscene or lewd behavior towards a crew member (i.e., actions of an overtly sexual, lecherous or lascivious nature);
- Verbal threats (i.e., threatening a crew member or another passenger with physical violence or bodily harm on board or while about to board an aircraft, or making threats in an attempt to board an aircraft);
- Tampering with any emergency or safety equipment on board the aircraft;
- Deliberately damaging any part of the aircraft or any property on board the aircraft.

Level – 3	**Life Threatening Behaviour**	**Serious**

Behavioral indicators include, but are not limited to, actions creating a fear of imminent death, such as:

- The threat, display or use of a weapon;
- Physical or sexual assault with intent to injure (i.e., violent, threatening, intimidating or disorderly behavior).

Level – 4	**Attempted or Actual Breach of the Flight Crew Compartment**	**Catastrophic**

An incident which constitutes a security threat and which includes, but is not limited to:

- An attempted or unauthorized intrusion into the flight crew compartment;
- A credible threat of death or serious bodily injury in an attempt to gain control of the aircraft;
- The display, use or threat to use a weapon to breach the flight crew compartment;
- Sabotage of or the attempt to sabotage an aircraft;
- Actions that render the aircraft incapable of flight or that are likely to endanger its safety of flight;
- Any attempt to unlawfully seize control of the aircraft.

4.11.2 Procedures on the Ground

To design and implement an effective training program regarding unruly/disruptive passengers, Pegasus Airlines is implementing its training program according to the TR-DGCA Security Training Directive that considers:

- The training programme is designed and adapted to the respective groups of staff: cabin crew and ground employees who deal directly with passengers prior to boarding may receive instruction and/or be provided with procedures for the handling of unruly passengers;
- Station managers may ensure that duty managers and senior employees are aware of both their authority to refuse passage and the correct procedures for doing so. Emphasis may be placed on assuring managers that they will receive full organization support. Station managers shall also be aware of procedures to follow upon arrival of the aircraft in case of police intervention and prosecution;
- Ground supervisors shall be reminded of their responsibility to pass information on potential troublemakers to the Pilot in Command and the Senior Cabin Crew Member of the flight concerned;
- Ground employees at different stations need to recognize that local rules and regulations differ from State to State. If this prevents full compliance, the company can at least adopt the general spirit of the policy and its legal services shall be solicited for advice.

4.11.2.1 Identification and Response for Unruly/Disruptive Passenger

Airport staff shall be encouraged to notify to supervisors any passengers whose behavior would suggest they might be unsuitable for carriage.

If a person appears at the check-in counter in what appears to be an intoxicated state or acting strangely, his/her condition and actions shall be reported to the ground supervisor before S/he is accepted onto the flight, allocated a seat and the checked baggage is accepted for carriage.

Whenever sporting groups, rock bands or other single-interest groups are to travel, special efforts must be made to monitor their behavior from the time of check-in to the time they board the flight. It might be necessary to use additional staff and/or contract security staff.

Where a potential problem is identified, an assessment shall be made by the Airline Representative or Passenger Handling Services Duty Manager, the PIC and the Senior Cabin Crew. The right to deny carriage of a passenger shall be published in the General Conditions of Carriage, which is available to passengers.

Other points that shall be considered when refusing a person's carriage at check-in:

- The person's condition may not be associated with intoxication; S/he may be suffering from a chronic illness, physical or neurological disability with similar symptoms to a person affected by intoxicating liquor;
- If the person contests the airline's decision, it may be necessary to have the person's physical condition examined by a medical practitioner. If the person is examined, the airline shall obtain a certificate of the medical practitioner's finding;
- An entry referring to the refusal to carry shall be included in the person's travel booking (PNR);
- A report setting the details of the refusal to carry shall be submitted by the employees who initiated and confirmed the refusal. The names of others who may give additional information regarding that refusal shall be included. A copy of PG-GU-FR-009 - Passenger Irregularity Report Form, available in Comply365, shall be filled and sent to security@flypgs.com.
- Future arrangements shall be made by the Aviation Security Department for the intoxicated person to be re-booked for a flight on a future date. The person's condition shall be reassessed on the day of travel and additional conditions of carriage may be imposed or refused.

A passenger's state of agitation, anxiety or intoxication may not be recognized until their arrival at the boarding gate. In addition, their condition could have changed from the point of check-in to being called to board the flight. Passengers availing themselves of early check-in or subject to a delay in departure may have the time to ingest a significant amount of intoxicating liquor at the airside bars and restaurants.

The following points shall be considered when a person is refused carriage at the boarding gate due to conditions that appear to make him/her unfit to fly:

Hold baggage of a passenger who has been refused carriage shall be removed from the flight;

The passenger shall be reunited with his/her checked baggage;

- Duty-free purchases shall be reported to Customs;
- The passenger shall be escorted back through the Immigration line to the landside of the terminal;
- The Senior Cabin Crew Member of the flight shall be informed of the passenger's removal;
- Arrangements shall be made for the passenger's name to be removed from the passenger manifest.

The risk of potentially disruptive passengers could be part of the pre-flight crew briefing, especially on routes known to carry a high number of such passengers. The details of the routes will be published by Aviation Security Department according to yearly reviewed statistics and risk assessment, via bulletin.

If a passenger engages in disruptive behavior while the aircraft is still on the ground, unless the situation can be resolved to the satisfaction of the on-board crew members, S/he shall be removed along with his/her baggage.

4.11.3 Procedures in the Air

The unruly passenger is handled with the co-ordination of the Senior Crew Member and by the Flight Crew initiative and authority.

Clear and simple communication between the cabin crew and the flight crew is crucial to coordinate teamwork and successfully diffuse an incident which could affect the safety of the flight, the aircraft and passengers aboard. The flight crew needs to be updated regularly on the progress of the situation by the cabin crew. The flight crew shall relay this information to the ground immediately as per their company procedures and/or the State's requirements.

Flight crew members shall never exit the flight crew compartment in order to assess a problem or to assist in resolving such matters. Responsibility to assess the situation and respond now lies in the hands of the cabin crew. In order to fulfil these responsibilities, cabin crew training has become significantly more comprehensive as per the various applicable State regulations.

The Pilot-in-Command shall report whenever a serious passenger disruption occurs during the flight, according to company policy via ACARS/VHF. If deemed necessary, the operator might request to be met on arrival by local law enforcement authorities and a representative of the air carrier if they consider that criminal prosecution is desirable. The crew shall record the contact information of all passengers who witnessed the incident, as their testimony might be required in later legal proceedings. The perpetrator shall be held by the authorities until a representative properly debriefs the crew. It shall then be decided if charges are to be brought against the perpetrator.

If charges are to be brought, all crew members shall be prepared to undergo police or aviation authority debriefings. Statements of evidence might also be required for judicial proceedings. The air carrier might consider filing a Report of an Incident of Unlawful Interference/Seizure. In addition to alerting law enforcement authorities, Pegasus Airlines Aviation Security Department must notify the State of Registry of the aircraft, the State of the Operator and States whose citizens were killed or injured.

Act according to the following levels, after discussion with the Pilot-in-Command. The Pilot-in-Command shall be informed whenever possible before any action is taken with problem passengers in the cabin and kept informed of all developments.

LEVEL 1	**DISRUPTIVE BEHAVIOUR - DURING FLIGHT**
Passenger receives a verbal warning because of disruptive behavior. Passenger stops disturbance – no other action needed.	
Forms	**The Senior Cabin Crew Member shall also fill *PG-GU-FR-009 - Passenger Irregularity Report Form* for informing the Aviation Security Department.**
LEVEL 2	**PHYSICALLY ABUSIVE BEHAVIOUR - DURING FLIGHT**
Passenger behavior becomes illegal. • Attempt to diffuse the situation verbally. If one cabin crew member fails, consider sending another one who might have more success; • If an unruly passenger refuses to stop the behaviour, Senior Cabin Crew will warn the unruly passenger on behalf of the PIC using the form below.	

Forms	***PG-GU-FR-008 - Irregularity Warning Card*** "You are acting against national and international civil aviation regulations. Please correct your behaviour. If you do not keep to our cooperative directives you will be reported to security at the destination airport. If necessary, the Pilot-in-Command will land at the nearest airport and you will be disembarked. If this is the case, your ticket fare thereafter and the expense of the aircraft landing and taking-off from this airport will be billed to you." The Senior Cabin Crew Member shall also fill the ***PG-GU-FR-009 - Passenger Irregularity Report Form*** for informing the Aviation Security Group Management
LEVEL 3	**LIFE –THREATING BEHAVIOUR –DURING FLIGHT**

Passenger still continues illegal behaviour.

- Communicate with the Pilot-in-Command via interphone and report the detail of the threatening behaviour of the unruly passenger.
- Defend the flight crew using whatever force is necessary to eliminate the threat;
- The Flight crew may declare an emergency and activate a landing plan for the nearest suitable airport if needed;
- As soon as operationally feasible, initiate a possible rapid descent;
- The Pilot-in-Command may continue to the scheduled destination or divert to the nearest airport for offloading the unruly passenger;
- The authorities will be called by the Pilot-in-Command before landing to meet the passenger upon arrival to the aircraft and hand over the copies of the forms with the unruly passenger to the airport authorities;
- Use of these devices requires the express approval of the Pilot-in-Command. Cabin crew will implement the restraint procedure as stated below in the "Restraint Section".

Forms	The Senior Cabin Crew Member shall fill the **"Passenger Irregularity Report Form (PG-GU-FR-009)"** for informing the Aviation Security Department
LEVEL 4	**ATTEMPTED BREACH or ACTUAL BREACH of THE FLIGHT CREW COMPARTMENT - DURING FLIGHT**

Passenger still continues illegal behaviour.

- The Pilot-in-Command shall maintain aircraft command and control at all cost;
- Cabin Crew communicates with the Pilot-in-Command via interphone and reports the detail of the threatening behaviour of the unruly passenger.
- Defend the cockpit using whatever force is necessary to eliminate the threat;
- The Pilot-in-Command shall declare an emergency and activate a landing plan for the nearest suitable airport;
- As soon as operationally feasible, initiate possible rapid descent;
- The authorities will be called by the Pilot-in-Command before landing to meet the passenger upon arrival to the aircraft and hand over the copies of the forms with the unruly passenger to the airport authorities;
- Use of these devices requires the express approval of the Pilot-in-Command if conditions allow. Cabin crew will implement the restraint procedure as stated below in the "Restraint Section".

Forms	The Senior Cabin Crew Member shall fill the ***PG-GU-FR-009 - Passenger Irregularity Report Form***for informing the Aviation Security Department.

Pegasus Airlines Aviation Security Department acts according to P*G-GU-PR-003 - Unruly Passenger Procedure,* available in Comply365. The purpose of this procedure is to ensure Pegasus Airlines flight safety and security, for the protection of the personal well-being and property of Pegasus, Pegasus passengers, Pegasus employees, as well as its service providers and their employees by defining the rules to follow when a passenger is showing unruly behaviour from the start of his/her reservation with Pegasus Airlines and onwards (ticket purchasing, check-in, boarding, flight, arrival and luggage delivery). The passenger may be banned from future flights.

4.11.3.1 Arrival

The support which can be expected from the Airport Police at the arrival station, will depend on the local set-up. Advice on what assistance to expect at each station must be made available to the Pilot-in-Command immediately.

Some situations could be judged by the Pilot-in-Command to be serious, but it may not warrant a formal complaint to the local authorities. However, it is the Pilot-in-Command's responsibility to raise the report of all such incidents to the Aviation Security Department for them to follow up.

If the situation is deemed serious and warrants a complaint to the local authorities, the Pilot-in-Command shall notify the station of arrival as well as the Pegasus Airlines IOCC of the situation on board via ACARS/VHF/, alerting the Security authorities.

4.11.3.2 Written Statement

- The SCC prepares the *PG-GU-FR-009 - Passenger Irregularity Report Form*, available in Comply365.
- The SCC shall also obtain the statements from other witness passengers and/or crew about the incident on the Passenger Irregularity Report Form.
- This form is signed by the Pilot-in-Command and at least two cabin crew members before handover to the local authorities.

4.11.3.3 Handover to Police

Upon arrival, Pegasus Airlines ground staff or the Contractor Handling Company staff will ensure that Police/Security personnel meet the aircraft on arrival. The Pilot-in-Command shall make a PA requesting all passengers to remain seated. The SCCM/CCM will identify the unruly passenger(s) to the authorities.

The Pilot-in-Command shall make available to the police the Passenger Irregularity Report Form. It must be noted that whenever the law enforcement officers are called to meet the flight, written statements will be taken on arrival and the crew may be interviewed.

If the incident had occurred and had been reported outside Türkiye, the Pilot-in-Command must also report it to the Pegasus Airlines IOCC immediately.

4.11.4 Authority for Use of restraints

4.11.4.1 Passenger Restraint

There are occasions when passengers demonstrate violent or unruly behavior; in almost every case, sympathetic handling and reassurance by the cabin crew is sufficient to calm the passenger down.

It is within the normal legal authority of the Pilot-in-Command to instruct passengers to follow instructions from members of the crew with regard to unacceptable behavior. Crew must exhaust all necessary steps to placate an unruly passenger and persuade him to adhere to crew instructions.

Where a passenger continues to be unruly and cannot be subdued, it is legitimate for the crew to take reasonable action to prevent the passenger continuing with such behavior. Crew may have to resort to using the Passenger Restraint Devices.

NOTE	The Pilot-in-Command has the power to restrain a passenger only if the passenger becomes unruly whilst the aircraft is airborne. If the passenger is unruly when the aircraft is still on the ground, the Pilot-in-Command shall have the passenger offloaded. If the passenger refuses to leave the aircraft, the Pilot-in-Command shall not use force but shall call for Police assistance to have the passenger removed.

The use of these devices requires the express approval of the Pilot-in-Command. In making his decision, the Pilot-in-Command will consider the following:

- All other means of placating the passenger must have been exhausted.
- The passenger's conduct must be harmful to the safety of other passengers, crew or the aircraft.

The Pilot-in-Command will bear in mind that the act of attempting to place a restraint device on the passenger may further aggravate the situation, thus provoking violence.

The number and content details of security restraint kits are described in the table

Table 4-4: Content and Number of Restraint Kits

Content	Number of Restraint Kits	Aircraft Type
4 Plastic Handcuffs 4 Plastic Body Restraining Straps 4 PG-GU-FR-009 - Passenger Irregularity Report Forms 1 Plastic Cutter	2	Airbus A320
	2	Boeing 737-800
	3	Airbus A321

- Only those crew suitably trained may use the plastic handcuffs.
- Flight crew members shall not be physically involved in restraining passengers.
- Only reasonable and necessary force may be used to affect the control and restrain.
- Prepare the plastic handcuffs for use: prepare the cuffs, adopt correct grip and body stance i.e. strongest foot rearward.
- Once control is achieved, check for tightness.
- At regular intervals thereafter (max 15 min) the restraints shall be checked to ensure that no injury is being caused to the passenger.
- Ensure the plastic handcuff cutting instrument is readily available shall an in-flight emergency require the release of the restrained passenger.
- To minimize disruption, if possible, isolate the restrained passenger by relocating surrounding passengers.
- In case where a restraint kit is used during flight, the used kit shall be replaced at the first return of the aircraft to a designated base station.

4.11.4.1.1 Reports

The following reports must be completed where restraints have been used:

- Passenger Irregularity Report Form (PG-GU-FR-009), provided in the restraint kits.
- IQSMS Security Report

4.11.4.1.2 Diversion

When a passenger has been restrained, a diversion is only to be considered in exceptional circumstances. The decision to divert shall take into account the safety of the aircraft, the wellbeing of the crew, passengers and the detainee. In the event of a decision to divert, the choice of diversion station shall be reported by the Pilot-in-Command and informed to the Pegasus Airlines IOCC for coordination and preparations.

4.11.4.1.3 Sedation

Under no circumstances may a passenger be forcibly sedated, whether or not restrained. Offers of assistance to administer sedatives from medical personnel travelling as passengers must not be accepted.

4.11.4.1.4 Emergency

In the event of a prepared emergency warranting passenger evacuation, the restrained passenger must be released in sufficient time to allow unhindered evacuation.

NOTE	Unruly passenger's foot restraint must be released 10 minutes before landing.

4.11.4.1.5 Removal of Restrained Passengers

Before landing, arrangements shall be made by the Pilot-in-Command via the Company frequency or ATC for the removal of the restrained passenger by the Police or Security Authorities.

4.11.4.1.6 Notification to Authorities

When the Pilot in Command offloads a person, the event and the reasons for offloading are to be fully reported to the Police by the Passenger Irregularity Report Form at the airport of offloading.

4.11.4.1.7 Prosecution

It is Pegasus Airlines policy that those passengers who affect the safety and security of other passengers and crew on Pegasus Airlines flights will need to be restrained in flight. Pegasus Airlines will pursue in full the prosecution and will pursue the operations and general costs that arise due to those passengers who need to be restrained in-flight.

All the information and incident reports related to the restrained passenger or passengers in flight will be passed on by the Pilot-in-Command and the Senior Cabin Crew to the Aviation Security Department.

4.11.5 Reporting Procedures

Pegasus Airlines implements an Integrated Document Management System, and all the necessary reporting forms can be obtained by Pegasus Airlines personnel from the link "https://pegasus.comply365.net/".

Contracted suppliers for Pegasus Airlines can gain access to the reporting forms from the link "https://document.flypgs.com/".

Flight Crew members and Cabin Crew members can also obtain the necessary printed forms from the Crew Briefing room at the airports.

Pegasus Airlines has an operational reporting system that encourages and facilitates personnel to report security incidents and threats, identify security deficiencies and raise security concerns. All Pegasus Airlines Flight Crew, Cabin Crew and also Passenger Handling Staff at SAW and other base stations have access to IQSMS and can provide a Security Report that will be assigned to all Aviation Security Department personnel.

4.11.5.1 Irregularity Warning Card

If an unruly passenger refuses to stop disrupting the other passengers/flight, following an attempt to defuse the situation, the Pilot in Command and Senior Cabin Crew will coordinate on the issuance of this Irregularity Warning Card (PG-GU-FR-008). The crew member shall issue this warning and fill the warning card and hand it over to the passenger. A copy of the card shall be sent to the Aviation Security Department

as co-mail. According to the SHY-IPC (Administrative Penalty Regulation), Aviation Security Department shall send the form to TR-DGCA.

4.11.5.2 Passenger Irregularity Report Form

If any unlawful interference occurs during a flight, the Pilot-in-Command shall be informed, and Senior Cabin Crew will complete this form. This form covers hijacking, seizure and any unruly passenger attempting to access the flight deck. If police were involved, then the senior police officer details shall also be noted. It will then be sent to the Aviation Security Department as co-mail. According to the SHY IPC (Administrative Penalty Regulation). Aviation Security Department shall send the form to TR-DGCA.

4.12 PROHIBITED ARTICLES

4.12.1 Carriage of Prohibited Articles by Passengers

Passengers shall not be permitted to carry into the security restricted areas or on board an aircraft the articles listed in point 4.10.3.

4.12.1.1 Exemptions

An exemption to point 4.10.1. may be granted on condition that:

- the appropriate authority has given consent that the article may be carried; and
- the air carrier has been informed about the passenger and the article that he is carrying prior to passengers boarding the aircraft, and
- the applicable safety rules are complied with.

These articles shall then be placed in secure conditions on board the aircraft.

4.12.1.2 Transport in Hold Baggage

Unless prohibited under point 5.10.3., articles prohibited under point 4.10.3 may be carried in hold baggage, provided that passengers have no unsupervised access to such baggage from the point at which the baggage is checked in to the point where it is reclaimed at arrival.

4.12.1.3 Other Articles

Security staff may refuse access to a security restricted area and the cabin of an aircraft any passenger in possession of an article not contained in point 4.10.3 over which they have concern.

4.12.2 Information to Passengers

Pegasus Airlines ensures that passengers are informed of the prohibited articles listed in point 4.10.3. before check-in is completed. The list of the prohibited items is available at the check-in counter, self-check-in desks, Pegasus Airlines official website (www.flypgs.com) and by the relevant airport authorities placing posters or notices in advantageous locations.

4.12.3 List of Prohibited Articles

Without prejudice to applicable safety rules, passengers are not permitted to carry the following articles into security restricted areas and on board an aircraft:

Table 4-5: List of Prohibited Articles in Cabin

a) guns, firearms and other devices that discharge projectiles – devices capable, or appearing capable, of being used to cause serious injury by discharging a projectile, including:

• firearms of all types, such as pistols, revolvers, rifles, shotguns • toy guns, replicas and imitation firearms capable of being mistaken for real weapons • component parts of firearms, including telescopic sights	• compressed air and CO2 guns, such as pistols, pellet guns, rifles and ball bearing guns • signal flare pistols and starter pistols • bows, cross bows and arrows • harpoon guns and spear guns • slingshots and catapults
b) stunning devices – devices designed specifically to stun or immobilise, including:	
• devices for shocking, such as stun guns, tasers and stun batons • animal stunners and animal killers	• disabling and incapacitating chemicals, gases and sprays, such as mace, pepper sprays, capsicum sprays, tear gas, acid sprays and animal repellent sprays
c) objects with a sharp point or sharp edge – capable of being used to cause serious injury, including:	
• items designed for chopping, such as axes, hatchets and cleavers • ice axes and ice picks • razor blades • box cutters • knives with blades of more than 6 cm	• scissors with blades of more than 6 cm as measured from the fulcrum • martial arts equipment with a sharp point or sharp edge • swords and sabres
d) workmen's tools – tools capable of being used either to cause serious injury or to threaten the safety of the aircraft, including:	
• crowbars • drills and drill bits, including cordless portable power drills • tools with a blade or a shaft of more than 6 cm capable of use as a weapon, such as screwdrivers and chisels	• saws, including cordless portable power saws • blowtorches • bolt guns and nail guns
e) blunt instruments – objects capable of being used to cause serious injury when used to hit, including:	
• baseball and softball bats • clubs and batons, such as billy clubs, blackjacks and night sticks	• martial arts equipment
f) explosives and incendiary substances and devices –capable, or appearing capable, of being used to cause serious injury or to pose a threat to the safety of the aircraft, including:	

• ammunition • blasting caps • detonators and fuses • replica or imitation explosive devices • mines, grenades and other explosive military stores	• fireworks and other pyrotechnics • smoke-generating canisters and smoke-generating cartridges • dynamite, gunpowder and plastic explosives

End of Section

5 SECURITY OF CHECKED BAGGAGE

For the purpose of this chapter, “secured baggage” means screened departing hold baggage, including courier baggage that is physically protected so as to prevent the introduction of any objects.

5.1 PURPOSE OF THE SECURITY MEASURES

All hold baggage shall be screened prior to being loaded onto an aircraft in order to prevent prohibited articles from being introduced into security restricted areas and on-board aircraft.

Bearing that in mind, hold baggage shall be accepted only from legitimate passengers in possession of a valid ticket and processed by a responsible agent or authorized representative. Pegasus Airlines ensures that every passenger travels on the same flight as their checked hold baggage. Where this is not the case, that hold baggage shall be considered as unaccompanied baggage. Such hold baggage shall be removed from the aircraft and shall not be carried on that flight.

5.2 PASSENGER IDENTIFICATION CHECKS

Before looking for the anomalies here under described, staff shall be properly trained for the assessment of how and who may pose a threat. Staff members shall realize that some threats can come from unwary passengers (naive travelers, framed terrorists, etc.). Passengers who have been exploited (mules), who may not fall or fall in different ways in these characteristics shall be dealt with accordingly with proper questioning.

When a passenger is checking in at the ticket counter or gate, the agent shall look for the following characteristics:

- Nervous or disoriented;
- Overly aggressive or cooperative;
- Passive, avert gaze, aloof.

While emotional characteristics can signal that something is wrong with a passenger, it does not necessarily mean that the passenger has a malicious intent. For many, flying is a very stressful experience. Others view flying as a necessary evil in their job and approach it with resentment. Whatever the reason behind a passenger's uneasiness of flying, the check-in or gate agent shall investigate whether it is simply enough to reassure or calm the passenger or otherwise.

5.2.1 Standards of Checks

Check-in or gate agents shall also look for the following characteristics, which may require further questioning for verifying with the passenger:

- A passenger with no baggage, too little or excessive baggage for the duration of the trip;
- A passenger claiming not to have key(s) or unable to open luggage if required;
- Name on baggage does not match name on ticket/passport;
- Unusual or illogical routing;
- One-way ticket (exceptions would be permanent residents returning home);
- A passenger unsuitably attired or not at ease for the class of travel;
- Arriving at check-in or boarding gate at the last minute;
- A passenger rushing the staff to complete procedures;
- Having someone else checking in for them;
- The passenger shall speak the language of the country issuing the passport or of the country in which they claim residency;
- The passenger shall have other identification documents or cards in the same name;

- The passenger can accurately recall the full name, date and place of birth listed in the passport;
- The passenger maintains secret contacts with others;
- The passenger insists on boarding a specific flight for no valid reason;
- The passenger seems to be lying or withholding information;
- Absence of contact/address details or passenger declines to provide them;
- History of “no-shows”;
- Available details of passenger history/travelled sectors arouse suspicion or concern;
- The passenger accepts a large penalty to amend ticketing or upgrade;
- The passenger displays inordinate interest in the type of aircraft/seating etc.;
- The passenger seems to be intoxicated.

In forming an assessment, it is important to recognize that no one aspect of the above criteria necessarily indicates the passenger is a possible security risk. However, the greater the combination of these criteria applying to the passenger, the greater the likelihood of a risk factor associated with their travel.

- Passengers may also try to conceal their true itineraries and ultimate destination. Check-in or gate agents shall look for the following signs of previous travel:
- Entry and exit stamps;
- Recently issued visas;
- Two passports or conflicting documents with conflicting information;
- Baggage tags;
- Clothing:
  - appropriate for the occasion (business, pleasure, stated occupation, etc.);
  - matching the climate of the destination;
  - matching the styles in the country of origin or destination;
  - fitting the passenger adequately; it shall be his/her own.

Check-in or gate agents also shall perform a quick check of the ticket. The following characteristics may signal a need to further investigate:

- The ticket was purchased in a third country (other than the destination or origin);
- The ticket was paid for in cash or in an unusual manner;
- The highest fare was paid, when present with other contra-indicators;
- Non-sequential tickets for family members could be a problem. Conversely, sequential tickets for unrelated persons could also be a problem;
- The name on the ticket must match the name in the passport;
- Source/location of supposed ticket purchase is questionable.

5.2.2 Location of Checks

Check–in:

All passengers shall prove their identity and their proper travel documents related to the destination country (passport, visa, etc.). This is to ensure that information about legitimate persons is not being passed on and used by other people. If any passenger is unable to prove his identity and that he has proper travel

documents, he shall be refused travel. The Check-in Agent shall confirm with each passenger that they do not carry any prohibited and dangerous items in their hold and hand carried baggage.

Group check-in:

As stated above the check-in procedures shall be implemented for group check-in. The checked-in baggage shall be protected as defined.

Boarding:

Each individual passenger shows their identity, proper travel documents and boarding card during the boarding. The ground handling agent shall provide the document match services and travel documents on each Pegasus Airlines flight.

5.3 QUESTIONING OF PASSENGERS

If there is a need to question a passenger, the contracted supplier or security agent shall explain the reasons to the traveller, whenever possible.

They shall ask questions to try to identify passengers who might pose a risk to the flight. The initial questioning shall generally be limited to two or three questions unless the passenger poses some concern, so as to avoid delaying the customer unreasonably. When checking in a group or family, the agent shall ask questions of all members of the group. Questions shall be open ended. It is important not to feed a possible passenger answer. Contracted suppliers and security agents shall be polite and friendly when asking questions and give the passenger time to answer without interruption.

5.3.1 Description of Questions

When asking questions of passengers, it is very important that agents make eye contact with the passengers in order to be able to assess their body language when they answer the questions. Signs of stress often manifest themselves in non-verbal behaviours and airline and security agents shall be able to identify them and judge what the source may be. It is important to keep in mind that the characteristics mentioned below do not necessary mean that the person is under stress or that they are a risk passenger. For example, they could be scared of flying, scared of missing the flight, or just angry because of the questioning.

Stress often shows itself as non-verbal behavior and can be divided into four main groups:

- Hand actions;
- Body movements;
- Body reactions;
- Behavioral pattern recognition.

Hand actions that show stress are:

- Clenched fists;
- Juggling coins or pocket contents;
- Arms crossed in a defensive stance;
- Constantly grooming hair;
- Rubbing eyes;
- Touching nose, lips, ears and groin;
- Nail biting;
- Knuckle cracking.

Body movements that are clear signs of nervousness include:

- Avoiding eye contact;
- Nervous laughter;
- Yawning;
- Foot tapping;
- Pacing;
- Licking and biting lips;
- Grinding teeth;
- Despondent stance;
- Shifting weight from foot to foot;
- Fidgeting with clothing;
- Touching face.

When a person is under stress, his/her body may react in the following ways:

- Perspiration;
- Blushing;
- Goose bumps;
- Pulsating Adam's apple;
- Pupil dilation;
- Dry mouth;
- Nervous speech.

Stress can cause a person to act in the following ways:

- Overly friendly or flirtatious;
- Aggressive;
- Rushing;
- Frustrated.

Passenger Questioning at Check-in:

Passenger questioning shall complement hold baggage screening at check-in counter. Those questions are:

- To whom does this baggage and the contents belong?
- Who packed your baggage?
- From the time the baggage has been packed until now, where has it been?

5.3.1.1 Passenger Risk Assessment

Passenger risk assessment can be performed electronically and/ or in the more traditional in-person environment. There is some debate about which method is the best solution for an air carrier to accurately assess its passengers.

A strength of automated passenger risk assessment is that the decision parameters can be kept confidential and changes to algorithms can be implemented quickly.

To a varying degree, in-person passenger risk assessment has always been used by air carriers to assist staff to identify passengers who may have malicious intents. Human factors can be a major flaw as regards

in-person risk assessment. The human element can make assessment highly irregular from passenger to passenger.

On the other hand, face-to-face contact when trying to determine risk can be very valuable. A passenger in possession of all the necessary documents who intends to commit his first act of unlawful interference might be able to get through a fully automated passenger risk system.

In order to assess passenger risk in the most efficient manner, a system shall be devised where both automated and in-person risk assessments are employed and complement each other. Automated passenger risk assessment shall be used to clear the vast majority of passengers.

The assessment criteria shall be such that around 90 percent of the passengers can be cleared by automated risk assessment programmes. The rest of the passengers will then have to take part in in-person risk assessment where air carrier staff will manually assess the passenger by asking questions, observing body language and verifying identification documents.

If the assessment systems are not developed to the point of allowing this integration, the two approaches can still be used separately, though the in-person assessment personnel shall consider all passengers in their assessments.

5.3.1.2 Passenger Risk Assessment (In-Person)

Passenger risk assessment is a very sensitive issue. Whereas assessments of travel history, purchase behaviour and various other travel documents can be undertaken with some objectivity, assessments of behavioural, non-verbal, and verbal indicators are much more subjective; they may therefore be more difficult to analyse and are potentially less defensible.

The check-in process presents an important opportunity for assessing those in the queue. Experienced air carrier staff can generally assess with a degree of accuracy the passengers that need to be looked at more closely and those passengers who pose no threat to the air carrier.

Pegasus Airlines or contracted passenger handling staff shall be aware of a variety of disruptive passenger behaviours, such as drunkenness or aggressiveness which might impact on the safety and comfort of other passengers, as well as behaviours that might indicate a security risk i.e. intentional or purposive wrong doing on the part of the passenger.

An increasing percentage of passengers check in online or via common-user self-service kiosks, do not check in hold baggage and first experience human interaction at the airport security checkpoint. For these passengers, behavioural analysis must be conducted either during the passenger queue and preparation process or at the screening point.

When performing passenger risk assessment, the representative of Pegasus Airlines or the contracted passenger handling company employee is looking for the presence of an anomaly. However, it is very important to keep in mind that abnormal does not necessarily mean wrong; it is merely an indicator that further assessment may be warranted. There is probably anecdotal evidence to support almost every type of abnormality encountered where, in the end, there was a logical explanation.

Finally, it is very important to stress that passenger risk assessment is in no way related to ethnicity or race; it must be evidence-based to the greatest extent possible.

5.3.1.3 Intervention

When Pegasus Airlines or a Ground Handling Staff member identifies a potential problem passenger by document verification, questioning or any other means, they shall notify their supervisor and the Border Police.

As far as possible the conversation with the supervisor/Border Police shall take place away from the traveler to ensure they cannot overhear the discussion. The supervisor shall then make contact with the local border authority who shall then continue with the necessary inquiry and/or questioning following their own guidelines.

The policy of the Pegasus Airlines Security Department is that contracted ground handling supplier staff shall never directly confront a passenger about the reliability of his/her travel documents or of their

intentions. Direct confrontation may lead to a violent reaction by the passenger. Also, false accusations can lead to libel suits which can cost Pegasus Airlines large sums of money and adversely affect its reputation.

5.3.2 Location of Delivery

- Check–in
- Boarding

5.3.3 Details of Service Provider

Pegasus Airlines has given the responsibility by contract to second and/or if necessary to third parties at all airports.

Please contact the Support Procurement Leadership Department, also refer to the Audit Reports.

5.3.4 Passenger Data Protection

According to the Turkish Data Protection Law, Pegasus Airlines shares the API / PNR data with the General Directorate of Immigration or another relevant authority in accordance with the Regulation on the Procedures and Principles on the Obligations of Air Carriers. This information may be shared by other agencies and the General Directorate of Immigration if it is necessary for aviation security and country security.

The data sharing by Pegasus Airlines is undertaken only via the Guest Relations Department and it is prohibited to share any passenger's data with relevant authorities without prior approval of Pegasus Airlines Legal Department. All data requests must be sent by mail to MISAFIR@flypgs.com or to the postal address.

5.4 PROCEDURES FOR SCREENING AND HAND-SEARCHING OF ORIGINATING CHECKED BAGGAGE AND COURIER

All hold baggage, including courier baggage, loaded on international and domestic flights is screened by certified screeners using approved screening methods. All hold baggage, including courier baggage, to be carried on a commercial aircraft is protected from unauthorized interference from the point it is screened or accepted into the care of the Pegasus Airlines or their contracted supplier, whichever is earlier, until departure of the aircraft on which it is to be carried. If the integrity of the hold baggage is jeopardized (unauthorized access, suspected access or uncertainty re integrity etc.), the hold baggage shall be re-screened according to point 5.4.1. before being placed on board an aircraft.

Once screened, only hold baggage belonging to passengers of the relevant flight or identified as unaccompanied baggage and authorized for transport is to be loaded

5.4.1 Standard of Screening and Searching

5.4.1.1 Hand Search

A hand search shall consist of a thorough manual check of the baggage, including all its contents, so as to reasonably ensure that it does not contain prohibited articles.

5.4.1.2 Screening Procedure Using X-Ray Equipment

Where x-ray equipment is used:

(a) It shall have threat image projection (TIP) software installed and employed; or

(b) between 10% and 20% of hold baggage, selected on a continuous random basis, shall also be screened by:

(i) a hand search; or

(ii) EDS equipment; or

(iii) Explosive detection dog (EDD); or

(iv) Explosive trace detection equipment (ETD); or

(v) the same x-ray equipment for a second time, whereby the same screener examines the baggage from a different angle with at least 60° and no more than 90° rotation, unless multi-view x-ray is used.

5.4.1.3 Alarm Resolution

Where EDS equipment is used and when a piece of hold baggage generates an alarm, either the alarm shall be resolved by the screener if he is satisfied that the baggage does not contain prohibited articles, or the baggage shall be screened again by one or more of the following methods:

(a) EDS equipment of a higher standard;

(b) EDS equipment that is of the same standard but used in a manner that allows a more detailed examination of the baggage;

(c) a hand search;

(d) x-ray equipment, whereby the same screener examines the baggage from a different angle with at least 60° and no more than 90°rotation, unless multi-view x-ray is used;

(e) x-ray equipment, whereby a screener examines the baggage from two different angles with at least 60° and no more than 90° rotation, unless multi-view x-ray is used;

(f) EDD;

(g) ETD equipment.

Where EDD as referred to in point (f) or ETD equipment as referred to in point (g) are employed for alarm resolution, either the whole bag shall be screened or, if it can be clearly identified, only the item(s) causing the alarm may be screened.

5.4.1.4 Dense Items

Where X-Ray or EDS equipment is used, any item whose density impairs the ability of the screener to analyse the contents of the baggage shall result in it being subject to another means of screening.

5.4.1.5 Use of Explosive Trace Detection (ETD) Equipment

Screening by explosive trace detection (ETD) equipment shall consist of the analysis of samples taken from both the inside and the outside of the baggage and from its contents. The contents may also be subjected to a hand search.

5.4.1.6 Screening of Hold Baggage by ETD Requiring Particulate Sampling

The screening, by ETD equipment which requires particulate sampling, of hold baggage shall use samples taken from at least the following:

(a) parts of the outside of the baggage that are frequently handled, such as zips, handles and clasps of the item; and

(b) the inside of the baggage including, where applicable, the inner lining of the baggage or the outside of any large items contained within the baggage.

5.4.1.7 Screening of Hold Baggage by ETD Requiring Vapour Sampling

The screening, by ETD equipment which requires vapour sampling, of hold baggage shall use samples taken from at least the inside of the baggage.

5.4.1.8 Equipment Failure Procedure

The hold baggage shall not be loaded to the aircraft until it is screened at least by one method defined in point 5.4.1.

5.4.1.9 Continuous Reviewing of Images

Person's screening hold baggage by x-ray or EDS equipment shall normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener shall not review images for at least 10 minutes. This requirement shall only apply when there is an uninterrupted flow of images to be reviewed.

There shall be a supervisor responsible for screeners of hold baggage in order to assure optimum team composition, quality of work, training, support and appraisal.

5.4.1.10 Hold Baggage Screening Systems

The methods available for "Hold Baggage Screening" (HBS) include but are not limited to:

- manual search,
- trace detection,
- explosive detection dogs (K-9),
- conventional X-ray,
- computer assisted (smart) X-ray systems,
- passenger risk assessment techniques.

As each airport has its own characteristics, there is no single solution suitable for all airports. The fundamental aim is to ensure the system that is developed can deal with current baggage throughput (including peak demand) and future forecasts (i.e., the planning has to be demand led) and can deliver an effective and efficient screening process that meets the required standards.

Key considerations in the successful management of HBS systems with the introduction of an in-line integrated baggage handling system include:

- the synchronization of the belt speed of conveying equipment to processing speed and capacity of the explosive detection system (EDS) technology that is employed;
- the elimination of any potential "bottle-necks" from hindering facilitation and the baggage transfer process by minimizing inclines on the baggage sortation system and baggage handling systems;
- the minimization of inclines on the baggage sortation system, where any alterations are made to integrate with or accommodate the HBS solution in operation.

All relevant baggage is searched or screened by a means acceptable to the relevant regulatory body. It is recommended that security staff ensure, before security controls are carried out, the status of each bag presented for examination . A bag can be designated as "clear" only when it has been determined that the bag and its contents do not contain any prohibited articles. Where a bag is screened by X-ray and has not been "cleared", further examination procedures are applied in an attempt to resolve the cause of the concern. The bag cannot be allowed to proceed for carriage until all concerns are resolved fully and effectively.

Where a multi-level search process is adopted, the following general principles are to be applied:

- the number of search levels is kept to a minimum,
- relevant information is passed on from one level to the next,
- each successive search level provides added security value,
- the search process is always "fail safe".

Each successive screening level provides clear additional security value derived from increased depth, quality and/or detail of the examination.

Where the status of a bag is ambiguous, the bag is to be treated as "uncleared" and subjected to the appropriate screening procedures. It is essential to ensure that no assumptions about the clearance status of a bag are allowed. X-ray operators do not clear a bag unless they are satisfied that no prohibited articles

are present and reject any bag about which they have any reservations or doubts. The system ought to reject automatically when:

- the operator fails to make a decision;
- the bag midtracks within the HBS system;
- the screening equipment fails to make a decision because insufficient information was obtained.

Effective contingency plans are in place to assure that, in the event of a breakdown or failure of the HBS system, all relevant bags can continue to be screened to the required standards. Examples of contingency options include:

- diverting bags to other available HBS facilities in operation;
- moving passengers to other check-in desks linked to operational HBS facilities;
- asking some passengers to take their baggage to central search facilities;
- setting up additional hand search facilities;
- bringing in mobile X-ray equipment;
- utilizing State approved emergency baggage screening mitigation techniques.

5.4.2 Location of Screening and Searching

Locations of baggage screening systems may include:

- Terminal areas;
- Security area before check-in;
- Screening in front of check-in;
- Screening devices at or behind check-in;
- Screening downstream in the baggage system.

Under all circumstances, all originating international and domestic hold baggage must undergo screening before access or delivery to the Security Restricted areas of an airport or aircraft.

5.4.3 Details of Screening Equipment

The following methods, either individually or in combination, shall be used to screen hold baggage:

(a) a hand search; or

(b) x-ray equipment; or

(c) explosive detection systems (EDS) equipment; or

(d) explosive trace detection (ETD) equipment; or

(e) explosive detection dogs.

Where the screener cannot determine whether or not the hold baggage contains any prohibited articles, it shall be rejected or rescreened to the screener's satisfaction.

Whatever method and location are selected, it shall take into account the requirement for the passenger to be present during a manual search and the ability to rapidly reconcile passengers with their baggage when a manual search is necessary, or an anomaly is detected.

5.4.4 Details of Operator or Service Provider

Inside Türkiye, the Ministry of Internal Affairs is responsible for the screening of checked baggage.

Outside Türkiye, responsibility rests with an authority which performs the screening or which contracts with security agency personnel. Also, depending on the regulations or risk assessment in some airports,

Pegasus Airlines can contract to second and/or if necessary to third parties, via the process described under the point 17.2.

5.5 PROCEDURES FOR TRANSFER OF CHECKED BAGGAGE SCREENING AND HAND-SEARCHING

Transfer of hold baggage may be exempt from screening, if:

(a) it has been previously screened to the standard detailed in this ACSP according to Doc 30 or NCASP;

(b) it arrives from a country where the security standards applied are recognised as equivalent to the common basic standards detailed in Doc 30 or it arrives from a country complying with Turkish NCASP Annex 25.

WARNING	Otherwise, the transfer of hold baggage must be subjected to the same implementation as point 5.4 involving checked baggage as regards the standard of screening, location of screening, details of screening, details of screening equipment, details of service providers.

5.5.1 Transit Hold Baggage

Transit hold baggage may be exempt from screening if it remains on board the aircraft.

5.6 PROTECTION OF CHECKED / HOLD BAGGAGE

Pegasus Airlines contracted ground handling service supplier or responsible local airport authority, or their contracted security service supplier, ensures that the hold baggage to be carried on an international or domestic flight must be protected from unauthorized interference from the point at which it is accepted into the care of Pegasus Airlines, until departure of the aircraft on which it is to be carried.

5.6.1 Description of Procedures

- Prior to being loaded, hold baggage shall be held in the baggage make-up area or other storage area of an airport to which only authorized persons may have access.
- Any person entering a baggage make-up or storage area without authorization shall be challenged and escorted out of the area.
- Originating and transfer hold baggage shall not be left unattended on the ramp or plane side prior to being loaded on the aircraft.
- Tail-to-tail transfer hold baggage shall not be left unattended on the ramp or plane side prior to being loaded.
- Access to lost-and-found offices in the terminal shall be restricted to prevent unlawful access to baggage and materials.

5.6.2 Rescreening of Unprotected Hold Baggage

Hold baggage that has not been protected from unauthorised interference shall be rescreened by at least one method according to the point 5.4.1.

5.6.3 Access to Screened Hold Baggage by Passengers

Passengers may not be allowed access to screened hold baggage, unless it is their own baggage and they are supervised by the contracted ground handling or security service supplier or other authorized personnel to ensure that:

(a) no prohibited articles as listed in point 5.10.3 are introduced into the hold baggage; or

(b) no prohibited articles as listed in point 4.10.3 are removed from the hold baggage and introduced into the security restricted areas or on board an aircraft.

5.6.4 Baggage in Critical Parts and Other Parts

5.6.4.1 Baggage in a Critical Part

Hold baggage that is in a critical part of the security restricted areas shall be considered as protected from unauthorised interference.

5.6.5 Baggage in a Part Other Than a Critical Part

Hold baggage that is in a part other than a critical part of the security restricted areas shall be considered as protected from unauthorised interference if:

(a) it is secured by a baggage lock etc.; or

(b) it is not left unattended.

Where secured baggage is handled by unscreened persons, the baggage shall not have been tampered with by this person, otherwise it must be rescreened by at least one method according to point 5.4.1 before being loaded onto an aircraft.

5.7 PROCEDURES FOR OFF AIRPORT CHECK-IN

Pegasus Airlines does not implement “Off-Airport Check-in” on its flights.

5.8 PROCEDURES FOR CARRIAGE OF FIREARMS AND WEAPONS

Pegasus Airlines flights do not carry weapons in the flight crew compartment areas.

5.8.1 Legal Provisions and Regulations

Pegasus Airlines carry weapons when legally permitted by all the State(s) involved, including those States involved in the flight departure, transit and arrival aerodromes in accordance with ICAO Annex 17, ECAC DOC 30, Turkish National Civil Aviation Security Programme and Article 93 of Turkish National Civil Aviation Law Number 2920.

5.8.2 Acceptance Procedures

5.8.2.1 Acceptance Procedures for Passengers

5.8.2.1.1 In Departure from Domestic Airports

The following must apply:

- An authorized and duly qualified person shall accept and determine that the weapon is not loaded, bullets are separated from the weapon and placed in a separate bag in the land side of the airport.
- One copy of the weapons delivery form shall remain with the police, one with the passenger and the third with weapons delivery person.
- Pegasus Airlines shall ensure that the weapons are transported between the initial acceptance point to the aircraft as it is described on National Civil Aviation Security Program.
- The weapons shall be accepted from the police and carried to the aircraft by “Airport Security Commission Approved Persons”. Those individuals can be airport police officers, Pegasus employees, contracted ground handling and private security staff in designated secure bags and routes of relative airport.
- Weapons shall be put in a locked case in the aircraft front cargo compartment where it cannot be reached by the passenger.

- Individual carrying the weapon shall remain by the aircraft and monitor the weapons against unauthorised and unlawful interference until cargo doors are closed.
- The ammunition must be securely boxed and carried separately to the weapon by airport police.
- Handling operation agent shall notify the pilot in command when weapons and ammunition are carried on the aircraft by Load Sheet Form or NOTOC. The weapon carriage information shall also be available in Cabin Smart Ops system and e-Load Sheet (if hardcopy is not used).
- According to the IATA's Dangerous Good Regulation 5kg of ammunition can be carried by a passenger on Pegasus Airlines flights.
- For international flights, permits for transportation of both sporting and all other weapons must be obtained from the official authorities of relative countries by the passenger. These permits must include departure, arrival and all transit and transfer destinations.
- These permits must be presented to the weapons accepting authority at the airport before passenger applies for check-in.
- Pegasus airline authorized ground handling representation must be informed regarding the inquiry.
- Ground handling (including outsourced companies) shall inform transit/transfer and arrival destinations via SITA message before the departure of the aircraft.
- Weapons and/or ammunitions return to the passenger by authorized person at the destination while implementing security procedures.
- Passengers are notified of the procedure via Pegasus Airlines General Rules - Section 9.4.9, availale at "www.flypgs.com".

5.8.2.1.2 In Departure from International Airports

- The passenger must be requested to declare the clearance of weapons and ammunitions for transportation by completing a Weapon Delivery Form.
- In some airports, an authorized and duly qualified person may accept and determine that the weapon is not loaded, bullets are separated from the weapon and placed in a separate bag in the land side of the airport.
- One copy of the weapons delivery form shall remain with the handling agent, one with the passenger and the third with weapons delivery person.
- Pegasus Airlines shall ensure that the weapons are transported between the initial acceptance point to the aircraft as it is described on relevant National Civil Aviation Security Program.
- Weapons shall be put in a locked case in the aircraft front cargo compartment where it cannot be reached by the passenger.
- Handling operation agent shall notify the pilot in command when weapons and ammunition are carried on the aircraft by Load Sheet Form or NOTOC. The weapon carriage information shall also be available in Cabin Smart Ops system and e-Load Sheet (if hardcopy is not used).
- According to the IATA's Dangerous Good Regulation 5kg of ammunition can be carried per passenger on Pegasus Airlines flights.
- Permits for transportation of weapons must be obtained from the official authorities of relative countries by the passenger. These permits must include departure, arrival and all transit and transfer destinations.
- These permits must be presented to the weapons accepting authority at the airport before passenger applies for check-in.
- Pegasus Airlines' authorized ground handling representation must be informed regarding the inquiry.

- Ground handling company (including outsourced companies) shall inform transit/transfer and arrival destinations via SITA message before the departure of the aircraft.
- Weapons and/or ammunitions return to the passenger by an authorized person at the destination while implementing security procedures.
- Passengers are notified of the procedure via Pegasus Airlines General Rules - Section 9.4.9, availale at "www.flypgs.com".

5.8.2.2 Bodyguards To Government VIPs

On all Pegasus Airlines flights, carriage of weapons is not allowed in the flight deck compartment.

VIP Guards Weapons Carriage in Cabin on Pegasus Airlines Flights within these principles are applicable as following:

This procedure is **only** applicable on Pegasus Airlines Domestic Flights. (Turkish Republic of Northern Cyprus flights are not evaluated as Domestic Flights.)

- Such Guards shall be public officials.
- Guards of persons with titles defined in point "5.8.2.2.1." are allowed to carry weapons in the cabin only if they are travelling with the person they are protecting and, on condition that they satisfy the following requirements.
  - If VIP Guards are travelling with the person they protect, this situation is considered as a mission order. If they are travelling alone, VIP Guards are subject to the standard Weapon Delivery Procedure as with any passenger.
  - By the regulation of TR-DGCA, it is considered that Pegasus Airlines has allowed “In Cabin Weapon Carriage Procedure” for Guards defined on point "5.8.2.2.1."
  - In the case that the carried weapon and ammunitions are used, the VIP Guard himself is taken to be responsible as regards passengers and Pegasus Airlines.
  - VIP Guards must act within established confidentiality criteria and procedures.
  - An appropriate training shall be provided by the institution/department responsible for VIP Guards depend according to standard requirements defined by the TR-DGCA. At the end of the training, Guards who will be in charge of carrying a weapon shall sign a written commitment including their authorization and responsibilities, or this commitment shall take place at the delivered training certificate. Weapons belonging to Guards not in possession of the concerned certificate shall be accepted according to standard Weapon Delivery Procedure. The certificate shall be shown during the check-in process.
  - The registration of VIP Guards travelling armed shall be performed by the VIP Protocol Office before the flight. The registration shall contain the Guards names’, weapons and flight details. On the transfer flight, the next flight details shall be declared, and the next airport shall be informed.
  - During the reservation or boarding card printing processes, Guards shall inform Pegasus Airlines’ staff or the Ground Handling Agent. During the Check-in process, a CWEA code shall be entered as the SSR. The Ground Handling Agent concerned shall inform the Senior Cabin Crew and/or Pilot-in-Command by fulfilling the Cabin Information Sheet, and/or via Smart Cabin and EFB (e-loadsheet) where relevant. The Senior Cabin Crew will verbally inform the Pilot-in-Command before the arrival of passengers including their number and seats occupied.
  - The seat next to the Guards shall be left empty as long as the seats availability make this possible.
  - As far as possible, Armed VIP Guards shall embark first onto the aircraft and disembark the last.
  - In the case of transfer flights, the Transfer Point Ground Operation Handling Service shall be informed about the seat number of the armed VIP Guards.

- In the Aircraft Cabin, VIP Guards shall carry their weapon with them or place it in a closed case they carry with them, separated from the bullets and magazine in the manner that it cannot be fired unintentionally and is not noticed by other passengers.

5.8.2.2.1 List Of Protocol Protection Officers Allowed To Carry Weapons In A Civil Aircraft Cabin

(1) President of Turkish Republic

(2) Turkish Grand National Assembly (Parliament) President

(3) Prime Minister

(4) Commander of Turkish Armed Forces

(5) Leader of the Main Opposition Party

(6) Former Presidents

(7) Chairman of the Constitutional Court

(8) First President of the Supreme Court

(9) Chairman of the Council of State

(10) Members of the Council of Ministers

(11) The Undersecretary of the National Intelligence Organization

5.8.2.3 Escorts of Prisoners/Deportees

The carriage of weapons by escorts of Prisoners or Deportees shall be subjected to the same procedure as defined under the point 5.8.2.

5.8.2.4 In-Flight Security Guards

Pegasus Airlines shall be entitled to apply to a State for the assignment of IFSOs to a flight when, in its judgment, such assignment is necessary to ensure the safety of the flight to its destination. Good and sufficient cause must be submitted to the Appropriate Authority to support the request for additional security in flight.

If permitted by the States involved, all IFSOs, whether operating overtly or covertly, shall be subject to the authority of the Pilot in Command, who shall be notified as to the number and the seats of armed persons on board the aircraft and their seat location.

The length of time that IFSOs may be kept on flying status has not been scientifically established, but it is believed that their duty shall not be greater than the crew duty.

Once a decision has been made to utilize IFSOs, it is essential that airline operators are consulted as to the procedures to be established and the training to be provided.

The following aspects shall be taken into consideration during IFSO training:

- Conduct of operations;
- Standards of performance;
- Operators and their network;
- Types of aircraft;
- Cabin equipment;
- Duties and responsibilities of the crew;
- Airport organizations;
- Routing of passengers and crews;
- Flight plans;

- Emergency procedures;
- Aggressive manoeuvres;
- Personal psychological problems on duty;
- Civil and military explosives and detonators;
- Explosive charges used for sabotage;
- Hand grenades and explosives in general.

If IFSOs are provided with firearms, it is important to use low calibre pistols that fire frangible bullets that explode on impact rather than penetrate through their target. Partly or fully jacketed bullets shall not be used as they may pass through the intended target and strike other persons or objects.

Under no circumstances shall IFSOs be employed in the role of pursers or other crew members.

A special training programme for all crew members will be included in the crew security training programme:

- Assuring a close and easy working relationship between crew members and guards;
- Enhancing communication capability between the guards and between the guards and the crew;
- Establishing arrangements to ensure ease in boarding the aircraft first and disembarking last at the end of the flight.

Provisions may be made for IFSOs to meet the crew prior to each flight departure. It is particularly important, at this time, to ensure that an accurate and discreet communications procedure is established and all members of the crew, as well as the agents, are familiar with it.

To avoid familiarity, an effort shall be made to rotate IFSOs to prevent them from travelling constantly with the same flight and cabin crews.

5.8.2.5 Military Personnel, Police And Law Enforcement Officers

Within the scope of Article 93 of Turkish National Civil Aviation Law Number 2920, procedures described in this chapter are only applicable on Pegasus Airlines Domestic Flights. Which prohibits carriage of weapons and ammunition during flight with exceptions included.

5.8.2.5.1 Personnel On Duty

In case of an individual or grouped transfer of military personnel, police or law enforcement officers in duty and in possession of an official document:

- A prior notification shall be given (minimum 24 hours) to Pegasus Airlines Aviation Security Department and/or EVP - Ground Operations,
- A pre-approval shall be given by the Aviation Security Department,
- Weapons, ammunitions and other military equipment shall be carried as hold baggage within the scope of Civil Aviation and Pegasus Airlines regulations and standards.

5.8.2.5.2 Personnel Off Duty

If military personnel, police or law enforcement officers are travelling off duty, they shall be considered as passengers and be subject to the same procedures as defined in point "5.8.2.1.1".

5.8.3 Protection on the Ground

Pegasus Airlines ensure that the weapons carried between the terminal and aircraft are as described in the National Civil Aviation Security Programme.

The weapons shall be carried by the “Airport Security Commission Approved Persons”. Those staff can be the Airport Private Security Identity Card holder, the Airline Ground Agent, the Ground Handling Company Agent or the Airport Security Police.

5.9 TREATMENT OF SUSPECT BAGS

If a bag raises suspicion, the reason must be ascertained. If an item is too opaque for proper analysis or cannot be properly inspected using a particular screening methodology, other methods shall be employed. If an item appears to be an explosive device (with all the necessary components):

(a) it shall be treated as an unaccompanied bag and subjected to additional screening; and

(b) if it cannot be confirmed with certainty that it does not contain any potentially dangerous item, the bag shall not be loaded on to the aircraft.

If security measures uncover a suspicious item in a bag, it is important that the:

(a) staff members do not touch the suspicious item;

(b) the airport security department and EOD unit are contacted;

(c) consignment is not moved by anyone except EOD unit personnel;

(d) the airport security department determines which areas are at risk and orders an immediate evacuation of these areas; and

(e) the EOD unit determines whether it is necessary to detonate the item, basing their assessment on the threat posed by the item.

Once the situation has been resolved, in cases where a dangerous item has been positively identified, all bags destined for the same flight and/or accepted shall be seen as a higher threat and shall undergo screening. Government regulators shall be notified of the discovery, as well as other passengers and aircraft operators operating from the affected facility.

5.10 PROHIBITED ARTICLES

Passengers shall not be permitted to carry in their hold baggage the articles listed in point 5.10.3.

5.10.1 Exemptions

An exemption to point 5.10 may be granted on condition that:

(a) the appropriate authority has national rules permitting carriage of the article; and

(b) the applicable safety rules are complied with.

5.10.1.1 Other Articles

Security staff may refuse the transportation of hold baggage containing an article not covered by point 5.10.3 over which they have concerns.

5.10.2 Information to Passengers

Pegasus Airlines will ensure that passengers are informed of the prohibited articles listed in point 5.10.3. before check-in is completed.

The list of the prohibited items is available on check-in counter, self-check-in desks, Pegasus Airlines official website (www.flypgs.com) and by the relevant airport authorities placing posters or notices in advantageous locations.

5.10.3 List of Prohibited Articles

Passengers are not permitted to carry the following articles in their hold baggage:

Explosives and incendiary substances and devices – explosives and incendiary substances and devices capable of being used to cause serious injury or to pose a threat to the safety of aircraft, including:

- ammunition
- blasting caps
- detonators and fuses
- mines, grenades and other explosive military stores
- fireworks and other pyrotechnics
- smoke-generating canisters and smoke-generating cartridges
- dynamite, gunpowder and plastic explosives

End of Section

6 PROCEDURES FOR SCREENING AND HAND-SEARCHING OF CREW, SUPERNUMERARIES, CABIN AND HOLD BAGGAGE

ICAO Annex 17 - 4.2.4:

Each Contracting State shall ensure that background checks are conducted on persons other than passengers granted unescorted access to security restricted areas of the airport prior to granting access to security restricted areas.

6.1 STANDARDS OF SCREENING AND SEARCHING

Persons other than passengers shall be screened by one of the following means:

(a) hand search;

(b) walk-through metal detection (WTMD) equipment;

(c) explosive detection dogs (EDD);

(d) explosive trace detection (ETD) equipment;

(e) security scanners which do not use ionising radiation;

(f) explosive trace detection (ETD) equipment combined with handheld metal detection (HHMD) equipment;

(g) shoe metal detection (SMD) equipment; or

(h) shoe explosive detection (SED) equipment

Items carried by persons other than passengers shall be screened by one of the following means:

(a) hand search;

(b) x-ray equipment;

(c) explosive detection systems (EDS) equipment;

(d) explosive detection dogs;

(e) explosive trace detection (ETD) equipment.

6.2 LOCATION OF SCREENING AND SEARCHING

The basic rule is that all persons other than passengers and all of their cabin baggage or carried items must undergo screening before being permitted to have access to an aircraft or security-restricted area. These procedures will need to be applied to all international flights and domestic flights which connect with them. Hold baggage screening procedures for all persons other than passengers shall be applied as in point 5.10.

6.3 DETAILS OF SCREENING EQUIPMENT

6.3.1 Use of EDD and ETD Equipment as A Primary Method of Screening Persons

The use of explosive detection dogs or ETD equipment is a primary method for screening of persons, as is WTMD or security scanner usage. These shall follow a defined methodology ensuring that persons subject to screening cannot foresee which method will be applied.

6.3.2 Persons Other Than Passengers Passing Through WTMD

Where persons other than passengers have passed through WTMD equipment and did not set off the alarm, between 10% and 20% of those persons shall be subjected to a hand search or be screened by a security scanner, EDD or ETD in order to detect prohibited articles.

6.3.3 Screening of Persons Other Than Passengers by ETD Equipment

The screening of persons other than passengers by ETD equipment shall use samples taken from at least the palms and backs of the person's hands or a personal item recently handled by the person (wallet, purse, passport etc.) and at least one of the following regions on the person's body, namely the outer waistband of the person or the top of the shoes worn.

6.3.4 Frequency of Random Screening

Where persons other than passengers and items carried have to be screened on a continuous random basis, the frequency shall be established by the appropriate authority on the basis of a risk assessment.

6.3.5 Use of X-Ray Equipment

Where x-ray equipment is used:

(a) it shall have threat-image projection (TIP) software installed and employed; or

(b) a hand search shall be used for at least 10% of the items carried or at least 10% of the items carried by the persons other than passengers, selected on a continuous random basis.

6.3.6 Screened Persons Temporarily Leaving Critical Parts

Screened persons other than passengers who temporarily leave critical parts may be exempt from screening on their return provided that they have been under constant observation by authorised persons sufficient to reasonably ensure that they do not introduce prohibited articles into those critical parts.

6.3.7 Prohibited Articles

6.3.7.1 Application

Persons other than passengers shall not be permitted to carry into security restricted areas the articles listed in point 6.3.8.

6.3.7.2 Exemptions

An exemption to point 6.3.7. may be granted on condition that the person is authorised to carry prohibited articles into security restricted areas in order to undertake tasks that are essential for the operation of airport facilities or aircraft, or for performing in-flight duties.

6.3.7.3 Reconciliation of Persons With Articles Carried

In order to allow reconciliation of the person authorised to carry one or more articles as listed in point 6.3.8. with the article carried:

(a) the person shall have an authorisation and shall carry it. The authorisation shall either be indicated on the identification card that grants access to security restricted areas or on a separate declaration in writing. The authorisation shall indicate the article(s) that may be carried, either as a category or as a specific article. If the authorisation is indicated on the identification card, then it shall be recognisable on a need-to-know basis; or

(b) a system shall be in place at the security checkpoint indicating which persons are authorised to carry which article(s), either as a category or as a specific article.

Reconciliation shall be performed before the person is allowed to carry the article(s) concerned into security restricted areas or on board an aircraft.

6.4 PERSONS OTHER THAN PASSENGERS - LIST OF PROHIBITED ARTICLES

(a) guns, firearms and other devices that discharge projectiles — devices capable, or appearing capable, of being used to cause serious injury by discharging a projectile, including:

- firearms of all types, such as pistols, revolvers, rifles, shotguns,

- toy guns, replicas and imitation firearms capable of being mistaken for real weapons,
- component parts of firearms, including telescopic sights,
- compressed air and CO2 guns, such as pistols, pellet guns, rifles and ball bearing guns,
- signal flare pistols and starter pistols,
- bows, cross bows and arrows,
- harpoon guns and spear guns,
- slingshots and catapults;

(b) stunning devices — devices designed specifically to stun or immobilise, including:

- devices for shocking, such as stun guns, tasers and stun batons,
- animal stunners and animal killers,
- disabling and incapacitating chemicals, gases and sprays, such as mace, pepper sprays, capsicum sprays, tear gas, acid sprays and animal repellent sprays;

(c) explosives and incendiary substances and devices —devices capable, or appearing capable, of being used to cause serious injury or to pose a threat to the safety of aircraft, including:

- ammunition,
- blasting caps,
- detonators and fuses,
- replica or imitation explosive devices,
- mines, grenades and other explosive military stores,
- fireworks and other pyrotechnics,
- smoke-generating canisters and smoke-generating cartridges,
- dynamite, gunpowder and plastic explosives.

(d) any other article capable of being used to cause serious injury and which is not commonly used in security restricted areas, e.g. martial arts equipment, swords, sabres, etc.

(e) LAGS carried into the security restricted area or on board an aircraft by persons other than passengers may be exempt from screening.

6.5 STORAGE

Articles as listed in point 6.3.7. may be stored in security restricted areas provided they are kept in secure conditions. Articles as listed in points (c), (d) and (e) of 4.10.3 may be stored in security restricted areas provided they are not accessible to passengers.

Pegasus Airlines responsible persons for storage of prohibited items in security restricted areas are described in PG-GU-PR-043 Procedure for Use of Prohibited Items in Security Restricted Areas only for Sabiha Gökçen, Antalya, İzmir Adnan Menderes, Ankara Esenboğa, Adana, Ercan, Trabzon and Kayseri airports.

6.6 DETAILS OF SERVICE PROVIDER

Inside Türkiye, the Ministry of Internal Affairs is responsible for screening of checked baggage.

Outside Türkiye, responsibility rests with the authority which performs the screening or the security agency personnel contracted by the authority to screen crew, cabin and checked baggage. Depending on the

regulations or risk assessment, Pegasus Airlines can in some airports contract to second and/or if necessary to third parties, via the process described in point 17.2.

End of Section

7 MEASURES FOR PASSENGER AND BAGGAGE RECONCILIATION

Person and baggage reconciliation is a procedure that uses a verifiable tracking system to bring attention to hold baggage that has been loaded or is about to be loaded on a specific flight despite the passenger's failure to board the aircraft concerned. The benefit of this procedure is to positively identify hold baggage that is not properly matched with a passenger or crew member on the specific flight, and to positively identify any passenger who has not boarded the aircraft as well as his or her associated hold baggage.

7.1 PURPOSE OF MEASURES

Pegasus Airlines ensures that hold baggage transported in the aircraft belongs to the passengers travelling on that flight. This requirement is in addition to, and shall be applied irrespective of, other security measures aimed at ensuring that the hold baggage does not contain any explosives or explosive devices.

7.1.1 Document to Be Presented During the Boarding Process

Pegasus Airlines contracted passenger handling services staff shall ensure, during the boarding process, that a passenger presents a valid boarding card or equivalent corresponding to the hold baggage that was checked in.

7.1.2 Document to be Presented During the Check-in Process

7.1.2.1 Domestic Flights

Only the following documents which contain the unique Turkish Republic Identification Card Number and a photo of the holder are acceptable for passenger ID check-in on domestic flights in compliance with security rules:

- ID Card
- Driving License
- Passport and equivalent documents
- Marriage certificate
- IDs given by official institutions or organizations
- Health certificate
- Birth certificate up to one month from the birth date (provided that it is accompanied by the parent's ID).

CAUTION	Turkish National ID Card must contain the photo of the holder if the person is 15 years old and over.

The following travel documents are not acceptable for domestic flights:

- Copy or fax of an ID card
- ID card number printout taken from the Internet
- Copies of acceptable ID and equivalent documents
- Any document which does not state the Turkish Republic Identification Card ID number for Turkish citizens

Turkish Citizens who would like to travel to the Turkish Republic of Northern Cyprus from Türkiye shall be accepted only with their national ID card or passport.

7.1.2.2 International Flights

The Travel Information Manual (TIM) and TIMATIC, where available, will be used as a reference document for Government travel document requirements. The rulings published in the TIM must be considered as final in the event of any dispute.

Presentation of a health certificate is the passenger's responsibility. The health certificate is not checked by Pegasus Airlines, unless the passenger presents it.

It shall not be assumed that a passenger returning to a European country is automatically eligible for re-entry because S/he has a return ticket. Some people enter some European countries on a limited entry visa. Their quota of entries shall be considered.

The right to refuse the travelling of a passenger holding a travel document which uses an unknown language is reserved by Pegasus Airlines.

If the travel document is in an unknown language, these legible details shall be checked:

- Validity
- Expiry date
- Place of issue
- Date of issue
- Passport owner signature

In case of through check-in, all travel documents shall be checked for the final destination and for all transfer points.

Passport Check Points:

- Expiry and validity date
- Matching his/her appearance and date of birth, photograph on the passport (identification of the passenger)
- Nationality: It helps when making decisions about a passenger
- Matching his/her name on the passport and on the ticket: The name shall be the same on the passport and ticket. If there is a surname change, the passenger shall need to present necessary documents (marriage certificate, court verdict etc.). If there are children who are registered on the parent's or the guardian's passport, the matching name of the child on the passport and ticket is mandatory
- If children hold their own passports or other travel documents, matching is mandatory again
- Not being damaged, not being falsified, being clear
- Passport owner signature

Visa Check Points:

- Expiration date: Passenger shall travel between the beginning and ending date of the visa issue date
- Number of entrances
- Single visa: This visa shall be used for just one entrance during the valid period. A single visa shall not be used after it is used . It is recommended that entrance and exit stamps shall be searched.
- Double visa: This visa shall be used for only double entrance during the valid period.
- Multiple visas: There are no limits for the number of entrances during the valid period in this type of visa.
- Total duration of stay may be restricted. Maximum duration of stay shall be observed.
- Type of visa: A visa is arranged that depends on the various intentions. The passenger's route shall be checked according to the intention of the visa.
- Duration of stay
- Name (If there is a name on the visa, it is matched with the one on the passport)
- Whether children are registered on the visa or not.

7.2 DESCRIPTION OF PROCEDURES

Screened cabin baggage placed in the hold of an aircraft during the boarding process due to space constraints on board the aircraft shall continue to be considered as cabin baggage.

Generally, hold baggage shall not be placed on board an aircraft unless:

(a) the hold baggage is properly marked externally to permit reconciliation with the relevant passenger or crew member;

(b) the passenger or crew member to whom the baggage belongs has checked in for the flight on which it is to be carried;

(c) prior to loading, the hold baggage is held in an area of the airport to which only authorized persons have access; and

(d) the hold baggage has been identified as either accompanied or unaccompanied.

To be effective, person and baggage reconciliation procedures shall be specific to the category of person, as follows:

(a) **Originating passengers:** Special attention shall be paid to standby travellers and other last-minute seat assignments, off-airport check-in and individuals who check in as part of a group but may fail to board the aircraft. When passengers travelling together are allowed to share the total baggage allowance, each member of the group shall check his or her baggage individually and be given individual baggage claim checks. Situations involving voluntary or involuntary disembarking prior to aircraft pushback shall also be considered, to ensure proper and complete passenger and baggage reconciliation;

(b) **Transfer or connecting passengers:** The hold baggage of a transfer passenger shall not be loaded unless the passenger has checked in, where required, and boarded the onward flight, and the baggage has been reconciled by the onward aircraft operator. During situations involving increased threat levels, it may be necessary for passengers to physically identify baggage before it is transported. Procedures to reconcile the baggage of passengers shall be defined, especially at hub stations, to ensure the minimum of interference with, or delay to, the activities of the airport and the operators;

(c) **Disembarking transit passengers:** If passengers disembark before reaching their final destination, their hold and cabin baggage shall be removed from the aircraft;

(d) **Crew members:** Typically, flight and cabin crews may deliver their own hold baggage to the aircraft. If crew members check in their hold baggage at an airport check-in counter, procedures similar to those for originating passengers shall apply;

(e) **The number of passengers boarding an aircraft shall be confirmed by the head count.** However, the passenger boarding process shall not be undertaken from the bridge unless measures such as keeping the bridge doors locked or ensuring the presence of an officer during boarding operations at the bridge access points, are applied.

The process of person and baggage reconciliation may be accomplished physically, by using a simple manual or semi-automated system, or by using a sophisticated automated electronic system that provides fast throughput. Airports with high volumes of passenger traffic are advised to employ an automated system. Whichever method is used, there shall be a system of verification, monitoring and inspection to ensure that correct reconciliation is performed. All necessary procedures shall be completed before the aircraft doors are closed. Security and other controls shall be in place so that passengers cannot disembark undetected after boarding and prior to aircraft push-back.

To facilitate effective person and baggage reconciliation, Pegasus Airlines will implement, in addition to baggage reconciliation procedures, appropriate security measures for manual and automated baggage tag stocks, in order to prevent any unauthorized use of baggage tags. This may be achieved by the Ground Operations Director by controlling the stocks from Pegasus Airlines Headquarters.

7.2.1 Physical / Manual Person and Baggage Reconciliation

In reconciling baggage using a physical system, all originating, and transfer baggage shall be personally confirmed by the passengers and/or crew members. The baggage shall be conveyed to the left-hand side of the aircraft and during the boarding process, each person shall be required to identify his or her baggage by pointing it out. Contracted ground handling loading staff may proceed with aircraft loading after each passenger presents the correct baggage claim tags as proof of ownership.

Gate baggage may be taken from passengers at the boarding gate or alongside the aircraft. Such baggage shall be tagged with DCS printed. The screening process is to be the same as cabin baggage.

7.2.2 Details of Equipment If Automated

In reconciling baggage using a manual or semi-automated system, the originating baggage may be processed as follows:

(a) a list is produced by the departure control system showing the baggage tag number of each baggage checked in for the flight; and

(b) the tag number on each baggage is checked against the departure control system list prior to its placement in a container or baggage cart, and a check will take place to ensure the tag number:

(i) appears on the departure control system list, and is ticked to confirm reconciliation and the baggage loaded for the flight; o

(ii) if not on the list, the baggage is set aside for later investigation as to its origin and destination.

Transfer baggage handled by a manual system shall never be loaded before confirming that the baggage belongs to a passenger or crew member who has checked in for the flight. It shall be delivered separately to the aircraft and loaded only after thorough verification by reference to the passenger and baggage manifest.

For gate baggage, each bag shall be tagged, and each tag number recorded on the passenger and baggage manifest on the DCS system, or limited release tag shall be filled for matching tag numbers with passenger and crew member names. If a passenger disembarks from the aircraft before pushback, the baggage reconciliation process, together with the departure control system list, makes it possible to ascertain whether any items shall be removed from the hold.

A fully automated person and baggage reconciliation system uses computer (DCS)-generated bar code tags and wireless laser bar code scanners to read printed baggage tags and is usually linked to external systems such as a departure control system. The system matches all loaded baggage with the passengers and, in addition, tracks baggage location within the airport, at the gate and on the aircraft.

A key component of an automated person and baggage reconciliation system is the capability to ensure that each person who checks in a bag is the same person who boards the aircraft, and not someone who has taken the original passenger's place. To achieve this, a passenger identification document check shall be undertaken at check-in and at the boarding gate.

At check-in, the name on the passenger's passport or other acceptable travel identification document shall be compared with the passenger details recorded for the flight in the electronic document control system, and the photograph on the travel identification document compared to the passenger.

At the boarding gate, the name on the passenger's boarding pass shall once again be compared with the name in the passport or other acceptable travel identification document, and the photograph shall be compared with the passenger. Additionally, the boarding pass shall be checked to ensure that it pertains to the flight being boarded.

Person and baggage reconciliation security measures shall be complemented by baggage check-in procedures. Specifically, passengers shall be queried about their baggage as they check in. Passengers may attempt to check in baggage belonging to other passengers, baggage that does not belong to them, and baggage which they may not have packed themselves or maintained under their supervision. Hold

baggage shall therefore not be accepted for carriage by check-in agents unless the owner of the baggage is present and answers the agent's questions satisfactorily.

7.2.3 Passenger Head Counting

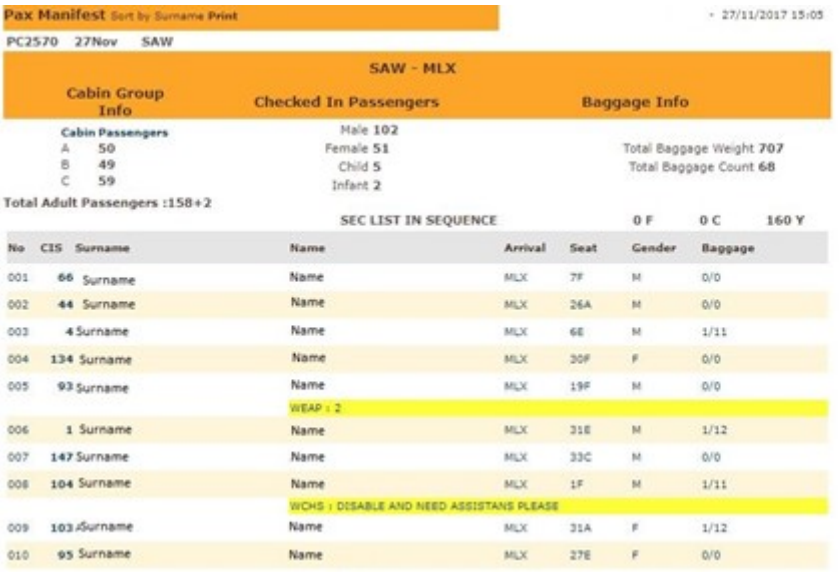
The number of passengers boarding an aircraft shall be confirmed by the head count. However, it may not be done for the passenger boarding process from the bridge. In this case measures such as keeping the bridge doors locked or the presence of an officer during the boarding operation at the bridge access points, shall be applied.

7.2.4 Details of Manifest If Relevant

Pegasus Airlines retains each hold baggage manifest and supporting documentation for not less than 24 hours, or for a time period that may be extended depending on the duration of the flight. Preferably, the manifest must be retained at the airport of departure or a local office of the aircraft operator, but under no circumstances shall the original hold baggage manifest be carried on the flight concerned. A copy may be carried if necessary.

The DCS system used by Pegasus Airlines contains the records of passengers and baggage separately. The following information is contained in the manifest and these records are saved on the DCS system for a minimum of 1 year.

Pegasus Airlines contracted ground handling responsible staff validates and authorizes the baggage manifest prior to pushback.



Pax Manifest Sort by Surname Print

27/11/2017 15:05

PC2570 27Nov SAW

SAW - MLX

Cabin Group Info	Checked In Passengers	Baggage Info
Cabin Passengers A 50 B 49 C 59	Male 102 Female 51 Child 5 Infant 2	Total Baggage Weight 707 Total Baggage Count 68

Total Adult Passengers :158+2

SEC LIST IN SEQUENCE 0 F 0 C 160 Y

No	CIS	Surname	Name	Arrival	Seat	Gender	Baggage
001	66	Surname	Name	MLX	7F	M	0/0
002	44	Surname	Name	MLX	26A	M	0/0
003	4	Surname	Name	MLX	6E	M	1/11
004	134	Surname	Name	MLX	30F	F	0/0
005	93	Surname	Name	MLX	19F	M	0/0
			WEAP : 2				
006	1	Surname	Name	MLX	31E	M	1/12
007	147	Surname	Name	MLX	33C	M	0/0
008	104	Surname	Name	MLX	1F	M	1/11
			WCHS : DISABLE AND NEED ASSISTANS PLEASE				
009	103	Surname	Name	MLX	31A	F	1/12
010	95	Surname	Name	MLX	27E	F	0/0

Figure 7-1: Example of Passenger Manifest

27/Nov/2017 PC2570 SAW - MLX

Number	Surname	Name	Gender	**Pnr_No	**Rez Code	**INBOUND&IT IN	Seat	**Bag SSR Type	P/W	B-ID	**Last Port	Cabin Class
1	Surname	Name	M	VH1Q8P	C1	SAW-M LX	6E	BAG	1/ 11	PC0783430	M LX	Y
2	Surname	Name	M	1JR6RE	F1	SAW-M LX	31E	BAG	1/ 12	PC0782309	M LX	Y
3	Surname	Name	M	248XYJ	I1	SAW-M LX	1F	BAG	1/ 11	PC0782628	M LX	Y
4	Surname	Name	F	2IUWXU	J1	SAW-M LX	31A	BAG	1/ 12	PC0782508	M LX	Y
5	Surname	Name	F	1LM6G9	L1	SAW-M LX	11E	BAG	1/ 14	PC0782380	M LX	Y
6	Surname	Name	M	1WQHTJ	O1	SAW-M LX	29D	BAG	1/ 12	PC0782810	M LX	Y
7	Surname	Name	F	X84KNE	P1	SAW-M LX	5B	BAG	1/ 7	PC0782686	M LX	Y
8	Surname	Name	M	WJVKZR	S1	SAW-M LX	28F	BAG	1/ 10	PC0782428	M LX	Y
9	Surname	Name	F	UKVTNB	T4	SAW-M LX	34C	BAG	1/ 27	PC0784520	M LX	Y

Figure 7-2: Example of Baggage Manifest

7.2.5 Identification of No-Show Passengers

7.2.5.1 Baggage Of Passengers Not On Board The Aircraft

(a) Pegasus Airlines ensures it will identify the hold baggage of passengers who did not board or who left the aircraft before departure, following the procedures described in point 7.2.

(b) If the passenger is not on board the aircraft, the hold baggage corresponding to his boarding card or equivalent must be considered as unaccompanied and the bag shall be offloaded from the aircraft.

7.2.5.2 Factors Beyond The Passenger's Control

7.2.5.2.1 Recording the Reason for Baggage to Become Unaccompanied

The reason that the baggage became unaccompanied shall be recorded before it is loaded onto an aircraft, unless the security controls as referred to in point 7.3. are applied.

7.2.5.2.2 Description of Factors Beyond the Passenger's Control

For the purposes of the transport of unaccompanied hold baggage, the following may be considered as factors beyond the passenger's control:

(a) the passenger was denied boarding (only overbooked cases) and S/he did not volunteer to give up his/her seat; or

(b) the passenger and/or his/her baggage was re-routed onto another flight and it was not at his/her request; or

(c) the baggage failed to transfer between two flights due to unforeseen reasons, causing it to miss the departing flight; or

(d) there was a malfunction of the baggage system, causing the baggage to miss the departing flight; or

(e) the baggage was loaded onto an aircraft other than that for which it was checked in; or

(f) the airline decided not to load or unload a bag for operational reasons and the passenger has not influenced the decision by changing his/her travel itinerary.

WARNING	If the passenger does not get on board his/her transfer flight, that cannot be considered as a factor outside the control of the passenger
WARNING	If the passenger becomes unruly , or she/he is stopped by border control officers or other relevant authorities, or S/he is stopped because of a lack of documents, that cannot be considered as a factor outside the control of the passenger.
CAUTION	In the case of points c) – f), Pegasus Airlines establishes that the passenger did travel on the flight on which S/he was checked in. If the passenger did not travel on the flight on which S/he was checked in, then the baggage shall be subjected to the security controls as referred to in point 7.3.

7.2.5.3 Disembarking / Offloading Passengers

If one or more passengers board the wrong aircraft or voluntarily disembark the aircraft, then the following shall be undertaken:

(a) reconciliation of the remaining passengers and baggage, and

(b) verification that no articles were left in the overhead bins and seat pockets to which the disembarking passengers may have had access, and

(c) the hold baggage of the disembarked passenger shall be offloaded, and

(d) if a suspicious item or situation is detected, the local security authority and Security Department shall be informed, and an aircraft security search shall be conducted prior to the aircraft entering into service, and

(e) cabin crew must fill the PG-GU-FR-009 Passenger Irregularity Report Form.

7.2.5.4 If Passenger Is Denied Carriage

The following procedures are required of the ground handling staff:

(a) Offload the passenger and his baggage in the DCS System. Inform the concerned unit(s)/ department(s).

(b) Document the case with details of the passenger's condition (e.g. intoxicated, general abuse, etc.).

In cases where refusal for carriage has been exercised, inform the GCC (guestcontrol@flypgs.com) by filling the ***PG-GU-FR-009 - Passenger Irregularity Report*** whenever safety / security is concerned.

Pegasus Security Department shall be informed by the GCC.

*See "https://document.flypgs.com" for PG-GU-FR-009 - Passenger Irregularity Report under Security Department>Forms.

The detail with the reasons for denying shall be recorded into the passenger's PNR on DCS where applicable.

7.2.6 Identification of Unaccompanied Baggage

Any baggage that is not transported on the same aircraft as its owner is categorized as unaccompanied baggage and is handled as air cargo.

Hold baggage that becomes unaccompanied baggage due to factors other than those mentioned in point 7.2.5.2. shall be removed from the aircraft and re-screened before loading it again.

Secure storage areas shall have been established where mishandled passenger baggage may be held until forwarded, claimed or disposed of, in accordance with local laws.

- Locked and secure storage cage or room
- Access and key control are properly supervised
- The baggage is subjected to additional screening before being loaded into an aircraft.

7.3 PROCEDURES FOR SCREENING OF UNACCOMPANIED BAGGAGE

Each item of unaccompanied hold baggage shall be accounted for on the hold baggage manifest and each entry on the manifest shall clearly show the baggage status, together with the baggage tag number.

A separate baggage record shall be kept by fulfilling the *PG-GU-FR-058 - Unaccompanied Baggage Security Control Form*, available in Comply365. This form must be kept by the Ground Handling Agent for 48 hours and must be available to the Pilot-in-Command upon request.

7.3.1 Standard of Screening

Unaccompanied hold baggage not covered by point 7.2.5.2. shall be screened by one of the methods laid down in point 5.4.1. and, where applicable, applying additional requirements laid down in 7.3.1.1.

7.3.1.1 Additional Screening Requirements

7.3.1.1.1 Unaccompanied Baggage by a Hand-Search

Where unaccompanied hold baggage is screened by a hand search, it shall be supplemented by the use of explosive trace detection (ETD) equipment.

7.3.1.1.2 Unaccompanied Baggage Screened by X-Ray Equipment

Where unaccompanied hold baggage is screened by x-ray equipment, it shall be examined by the same screener from two different angles with at least 60° and no more than 90° rotation, unless multi-view x-ray is used.

7.3.1.1.3 Unaccompanied Baggage Screened by EDS Equipment

Where unaccompanied hold baggage is screened by EDS equipment, the equipment shall meet at least Standard 2.

7.3.2 Location of Screening

Locations of baggage screening systems may include:

- Terminal areas;
- Security area before check-in;
- Screening in front of check-in;
- Screening devices at or behind check-in;
- Screening downstream in the baggage system.

7.3.3 Details of Screening Equipment

Unless unaccompanied baggage has been previously screened to the required standard and has become separated from its owner as a result of factors clearly beyond the passenger's control, all unaccompanied hold baggage, both originating and transfer, shall be screened by one of the following methods:

(a) EDS;

(b) advanced technology, where the images of all baggage are viewed by an X-ray operator;

(c) conventional X-ray equipment, with each item of baggage viewed from two different angles by the same operator at the same screening checkpoint;

(d) manual search supplemented by the use of ETD equipment on open baggage; or

(e) other methods approved by the appropriate authority, such as a dog team.

7.3.4 Details of Operator or Service Provider

Inside Türkiye, the Ministry of Internal Affairs is responsible for the screening of checked baggage.

Outside Türkiye, responsibility rests with the authority which performs the screening or the security agency personnel contracted by the authority to perform the screening of unaccompanied baggage. Depending on the regulations or risk assessment in some airports, Pegasus Airlines can contract to second and/or if necessary to third parties, via the process described in point 17.2.

Unaccompanied baggage procedures shall be performed by contracted ground handling suppliers.

End of Section

8 SECURITY OF AIRCRAFT

The security of the aircraft is the responsibility of Pegasus Airlines . The primary measure, however, to prevent unauthorized access to aircraft is the safeguard of the landside-airside boundary. The security measures taken in the area immediately around the aircraft are sof paramount importance.

Before departure, an aircraft shall be subjected to an aircraft security check or aircraft security search in order to ensure that no prohibited articles are present on board. An aircraft in transit may be subjected to other appropriate measures.

8.1 PURPOSE OF SECURITY MEASURES

The main purpose of the security measures are to detect prohibited articles and unlawful interferences that jeopardize the security of the aircraft, passengers, crews and all personnel. Measures will be taken as a precaution against theft, espionage or sabotage etc.

8.2 SEARCHES AND CHECKS OF AIRCRAFT

Pegasus Airlines has established and maintains a training programme on security check and search procedures for different aircraft types (Airbus A320, Airbus A321 and Boeing 737) for all relevant staff, including flight and cabin crew. In addition, Pegasus Airlines Aviation Security Department has developed a security procedure checklist for each aircraft type in service and the Chief Flight Operations Officer, EVP - Cabin Operations Managers or related staff shall distribute this to flight crew and relevant staff.

Aircraft Security Searches are thorough inspections of the interior and exterior of aircraft for the purpose of identifying any suspicious objects, weapons, explosives or other dangerous devices, articles or substances. Determination of whether a check or search shall be conducted shall be made in accordance with the results of a security risk assessment carried out by the relevant national authorities. Additionally, aircraft security searches shall be conducted if an aircraft is suspected of being a possible target.

Aircraft Security Checks: Pegasus Airlines do not perform any security checks, only a security search is performed.

CAUTION	All aircraft security searches shall be conducted once when all service providers (caterers, cleaners, duty-free and others) other than those involved in the security function, have left the aircraft or are under surveillance by the cabin crew. Sterility shall be maintained throughout the boarding process and pre-departure.

To be effective, searches shall be carried out in good lighting conditions.

Searchers are looking for something that:

- shall not be there;
- Cannot be readily identified;
- Is out of place;
- Appears to have been concealed.

Searches of high-risk aircraft shall be conducted by trained and competent flight crew and cabin crew or by security personnel, assisted by aircraft crew or aircraft engineering staff.

8.2.1 Search of Aircraft

An aircraft security search means an inspection of the interior and accessible exterior of the aircraft in order to detect prohibited articles and unlawful interferences that jeopardize the security of the aircraft;

In addition to an aircraft security search, prior to the commencement of each international flight and domestic flight a regular search of an aircraft for suspected explosive devices and/or weapons is conducted when an aircraft is put into service following maintenance or after an overnight stop.

8.2.1.1 Standard of Searches

An aircraft security search shall consist of an examination of the following areas, when they are accessible without the use of tools, keys, stairs or other aids, and without breaking seals.

CAUTION	There are two security levels searches laid down, any one of which may be applied to all aircraft in the fleet in given circumstances Class 1 and Class 2 where the implementation for Class 2 is in specific airports. The information on the airports is published by Aviation Security Department Bulletin in Comply365 PG-GU-KB-00014. For details and descriptions of Security Standards (Class 1 – Class 2) please refer to point 14.2.

Pegasus Airlines aircraft service panels and hatches must be sealed if the aircraft is in service depending on the aircraft type, the related service panels and hatches shown on the information card PG-GU-BK-002 Aircraft Security Search Information Card (available in Comply365 and EFB) must be filled by the technician staff. The filled information card is kept in the flight crew compartment area. Detailed sealing procedures are described in PG-GU-PR-044 - Security Seal Supply, Stock and Implementation Procedure available in Comply365 and EFB.

200 seals are available for the in-flight crew compartment cockpit library. If there are not enough seals, then Pegasus Airlines technical staff in the following airports SAW, ADB, AYT and ESB airports' line maintenance offices can provide extra seals.

Pegasus Airlines seals are painted in red with black printing. If the words "OPENED VOID" does not appear horizontally across the seal, this indicates the integrity of the seal. Examples of seals are available in the Comply365 system with the reference PG-GU-BK-003.

While performing the security search the seals on that aircraft must be inspected by the flight crew for signs of tampering. Also, the serial numbers on the checklist must be the same as those present on the seals. If tampering is detected, the related service panel, hatch or area must be inspected, and new seals must be put in place.

If uninterrupted access control cannot be guaranteed and a broken or missing seal(s) has been noted by the flight crew, S/he shall:

- advise IOCC,
- perform a thorough Aircraft Security Search according to point 8.2.1.1.1.,
- if anything suspicious is detected, proceed according to point 14.1.5,
- if nothing suspicious is detected, normal operation can continue,
- the flight crew shall file a report after the event.

8.2.1.1.1 When to Perform and Aircraft Security Search

(a) An aircraft shall at all times be subjected to an Aircraft Security Search whenever there is reason to believe that unauthorised persons may have had access to it.

(b) An aircraft arriving from a country where the security measures are not recognised as equivalent to the standard detailed in ECAC Doc. 30 and Turkish NCASP shall be subjected to an aircraft security search any time after passenger disembarkation from the area to be searched and/or the unloading of the hold.

(c) An aircraft arriving into, or departing from, a part other than a critical part of the aerodrome shall be subjected to an aircraft security search at any time before departure.

(d) An aircraft that was accessible in a part other than a critical part and is then moved into a critical part shall be subjected to an aircraft security search at any time before departure. If the search is carried out before moving the aircraft into a critical part, the areas of the aircraft searched shall be

either sealed, locked or under constant monitoring by persons responsible and trained for protecting aircraft until the aircraft arrives in the critical part. Please see Chapter 8.3.1.2.

8.2.1.1.2 How to Perform and Aircraft Security Search

8.2.1.1.2.1 Presence of Passengers

During the examination of the areas in the cabin of the aircraft, no passengers will be present in the area to be examined, unless the aircraft is in transit.

8.2.1.1.2.2 Presence of Passengers for Aircraft in Transit

Where an aircraft is in transit, the aircraft security search may be performed whilst passengers remain on board provided that:

(a) the passengers are in possession of their cabin baggage when the examination is performed; and

(b) the passengers are under supervision in order to prevent movement through the aircraft when the search is being performed.

CAUTION	In the event of en-route stops where transit passengers remain on board with the intent of continuing their journey, cabin crew members shall ensure that any items left behind by passengers disembarking from such flights and ending their journey are removed from the aircraft, or otherwise dealt with appropriately before departure.

Transit passengers remaining on board must be asked to positively identify their belongings, perhaps by placing them on their laps, while the cabin crew conducts a security search. Transit passengers shall be permitted to leave the aircraft only after such an inspection if, for example, transit passengers are permitted to exit the aircraft to stretch their legs before re-embarking on the aircraft. In addition, a post-flight cabin inspection shall verify that nothing hazardous has been left behind by passengers.

8.2.1.1.2.3 Methods of Examination of an Aircraft

(a) The examination of the areas shall be done by a hand search.

(b) A visual check may be used as an alternative method for the examination of those areas that are empty, such as aircraft hold.

(c) Explosive detection dogs may be used as a supplementary method of examination.

(d) Explosive trace detection (ETD) equipment may be used as a supplementary method of examination.

8.2.1.1.2.4 Areas of an Aircraft to be Examined

An aircraft security search shall consist of an examination of all of the following areas, when they are accessible without the use of tools, keys, stairs or other aids, and without breaking seals:

- overhead bins
- cupboards and storage compartments, including crew storage areas
- toilet compartments
- galley areas
- seat pockets
- areas under seats, between seats and between the seat and the wall
- flight crew compartment, if left unattended
- aircraft hold, unless sealed
- items contained within the hold
- aircraft service panels and service hatches

- wheel wells
- between 5% and 10% of lifejacket pouches (10% in UK flights)

8.2.1.2 Information on the Aircraft Security Search

The following information on the aircraft security search of a departing flight shall be recorded and kept at a point not on the aircraft for the duration of the flight or for 24 hours, whichever is longer:

(a) flight number; and

(b) origin of the previous flight.

Where an aircraft security search was performed, the information shall also include:

(a) date and time that the aircraft security search was completed; and

(b) the name and signature of the person responsible for the performance of the aircraft security search.

Upon completion of an aircraft security search, it shall be recorded via EFB (in compliance with PG-GU-FR-001 - Aircraft Security Search Information Form, available in Comply365 and EFB) by the Pilot-in-Command and stored electronically. In any case where EFB cannot be used, PG-GU-FR-001 - Aircraft Security Search Information Form shall be filled and signed by the Senior Cabin Crew and Pilot-in-Command and handed over to the contracted ground handling personnel. The contracted ground handling personnel shall keep this form for at least a minimum of 24 hours in the departure station with the other related flight documents.

8.2.2 Details of Service Provider

Where an aircraft is in a critical part, the aircraft security search may be performed whilst service providers are on board the aircraft.

Pegasus Airlines flight and cabin crew performs the aircraft security search process.

Depending on the regulations or risk assessment in some airports, Pegasus Airlines can transfer this responsibility by contract to second and/or if necessary to third parties.

8.3 CONTROL OF ACCESS TO AIRCRAFT

To prevent unauthorized access, aircraft in security restricted areas shall be monitored while undergoing preparation for service, maintenance, cleaning, etc. Aircraft crew, ground staff and maintenance personnel servicing the aircraft must challenge any unauthorized or unrecognized persons approaching or attempting to gain access to an aircraft and confirm their legitimacy. Unauthorized persons must be reported to superiors or to law enforcement officers and to the Pegasus Airlines Aviation Security Department without any delay.

Aircraft undergoing maintenance, when left unattended by authorized personnel, or not in operation shall have all the access points secured, with stairs stowed or removed and loading platforms retracted. Stairs left near aircraft shall be immobilized. Tamper-evident stick-on security seals shall be used on panels and doors to make any unauthorized access evident during pre-departure checks.

Aircraft in service shall be kept under sufficient surveillance by technical, flight or cabin crew and ground handling staff, in order to detect unauthorized access. If greater security is considered necessary for a specific aircraft, security personnel will control access to the aircraft and its general vicinity and must assume responsibility for the aircraft's security.

Pegasus Airlines will ensure that persons working at airports under its control in a security-restricted area shall display a valid Aviation Security Identification Card issued by the relevant airport operator or another approved authority.

Prior to the first flight of the flight crew on an aircraft during a duty period or on an aircraft after it has been left unattended by the flight crew, the flight crew shall ensure the availability, accessibility and serviceability of the aircraft flight crew compartment systems and emergency equipment. This includes interior pre-flight inspection of systems and equipment, is to be conducted by the flight crew prior to the first flight.

Where a new flight crew has assumed control of the aircraft cabin or after an aircraft has been left unattended by a flight crew or cabin crew; then the flight crew or cabin crew onboard shall ensure the availability, accessibility and serviceability of the aircraft cabin emergency systems and equipment. This procedure includes a pre-flight inspection of such systems and equipment which, as a minimum, shall be conducted by the flight crew or, if applicable, delegated to the cabin crew prior to the first flight.

8.3.1 Standard of Access Control

8.3.1.1 Protection Measures

Regardless of where an aircraft is parked at an airport, each of its external doors will be protected against unauthorised access by:

(a) ensuring that persons seeking to gain unauthorised access are challenged promptly; or

(b) having the external doors closed. Where the aircraft is in a critical part, external doors that are not accessible by a person from the ground shall be considered closed if access aids have been removed and placed sufficiently far from the aircraft as to reasonably prevent access by a person; or

(c) having electronic means which will immediately detect unauthorised access; or

(d) having an electronic airport identification card access system at all doors leading directly to the passenger boarding bridge, adjacent to an open aircraft door, which only allows access for persons that are trained in accordance with PG-GU-EK-002 Security Training Programme (available in Comply365). Such persons must ensure that unauthorised access is prevented during their use of the door; and

(e) being parked, wherever possible, away from the perimeter fence or other easily penetrable barriers and in well-illuminated areas.

8.3.1.2 Aircraft Parked in Hangar

Point 8.3.1. may not be applied to an aircraft parked in a hangar that is locked or otherwise protected from unauthorised access.

8.3.1.3 Additional Protection of Aircraft With Closed External Doors in a Part Other Than a Critical Part

8.3.1.3.1 Measures for External Doors

Where external doors are closed and the aircraft is in a part other than a critical part, each external door shall also:

(a) have access aids removed; or

(b) be sealed; or

(c) be locked; or

(d) be monitored.

Point a) shall not apply for a door that is accessible from the ground by a person.

8.3.1.3.2 Access Aids Removed

Where access aids are removed for doors that are not accessible by a person from the ground, they shall be placed sufficiently far from the aircraft as to reasonably prevent access.

8.3.1.3.3 External Doors Locked

Where external doors are locked, only persons with an operational need shall be able to unlock these doors.

8.3.1.3.4 External Doors Monitored

Where external doors are monitored, the monitoring shall ensure that unauthorised access to the aircraft is immediately detected.

8.3.1.3.5 External Doors Sealed

The use of seals to the external doors on special airports is published by the Aviation Security Department according to the assessed risk analysis via the bulletin PG-GU-KB-00014 - Additional Security And Class 2 Security Level Implementation, available in Comply365 and Pegasus EFB Application. Sealing implementation is also performed in the following circumstances;

- Required by Airport Authorities,
- VIP flights,
- Received threat or suspicious condition,
- Pilot-in-Command decision (insufficient security of the airport)

CAUTION	The sealing of external doors is not the same implementation as the sealing of hatches/ panels of aircraft in service for a security search as detailed in point 8.2.1.1.

When external doors are sealed:

(a) The seals shall be tamper-evident, individually numbered and controlled; and

(b) Seal numbers shall be recorded on PG-GU-FR-005 Layover/Overnight Sealing Form - Boeing, PG-GU-FR-006 Layover/Overnight Sealing Form - A320 or , PG-GU-FR-057 Layover/Overnight Sealing Form - A321 (all available in Comply365 and Pegasus EFB Application, Class 1 or Class 2 depending on the published security level) according to the related areas by the flight crew and kept in the station file by the Ground Operations staff. The filled form shall be handed over for the flight crew of the next flight.

(c) Prior to accessing the aircraft, the seals and seal numbers shall be inspected for signs of tampering. If tampering is detected or suspected, the relevant parts of the aircraft shall be subjected to an aircraft security search before boarding or loading.

(d) The related aircraft sealing forms are available in the flight crew compartment.

Where external doors are sealed, and the aircraft is then moved into a critical part, these requirements shall also apply in the critical part.

8.3.1.4 Details of Service Provider

Where an aircraft is in a critical part, the aircraft security search may be performed whilst service providers are on board the aircraft.

Pegasus Airlines flight and cabin crew performs the aircraft access control while the aircraft is in service. If the aircraft is under maintenance Technic staff will perform the access control. During turn-around, if the crews are changing the operational ground staff has the responsibility of access control of the aircraft.

Also depending on the regulations or risk assessment in some airports, Pegasus Airlines can pass on responsibility by contract to second and/or if necessary to third parties, via the process described in point 17.2.

8.4 SECURING THE FLIGHT CREW COMPARTMENT

All Pegasus Airlines aircrafts flight crew compartments are equipped with a flight crew compartment door; this door can be locked and means can be provided by which the cabin crew can discreetly notify the flight

crew in the event of suspicious activity or security breaches in the cabin. The Pilot -in-Command defines the code words used by cabin crew members to alert the flight crew of potential danger for each flight.

The approved flight crew compartment door is designed to resist penetration by small arms fire and grenade shrapnel and to resist forcible intrusions by unauthorized persons. This door can be locked and unlocked from either pilot's station.

(a) This door can be closed and locked from the time all external doors are closed following embarkation until any such door is opened for disembarkation, except when necessary to permit coming and going by authorized persons; and

(b) means can be provided for monitoring from either pilot's station the entire door area outside the flight crew compartment to identify persons requesting entry and to detect suspicious behavior or potential threat.

8.4.1 Pegasus Airlines Flight Crew Compartment Access Door Procedures

Flight crew compartment access is granted by the viewer, or the camera system installed.

Before the flight the Flight Crew Compartment door shall be closed and locked before boarding and the flight and cabin crew communication shall be undertaken via the interphone. In case of any mandatory situation of entrance to the Flight Crew Compartment during the boarding for example by the Operational Staff (Supervisor, Ramp Agent etc.) the entrance request will be forwarded to the Flight Crew via the interphone after confirming that there is no risky situation by the Senior Cabin Crew. The door will be locked during the conversation in the Flight Crew Compartment When the conversation is completed, the flight crew will call the cabin crew via the interphone and then a safe exit will be provided.

Pegasus Airlines policy for the Flight Crew Compartment door is to be kept locked during the entire flight, even during positioning flights. In Flight the Flight Crew Compartment Door shall not be opened if there is no urgent need. Whenever the Flight Crew Compartment door is opened, existing security precautions shall be fully applied.

Following any communication, if entry to the Flight Crew Compartment is required, it will be subject to the following conditions:

Table 8-1: Entry/Exit Procedure to the Flight Crew Compartment

FOR AIRCRAFT EQUIPPED WITH SURVEILLANCE CAMERA	
1.	Turn on the camera (if closed) when the chime is heard.
2.	Communicate and identify the person who performed the chime via SVC.
3.	Unlock the door
FOR AIRCRAFT NOT EQUIPPED WITH SURVEILLANCE CAMERA (ALTERNATIVE PROCEDURE FOR AIRCRAFT EQUIPPED WITH SURVEILLANCE CAMERA)	
1.	The SCCM/CCM will call the Flight Crew Compartment via the interphone and notify the flight crew that they are about to enter by giving the pre-determined CODE which has been agreed during the flight and in the cabin crew briefing prior to the flight; the door will be opened after the pre-determined code is confirmed by the flight crew.
2.	If the agreed CODE is not passed correctly, or if there is any hesitation, uncertainty, nervousness or doubt evident from the SCCM/CCM, the flight crew SHALL NOT allow entry until the inconsistencies have been resolved. The pilot doing the monitoring will stand up and check visually through the cockpit door viewer for evidence of unusual or suspicious activity. If clear, the Pilot-in-Command shall contact the SCCM on the interphone to receive the agreed CODE, to establish the reason for the previous uncertainty and to positively confirm that the cabin is secure. When the Pilot-in-Command is absolutely satisfied that there is nothing suspicious, then he will allow entry by using the appropriate switch.

3.	Before opening the Flight Crew Compartment door, the SCCM draws the corridor curtains shut and ensures galley security by placing a trolley in front of the drawn curtain. The Cabin crew will ensure the galley security as long as the SCCM is inside the cockpit.

CAUTION	**After Flight,** the Flight Crew Compartment door shall be kept locked until the last passenger has disembarked from the aircraft.

The Flight Crew Compartment door access code is updated by the Executive Senior Vice President – Technical Department in Pegasus Airlines fleet. Until the complete update, the old or the new access code will be active. The new access code is not registered in any electronic media other than Pegasus EFB Application. The flight crew shall inform the cabin crew verbally during the flight and the cabin crew briefing about the new access code. Flight Crews are informed via a bulletin published in Pegasus EFB Application when the updating process starts and when it is completed. Pilots shall not share the password in any electronic medium.

NOTE	The update of the flight crew compartment door passwords will be performed according to PG-GU-PR-002 Cockpit Door Password Creation, Distribution and Update Procedure, available in Comply365.

8.5 SECURING OF THE AIRCRAFT

In order to prevent the introduction of unauthorized weapons, explosives or other dangerous devices or items on board by persons other than passengers, the aircraft shall be secured prior to any overnight/ layover. This will be completed by the technician or flight crew, following completion of the Ground Handling and Servicing functions, including cabin cleaning. The Flight crew or responsible technicians perform security controls according to PG-GU-FR-004 - Layover Night Stop Form, available in Comply365. The completed checklist must be held for 48 hours by the technical department or in trip file at the overnight/layover station.

In the event that a technician is not on duty to carry out the overnight checklist, the Pilot-in-Command will be responsible for the completion of the overnight / layover checklist which must be held for 48 hours in the Flight Envelope.

- For aircraft parked remotely from a loading bridge:
  - Closing all exterior doors and exterior hatches of the aircraft;
  - Removing all stairs;
  - Ensuring no portable stairs, lift devices or passenger transfer vehicles are in the immediate vicinity of the aircraft.
- For aircraft parked with access to a loading bridge:
  - Closing all exterior hatches of the aircraft;
  - Closing all exterior doors of the aircraft not served by a bridge;
  - Locking the door between the terminal and the bridge;
  - Ensuring no portable stairs, lift devices or passenger transfer vehicles are in the immediate vicinity of the aircraft;
  - Locking or keeping under constant surveillance doors that provide access to the bridge from the apron or retracting the bridgehead from the aircraft and deactivating the bridgehead positioning controls.

End of Section

9 SECURITY OF AIRLINE CATERING, STORES AND SUPPLIES

For the purpose of this chapter, 'in-flight supplies' means all items intended to be taken on board an aircraft for use, consumption or purchase by passengers or crew during a flight, other than: a. cabin baggage; and b. items carried by persons other than passengers; and c. air carrier mail and air carrier materials.

For the purpose of this chapter, 'regulated supplier of in-flight supplies' means a supplier whose procedures meet common security rules and standards sufficient to allow delivery of in-flight supplies directly to the aircraft.

For the purpose of this chapter, 'known supplier of in-flight supplies' means a supplier whose procedures meet common security rules and standards sufficient to allow delivery of in-flight supplies to an air carrier or regulated supplier, but not directly to the aircraft.

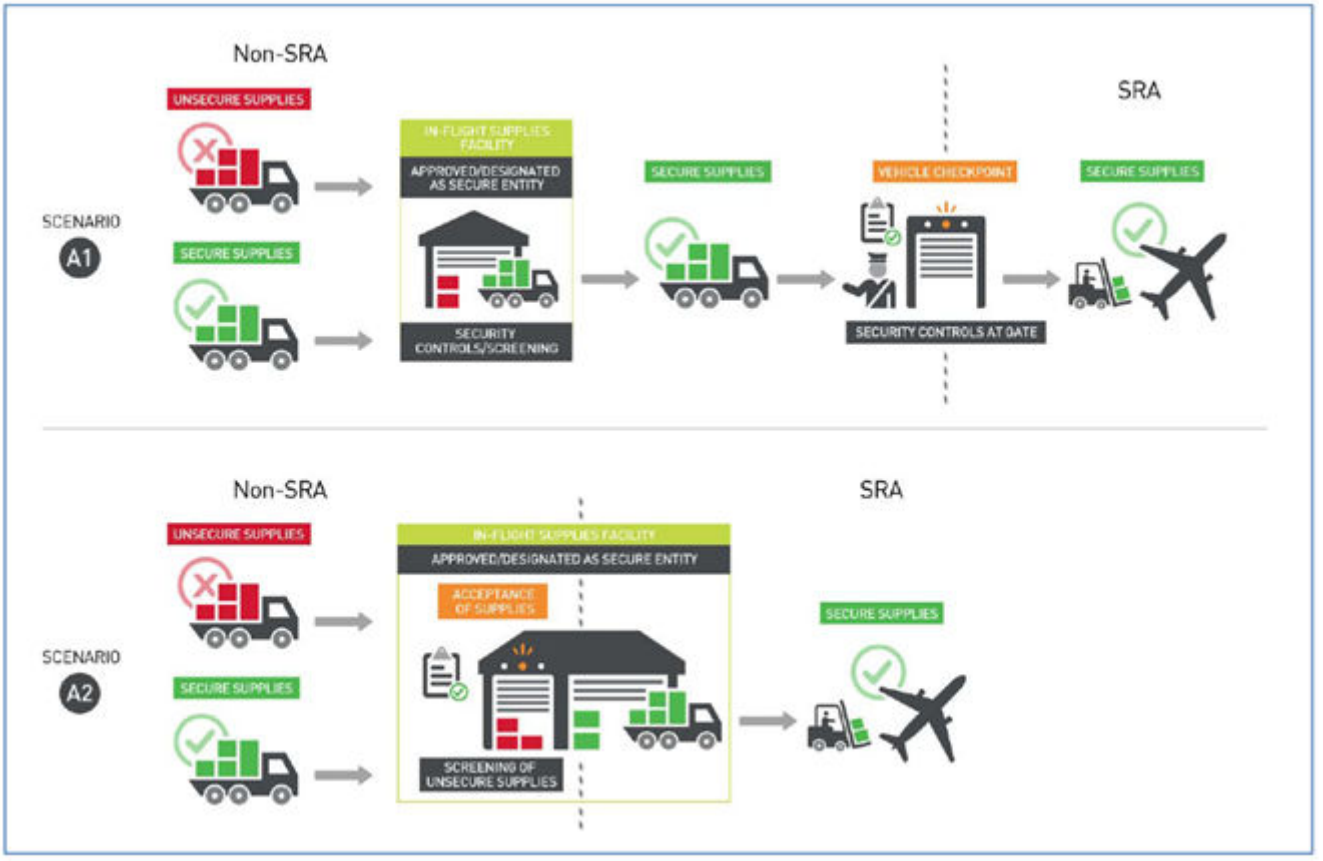


Figure 9-1: Security Control Process for Secure In-Flight Supplies Through a Supply Chain Scenarios

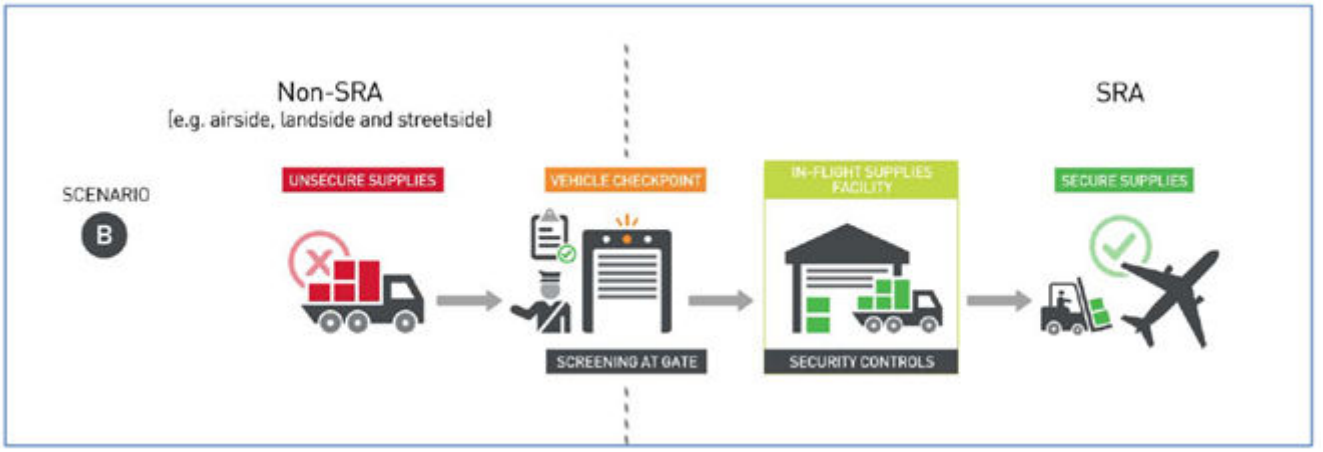


Figure 9-2: Security Control Process for Unsecure In-Flight Supplies - Scenario 1

Figure 9-3: Security Control Process for Unsecure In-Flight Supplies - Scenario 2

9.1 PURPOSE OF MEASURES

Stores and supplies intended for carriage on passenger flights may provide a means to introduce weapons, explosives or other restricted articles or dangerous devices on board an aircraft. Therefore, security controls shall be implemented to ensure that such stores and supplies, including catering and cleaning stores and supplies, do not include restricted articles that could endanger the safety of passengers, crew and aircraft.

The security measures described below shall be implemented by the aircraft catering companies contracted by Pegasus Airlines, to prevent the introduction of weapons, explosives or other restricted articles on board an aircraft through catering and cleaning stores and supplies.

In-flight supplies shall be screened before being taken into a security restricted area, unless:

(a) the required security controls have been applied to the supplies by an airline that delivers these to its own aircraft and the supplies have been protected from unauthorised interference from the time that these controls were applied until delivery at the aircraft; or

(b) the required security controls have been applied to the supplies by a regulated supplier and the supplies have been protected from unauthorised interference from the time that these controls were applied until arrival at the security restricted area or, where applicable, until delivery to the air carrier or another regulated supplier; or

(c) the required security controls have been applied to the supplies by a known supplier and the supplies have been protected from unauthorised interference from the time that these controls were applied until delivery to the air carrier or regulated supplier.

Pegasus Airlines Aviation Security Department shall be ensured during audits that service providers of in-flight supplies have the procedures in place to ensure pre-employment and recurring background checks in accordance with applicable national requirements. This shall apply to all personnel having unescorted access to in-flight supplies.

9.2 DESCRIPTION OF MEASURES AT SUPPLIER'S UNIT

Regulated suppliers shall be approved by the appropriate authority.

Any entity that ensures the security controls as referred to in this point and delivers inflight supplies directly to aircraft, shall be approved as a regulated supplier.

Any entity ('the supplier') that ensures the security controls as referred to in point 9.2.1.4. and delivers in-flight supplies, but not directly to the aircraft, shall be designated as a known supplier by the operator or the entity to whom it delivers ('the designating entity'). This shall not apply to a regulated supplier.

9.2.1 Standard of Physical Security of Premises

Obligations of Pegasus Airlines regulated suppliers and known suppliers:

An air carrier, a regulated supplier and a known supplier of in-flight supplies shall:

(a) appoint a person responsible for security in the company; and

(b) ensure that persons with access to in-flight supplies receive general security awareness training in accordance with PG-GU-EK-002 Security Training Programme (available in Comply365) before being given access to these supplies; and

(c) prevent unauthorised access to its premises and in-flight supplies; and

(d) reasonably ensure that no prohibited articles are concealed in inflight supplies; and

(e) apply tamper-evident seals to, or physically protect, all vehicles and/or containers that transport in-flight supplies.

Point e) shall not apply during airside transportation.

9.2.1.1 Use of Another Company for Transporting Supplies

If a known supplier uses another company that is not a known supplier to Pegasus Airlines or a regulated supplier for transporting supplies, the known supplier shall ensure that all security controls listed in point 9.2.1.4 are adhered to.

9.2.1.2 Additional Obligations of Air Carriers and Regulated Suppliers

Pegasus Airlines and the contracted regulated supplier of in-flight supplies shall:

(a) screen those supplies in accordance with points 9.2.1.4 to 9.2.1.9. when receiving supplies from a company that is not a regulated supplier or known supplier; and

(b) ensure that persons with access to in-flight supplies are subjected to a pre-employment check in accordance with PG-GU-EK-002 Security Training Programme; and

(c) ensure that persons implementing, or responsible for implementing, security controls are recruited, trained and certified in accordance with PG-GU-EK-002 Security Training Programme.

9.2.1.3 Selection of Appropriate Screening Methods

When screening in-flight supplies, the methods employed shall take into consideration the nature of the supplies and shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the supplies.

9.2.1.4 Methods of Screening

The following means or method of screening, either individually or in combination, shall be applied:

(a) visual check;

(b) hand search;

(c) x-ray equipment;

(d) EDS equipment;

(e) ETD equipment in combination with point a);

(f) explosive detection dogs in combination with point a).

Where the screener cannot determine whether or not the item contains any prohibited articles, it shall be rejected or re-screened to the screener's satisfaction.

9.2.1.5 Screening Methods - Visual Checks

A visual check shall consist of a thorough visual check of the supplies and shall only be allowed:

(a) in combination with other methods; or

(b) where all parts of the supplies can actually be seen, with or without aids; or

(c) where supplies are of a nature that makes the concealment of prohibited articles impossible; or

(d) where ETD or EDD is not available and the size, weight or nature of the in-flight supplies does not permit the use of x-ray equipment, EDS equipment or a hand search. In this case the visual check shall include a careful examination of the packaging for signs of tampering and where items are consolidated, each individual item shall be checked.

9.2.1.6 Screening Methods - Hand Search

A hand search shall consist of a thorough manual check of the supplies.

9.2.1.7 Screening Methods - EDS

When an explosive detection system is used the screener shall view all images.

9.2.1.8 Unpredictable Security Measures

The following method shall apply to screening as required by point 9.2.1.4.: at least 25% of all vehicles or persons delivering in-flight supplies shall be selected on a continuous random basis.

From the supplies carried by the selected vehicle or person a representative sample of at least 25% shall be further selected in an unpredictable manner for screening.

The unpredictable selection shall follow a defined methodology ensuring that persons delivering in-flight supplies cannot foresee which supplies will be screened.

9.2.1.9 Alternative to Screening

As an alternative to screening upon access to security restricted areas, in-flight supplies selected for screening in accordance with point 9.2.1.8. may be escorted to the point of unloading and subject to screening during or after unloading. Until screening is completed, in-flight supplies shall be under constant supervision by security personnel trained in accordance with PG-GU-EK-002 Security Training Programme or ECAC Doc. 30.

9.2.2 Standard of Access Control to Premises

The premises used for preparing and storing aircraft operator catering or cleaning supplies intended for carriage on board an aircraft shall be secured at all times against unauthorized access. Such security may be achieved by implementing appropriate access control measures and procedures, which may include a permit identification system and/or electronic card access.

In addition, openings such as windows, loading and unloading docks shall be kept secure with suitable locking devices and/or bars.

If an aircraft catering or cleaning establishment is located within a security restricted area, all airside security requirements shall be met. If the establishment is located outside the airport perimeter, supplies shall be transported to the aircraft in locked or sealed vehicles.

9.3 DESCRIPTION OF MEASURES FOR DESPATCH AND TRANSPORTATION

Catering companies that utilize forward kitchens or storage areas located within airport security restricted areas and cleaning companies that use storage areas within security restricted areas, shall ensure that their facilities, as well as the transport of supplies from off-airport sites, meet the same security requirements that apply to the delivery of stores from landside preparation and storage buildings to the aircraft.

All deliveries of raw materials and equipment to premises used for the preparation or processing of catering stores and supplies shall be appropriately broken down prior to the preparation process to ensure that they do not contain any restricted articles and shall then be held in secure conditions. Deliveries that cannot be broken down, such as audio headsets, amenity or first aid kits, blankets in bulk, and bottles of mineral water, shall be sealed or made tamper-evident by the vendor or supplier of the goods.

Aircraft catering and cleaning companies shall have written agreements with suppliers that cover security aspects, and shall periodically verify, through quality control measures, that these agreements are upheld by suppliers.

If there is any sign of interference or tampering with deliveries of stores or supplies, the catering or cleaning company shall conduct a manual search of the goods to confirm that they do not contain restricted articles.

Preparers of catering products, including those assembling carts and containers, shall be kept under surveillance to deter the placement of any restricted articles within stores or supplies.

Chilling rooms and refrigerators containing prepared meals and catering carts or containers shall be kept secure whenever immediate access is not required, and access shall be controlled at all other times.

Appropriate documentation detailing the nature of catering stores and supplies, the aircraft operator, flight number, date and destination and, whenever appropriate, the seal numbers, shall be issued for each consignment of aircraft stores and supplies.

9.3.1 Standard of Access Control to Prepared Meals

If seals are used to secure carts and vehicles used for storing and transporting stores and supplies intended for carriage on an aircraft, aircraft catering and cleaning companies shall only use seals that are tamper proof and numbered. In order to prevent any unauthorized use of such seals, proper stock control and auditing procedures shall be instituted.

If any doubt arises regarding potential misuse of the seals or if the integrity of the seal stock is compromised, the catering company shall proceed to remove all seals used on catering carts and vehicles intended for transport on an aircraft, and thoroughly search the catering carts and vehicles from which seals have been removed.

Additionally, all seals from the suspected compromised stock shall be removed from storage and destroyed, in order to prevent their reintroduction into the catering company security system.

Before closing a catering cart or container for dispatch to an aircraft, the cart or container and its contents shall be checked by a designated person, to the extent permitted by local laws and hygiene standards, to ensure that it does not contain any restricted articles and has not been tampered with. Immediately on completion of a check, catering carts or containers shall be secured using tamper-evident seals.

The person designated to carry out a security check shall note its completion on the delivery documentation, either the delivery note, vehicle dispatch documentation or aircraft operator catering order, and sign the documentation.

Immediately prior to loading, vehicle storage compartments shall be checked by a person designated by the aircraft caterer, other than the driver or other vehicle crew, to ensure that no unauthorized persons or restricted articles are inside. Once loaded, vehicle compartments shall be appropriately secured.

Seals used to secure vehicles, catering carts and containers shall be held under secure conditions and affixed by the person designated to carry out the security check. The relevant seal numbers shall be annotated on the vehicle dispatch documentation.

Seals on delivery vehicles shall be checked against appropriate documentation, such as vehicle dispatch documentation, by the airport authority at the designated entrance to an airport security restricted area, and by the aircraft operator on delivery at an aircraft. If there is any discrepancy with the accompanying documentation that cannot be resolved, or any signs of interference with the seals, the load shall be regarded as unsecure and shall not be taken into security restricted areas or loaded on board an aircraft.

If seals are used on delivery vehicles when delivering multiple loads for different locations within airport sterile areas, they shall be broken by the driver at the first delivery point or at the entrance to a security restricted area.

For subsequent deliveries detailed for that load within the security restricted area, the vehicle need not be re-sealed, but the vehicle crew shall ensure that the storage compartment remains secure and/or supervised at all times.

9.3.2 Standard of Access Control to Dispatch Bank

Catering stores and supplies may be transported either by the catering company or a haulier whose security measures and operating procedures have been approved by the catering company and the aircraft operator. Any vehicles supplied by companies located outside the security restricted areas and used for transporting catering or cleaning stores and supplies to and from an aircraft shall be locked or sealed to prevent unauthorized access. If signs of interference are found, the aircraft operator shall be notified.

9.3.3 Standard of Access Control to Vehicles

The security of catering and cleaning stores and supplies shall be maintained during transfer from a company's premises to the aircraft.

Delivery vehicles shall not normally be left unattended. However, if this is unavoidable, catering companies shall ensure protection through the use of specific measures such as numbered seals. Details of such measures, including record-keeping procedures for the use of seals, shall be clearly described in the company security programmes.

Cleaning company vehicles shall be checked by drivers for any signs of tampering if they have been left unattended. Drivers shall notify the aircraft operator of any evidence of interference and all cleaning supplies to be taken on board an aircraft shall be checked to ensure that no dangerous devices, articles or substances are concealed in such supplies.

9.3.4 Receipt of Stores and Supplies

Aircraft operators shall check the identity of the vehicle crew by referring to their identification permits.

Additionally, after deliveries of catering or cleaning supplies, the aircraft operator crew shall check the delivered goods on a random basis to ensure that they do not contain any dangerous devices, articles or substances and, if sealed, that there is no sign of interference.

Any consignment of catering stores or supplies showing evidence of unauthorized interference shall be regarded as unsecure and shall be either manually searched to ensure that it does not contain any dangerous devices, articles or substances, or removed from the aircraft. All irregularities shall be immediately reported to the aircraft operator.

Supplies from a company that does not comply with the security measures described above shall not be taken on board an aircraft unless a full inspection of the supplies is conducted.

9.4 CHECKING OF CATERING SUPPLIES BY CABIN CREW

9.4.1 Verification of Catering Supplies

All catering trolleys shall be received as sealed units upon loading onto the aircraft.

The Cabin Crew shall verify the seal numbers by matching them with the numbers listed on the electronic freight bill.

Additionally, the cabin crew shall physically inspect each seal for any signs of tampering, which include at least:

- Broken seals and,
- Improperly affixed seals, including those that appear manipulated, or damaged.

Accepted trolley units are exempted from a security search during the pre-flight security search as described in Chapter 8.2.1 of the ACSP.

9.4.2 Handling of Irregularities

If any evidence of unauthorized interference or tampering is detected on the seals, the issue shall be reported immediately to the Senior Cabin Crew.

In such cases, the catering consignment shall be regarded as unsecure and the supplies shall be subject to a thorough security search before acceptance and/or during the pre-flight security search.

Any irregularities in the catering supplies acceptance shall be reported as a Security Report via the IQSMS system.

End of Section

10 SECURITY OF AIRCRAFT CLEANING OPERATIONS

To prevent unauthorized access, aircraft in security restricted areas shall be monitored while undergoing preparation for service, maintenance, cleaning, etc. Aircraft crew, ground staff and maintenance personnel servicing aircraft shall challenge any unauthorized or unrecognized persons approaching or attempting to gain access to an aircraft and confirm their legitimacy. Unauthorized persons shall be reported to superiors or law enforcement officers.

10.1 PURPOSE OF MEASURES

Stores and supplies intended for carriage on passenger flights may provide a means to introduce weapons, explosives or other restricted articles or dangerous devices on board an aircraft. Therefore, security controls shall be implemented to ensure that cleaning stores and supplies do not include restricted articles that could endanger the security of passengers, crew and aircraft.

10.2 DESCRIPTION OF MEASURES

Pegasus Airlines requires its aircraft catering and cleaning companies to implement security measures and best practices common within the civil aviation industry, to ensure that their operations are not used as a means to commit an act of unlawful interference. In this regard, aircraft catering and cleaning companies shall be requested to establish a security programme consistent with their operations, which shall be approved by the appropriate authority.

10.2.1 Standard of Access Control to Cleaning Stores

The premises used for preparing and storing aircraft operator cleaning supplies intended for carriage on board an aircraft shall be secured at all times against unauthorized access. Such security may be achieved by implementing appropriate access control measures and procedures, which may include a permit identification system and/or electronic card access.

In addition, openings such as windows, loading and unloading docks shall be kept secure with suitable locking devices and/or bars.

If an aircraft cleaning establishment is located within a security restricted area, all airside security requirements shall be met.

Pegasus Airlines ensures that persons with access to cleaning operations are subjected to a pre-employment check-in and trained in accordance with PG-GU-EK-002 - Security Training Programme (available in Comply365).

End of Section

11 SECURITY OF CARGO, COURIER, EXPRESS PARCELS AND MAIL

Pegasus Airlines carry cargo, courier or express parcels if the cargo terminal security measures are implemented in accordance with requirements established under the appropriate civil aviation security programme and with the standards as described below and in the Pegasus Airlines Cargo Operations Manual. All cargo, courier and express parcels shall be subjected to the security controls detailed hereunder before being placed on board the aircraft.

Cargo (Revenue or non-revenue) for transport on Pegasus Airlines Aircraft shall be protected from unauthorized interference from the point of acceptance after screening or security controls have been applied until arrival at the airport of destination. Such protection shall be provided at all times when the cargo is in the custody of personnel performing cargo and ground handling operational functions.

NOTE	Pegasus Airlines is certified as ACC3 Carrier. All information about ACC3 implementation is defined in PG-GU-EK-003 - ACC3 Security Programme, available in Comply365. Please contact security@flypgs.com.

11.1 PURPOSE OF MEASURES

Air cargo and mail has unique characteristics and, in order to ensure their security and the security of the people and infrastructure involved, particular security requirements must be met and appropriate controls put in place.

Consignors of freight, postal authorities and commercial couriers must do their utmost to ensure that no items that may jeopardize the security and safety of the flight are included in consignments (other than those that are carried in accordance with the applicable safety rules and dangerous goods regulations) that are for loading on a Pegasus Airlines aircraft.

11.2 DESCRIPTION OF MEASURES FOR CARGO

Air cargo and mail operations face two main threats, namely:

(a) placement of an improvised explosive device (IED) in cargo or mail to be loaded onto an aircraft; and

(b) use of all-cargo aircraft as a means of attacking a ground-based target through the unlawful seizure of the aircraft.

In the context of air cargo and mail security and, in particular, in view of past attacks on commercial aviation committed by concealing an IED in a consignment, it is essential to remain vigilant to ensure that cargo and mail are not used to commit acts of unlawful interference against civil aviation. Cargo and mail may be perceived as a potential medium of attack because:

(a) the environment in which the air cargo and mail industry operates is growing and is becoming increasingly complex;

(b) the capacity of the industry to respond to this growth and complexity is challenged by the presence of multiple actors who handle air cargo and mail entering and exiting the supply chain;

(c) security measures that are applied to cargo and mail vary among States and are often based on risk assessments conducted by national authorities, resulting in differing approaches to implementation. This creates potential vulnerabilities in the air cargo supply chain and difficulties for aircraft operators having to implement different standards; and

(d) awareness of the vulnerabilities of the air cargo supply chain is increasing, as a result of information disseminated by terrorists and the media.

11.2.1 EU and UK ACC3 Stations

Pegasus Airlines is certified as an ACC3 Carrier in SAW, ESB, ADB and AYT Airports.

All information about ACC3 implementation, including the details required under Attachment 6-G of Regulation (EU) 2015/1998 and the UK NASP for each station, are defined in PG-GU-EK-003 - ACC3 Security Programme, available in Comply365. The ACC3 Security Programme is submitted for approval to the LBA and the UK DfT, which are respectively the relevant authorities for EU and UK ACC3 Designation. For the purpose of regulatory compliance, the ACC3 Security Programme shall be considered as an annex to this Air Carrier Security Programme.

11.2.2 Procedures for Acceptance

Regulated agents, known consignors, account consignors and aircraft operators are the key entities involved in an air cargo secure supply chain system. The figure below illustrates the flow of cargo through a secure supply chain until it is loaded onto a commercial aircraft for transport by air.

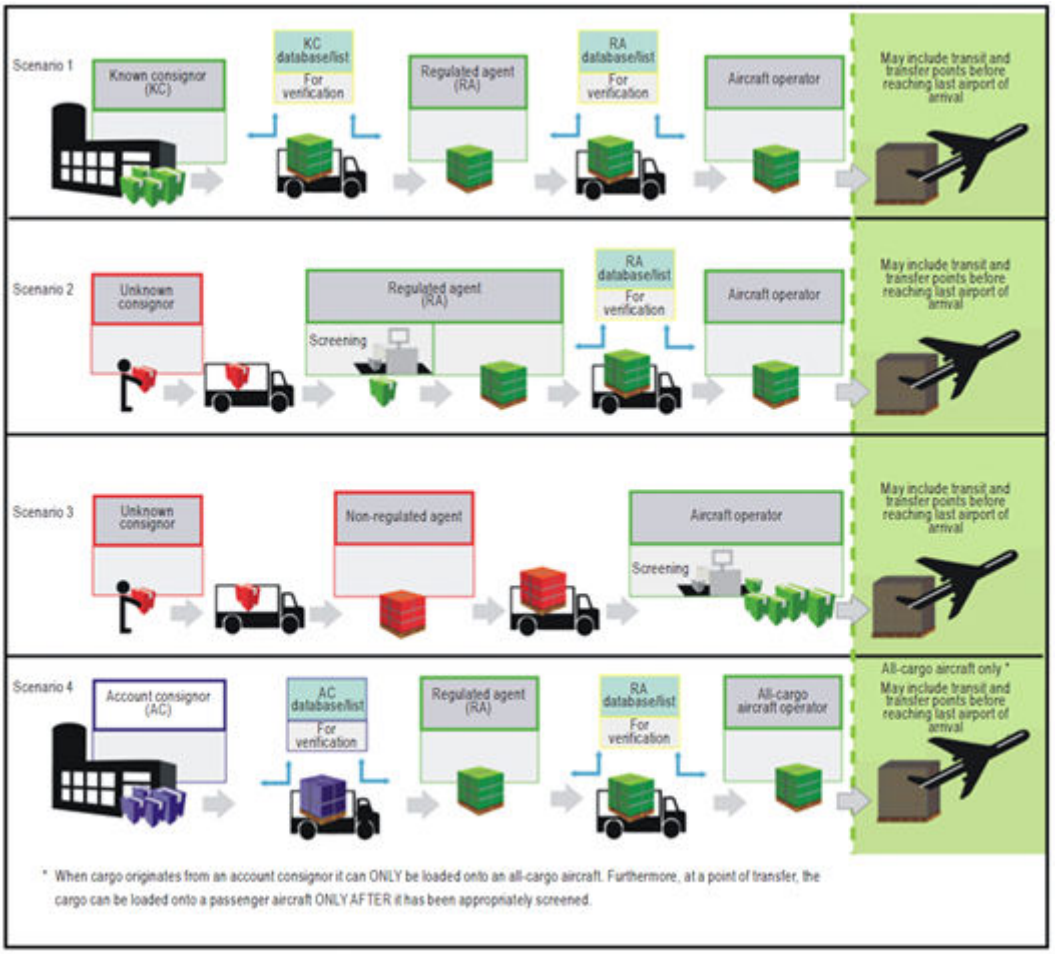


Figure 11-1: Movement of Cargo and Mail Through a Secure Supply Chain

Air cargo and mail shall be processed for transport by air in an operating environment that meets the following objectives:

(a) cargo and mail shall come from a secure supply chain or be screened to effectively detect prohibited items;

(b) additional security measures beyond baseline procedures shall be applied to cargo and mail that are deemed high risk;

(c) once secure, cargo and mail shall be kept secure throughout their entire journey, including at transfer and transit points;

(d) cargo and mail operations shall be subjected to oversight and quality control activities; and

(e) unnecessary duplication of security controls shall be avoided.

In accordance with these objectives, this chapter examines cargo and mail security from the point where a consignment enters a secure supply chain or is screened until it reaches its last airport of arrival.

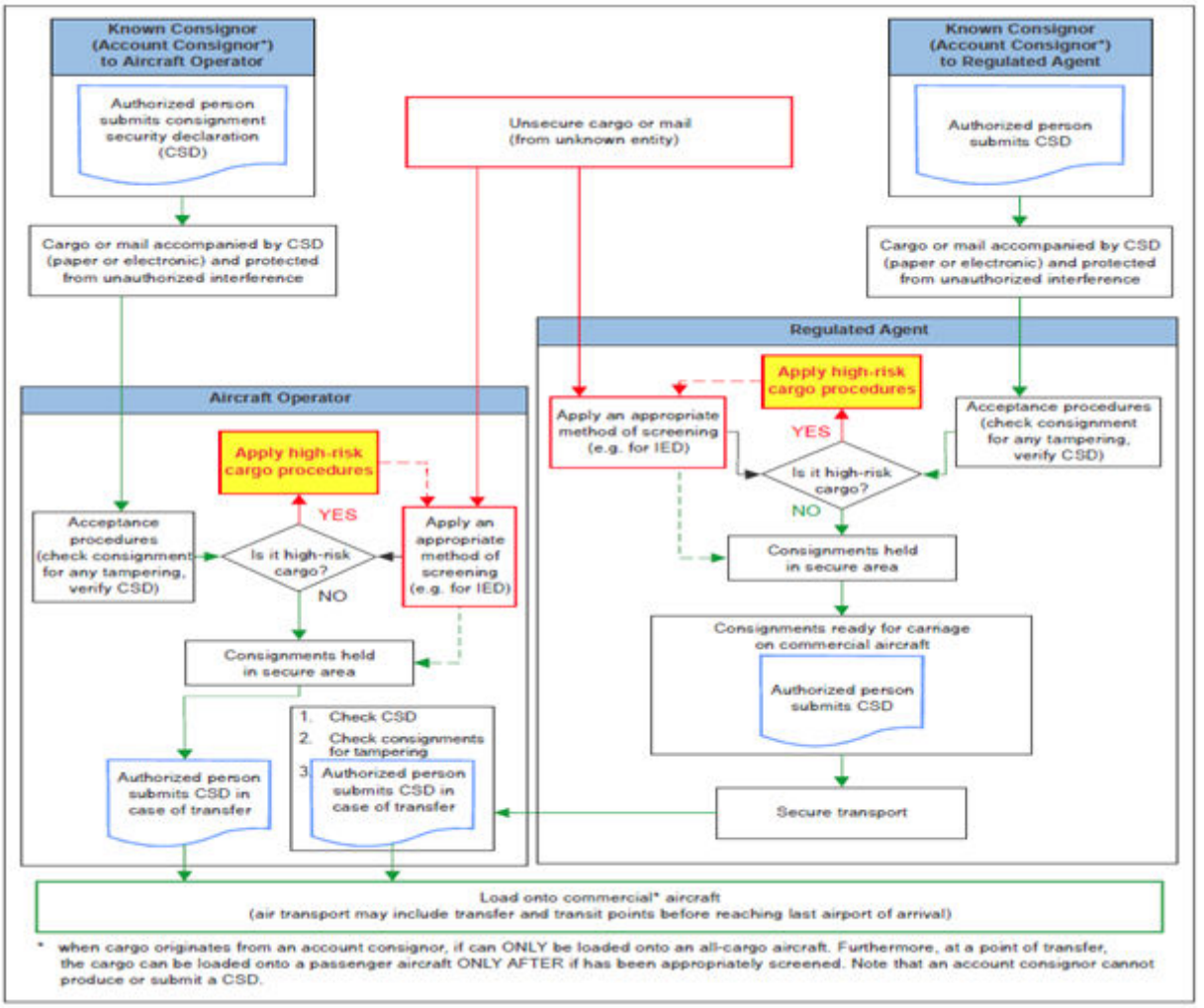


Figure 11-2: Air Cargo Supply Chain

NOTE	PG-GU-BK-005 - Air Cargo Acceptance Decision Making Tool (available in Comply365) can be used as guidance material by the acceptance staff.

11.2.3 Regulated Agent Scheme and Criteria

A regulated agent is an entity such as a freight forwarder that conducts business with Pegasus Airlines and provides security controls that are accepted or required by the appropriate authority in respect of air cargo and/or mail. Pegasus Airlines may also act as a regulated agent. Pegasus Airlines shall accept only consignments from regulated agents that are approved from the appropriate authority from a list of approved regulated agents.

11.2.3.1 Acceptance of Consignments

11.2.3.1.1 Origin of the Consignments

When accepting any consignments, a regulated agent shall establish whether the entity from which it receives the consignments is a regulated agent, a known consignor, an account consignor or none of these.

11.2.3.1.2 Person Delivering the Consignments

The person delivering the consignments to the regulated agent or air carrier shall present an identity card, passport, driving licence or other document which includes his or her photograph and which has been issued or is recognised by the national authority.

The card or document shall be used to establish the identity of the person delivering the consignments.

11.2.3.1.3 Establishment of the Security Status

When accepting consignments from a regulated agent, the receiving regulated agent shall establish the security status of the consignment by verifying whether or not "SPX", “SHR” or "SCO" is indicated on the accompanying documentation. If there is no such indication, it shall be deemed that no security controls have previously been applied.

11.2.3.1.4 Consignments Previously Secured

When accepting consignments to which security controls have previously been applied, the regulated agent shall establish the identity and address of the agent or consignor.

This shall be done at least by verifying whether the agent or consignor is listed as a regulated agent or known consignor in the ‘database on supply chain security’.

The verification can be considered as done if the regulated agent verified earlier on the same day that the entity from which it receives consignments is listed in the 'database on supply chain security'.

The list of TR-DGCA approved regulated agent database is accessible via the following link:
http://web.shgm.gov.tr/documents/sivilhavacilik/files/havacilik_isletmeleri/acenteler/17.6_Yetkili_Acente_Liste.pdf
The EU Database on Supply Chain Security lists all EU-ACC3, RA3 and KC3 designations, and is accessible via the following link:
https://ksda.ec.europa.eu/public/screen/home
The UK Database on Supply Chain Security lists all UK-ACC3, RA3 and KC3 designations, and is accessible via the following link:
https://securesupplychain.caa.co.uk
The list of Pegasus Airlines approved Regulated Agent (RA3) is accessible via the following:
PG-KA-FR-010 - RA3 Validated Stations Database, available in Comply365.

11.2.3.1.5 Consignments Not Previously Secured

The regulated agent shall ensure that consignments to which not all required security controls have previously been applied are:

(a) screened in accordance with point 11.2.5.; or

(b) accepted for storage under the regulated agent's exclusive responsibility, having been selected autonomously without any intervention of the consignor or any person or entity other than those appointed and trained by the regulated agent for that purpose.

Point (b) may only be applied if it is unpredictable for the consignor that the consignment is to be transported by air.

When accepting consignments for which not all the required security controls have previously been applied, the regulated agent may also elect not to apply the security controls as referred to in point 11.2.3.1, but to hand the consignments over to another regulated agent to ensure the application of these security controls.

Protection of secured consignments

After the security controls referred to in point 11.2.3.1 have been applied, the regulated agent shall ensure that:

(a) Unescorted access to these consignments is limited to authorised persons; and

(b) these consignments are protected from unauthorised interference until they are handed over to another regulated agent or air carrier. Consignments of cargo and mail that are in a critical part of a

security restricted area shall be considered as protected from unauthorised interference. Consignments of cargo and mail that are in parts other than a critical part of a security restricted area shall be located in the access-controlled parts of the regulated agent's premises or, whenever located outside of such parts, shall:

- be physically protected so as to prevent the introduction of a prohibited article; or
- not be left unattended and with access to them limited to persons involved in the protection and handling of cargo

11.2.3.1.6 Documentation

After the security controls referred to in point 11.2.3.1 and point 11.5. have been applied, the regulated agent shall ensure that any consignment tendered to an air carrier or another regulated agent is accompanied by appropriate documentation, either in the form of an air waybill or in a separate declaration and either in an electronic format or in writing.

For a detailed description of filling a consignment security declaration form, please refer to point 11.9. Consolidations.

In the case of consolidations, the requirements under this point and point 11.10. will be considered as met if:

(a) the regulated agent performing the consolidation retains the information required under point 11.10. for each individual consignment for the duration of the flight(s) or for 24 hours, whichever is the longer; and

(b) the documentation accompanying the consolidation includes the alphanumeric identifier of the regulated agent who performed the consolidation, a unique identifier of the consolidation and its security status.

Point (a) shall not be required for consolidations that are always subject to screening or exempted from screening in line with points 11.2.9.d) and e) if the regulated agent gives the consolidation a unique identifier and indicates the security status and a single reason why this security status was issued.

11.2.3.1.7 Staff Training and Recruitment

A regulated agent shall ensure that all staff implementing security controls are recruited and trained in accordance with the requirements of PG-GU-EK-002 Security Training Programme (available in Comply365) all staff with access to identifiable air cargo or identifiable air mail to which the required security controls have been applied and have been recruited and subject to security awareness training.

11.2.4 Known Consignor Scheme and Criteria

11.2.4.1 Approval of Known Consignors

Pegasus Airlines shall accept consignments from known consignors that shall be approved by the appropriate authority.

11.2.4.1.1 Security Controls to be Applied by a Known Consignor

A known consignor shall ensure that:

(a) there is a level of security on the site or at the premises sufficient to protect identifiable air cargo and identifiable air mail from unauthorized interference; and

(b) all staff implementing security controls are recruited and trained in accordance with the requirements of chapter 13 and all staff with access to identifiable air cargo or identifiable air mail to which the required security controls have been applied have been recruited and subject to security awareness training in accordance with the requirements of chapter 13; and

(c) during production, packing, storage, dispatch and/or transportation, as appropriate, identifiable air cargo and identifiable air mail is protected from unauthorized interference or tampering.

When, for whatever reason, these security controls have not been applied to a consignment, or where the consignment has not been originated by the known consignor for its own account, the known consignor shall clearly identify this to the regulated agent so that point 11.2.3.15. can be applied.

11.2.4.1.2 Consignments That Need to be Screened

The known consignor shall accept that consignments to which the appropriate security controls have not been applied are screened in accordance with point 11.2.5.

11.2.5 Standard of Screening and Physical Examination

11.2.5.1 Methods of Screening

Cargo and mail shall be screened by at least one of the following methods:

(a) hand search;

(b) x-ray equipment;

(c) EDS equipment;

(d) explosive detection dogs (EDD);

(e) ETD equipment;

(f) visual check;

(g) metal detection equipment (MDE).

11.2.6 Location of Screening and Physical Examination

The basic rule is that all cargo shall undergo screening before being permitted to have access to an aircraft or security-restricted area. These procedures will need to be applied to all international flights and to domestic flights which connect with them.

11.2.7 Details of Screening Equipment

11.2.7.1 Hand Search

A hand search shall consist of a thorough manual check of the consignment, including all its contents.

11.2.7.2 X-Ray

(1) As from 1 July 2014, a consignment screened by single view x-ray equipment shall be examined from at least two different angles with at least 60° and no more than 90° rotation by the same screener, if the depth of the consignment to be penetrated by the x-ray beam exceeds 130cm.

(2) Consignments for which the screener cannot reasonably ensure that they do not contain prohibited articles after screening from two different angles, shall be either rejected or subjected to another appropriate means or method of screening.

11.2.7.3 ETD

(1) Screening by ETD equipment shall consist of the analysis of trace particles or vapour samples taken from both the inside and the outside of the consignment and from its contents

(2) Trace particles or vapour samples shall be collected from at least the following areas:

(a) internal and external box seams, if applicable, under any protective wrapping;

(b) a minimum of 2 external surfaces, under any protective wrapping;

(c) any areas used for manual handling or lifting;

(d) any areas which appear to have been subject to tampering.

(3) ETD equipment may not be used, other than in combination with other appropriate means or methods, for screening consignments if any of the following conditions apply:

(a) if it is not possible to access any area listed at point 2 (a)-(d) above; or

(b) the consignment surfaces are wet or damp; or

(c) the consignment surfaces are obscured or otherwise protected by packing material which may reduce or impede the effectiveness of the sample collection.

11.2.7.4 Visual Check

(1) A visual check shall consist of a thorough visual check of the consignment and shall only be allowed:

(a) in combination with other methods; or

(b) where all parts of the consignment can actually be seen, with or without aids; or

(c) for live animals.

11.2.7.5 Metal Detection Equipment

Metal detection equipment (MDE) shall only be used to screen consignments of cargo and mail which would not normally be expected to contain any metallic parts.

11.2.8 Details of Operator or Service Provider

Please refer to Pegasus Airlines Cargo Operations Manual PG-KA-EK-001, available in Comply365.

11.2.9 List of Exemptions From Security Screening or Physical Examination

The following consignments may be exempt from screening:

(a) time-critical consignments of life-saving materials, provided that they come from a reliable source and are accompanied by appropriate documentation; and

(b) bio-medical samples which may be damaged if subject to screening, provided that they come from a reliable source and are accompanied by appropriate documentation; and

(c) nuclear materials, provided that they are protected in accordance with the Convention on the Physical Protection of Nuclear Materials, New York and Vienna, 3 March 1980; and

(d) consignments which are individually less than 6 millimetres in thickness and less than 250 grams in total weight; and

(e) consolidations composed uniquely of consignments exempt under d); and

(f) transfer cargo and mail unless:

(i) A Member State has received information that the cargo or mail cannot be considered as having been subject to appropriate security controls; or

(ii) It has not previously been screened or subject to security controls by a regulated agent or known consignor and is to be transferred from an all-cargo or all-mail aircraft to a passenger aircraft.

11.2.9.1 Reliable Sources

For the purposes of point 11.2.9. a) and b), reliable sources shall include established medical and charitable organizations, for which the regulated agent or appropriate authority has confirmed:

(a) he address; and

(b) the nature of the business or operation; and

(c) contact details of a person accepting responsibility for the consignment; and

(d) VAT reference number or company registration number.

The documentation shall indicate the source of the consignment, details of the intended recipient and a description of the contents.

11.2.9.2 Other Exemptions

The appropriate authority may, on the basis of a risk assessment, allow the following consignments to be exempt from screening or to be subjected to special security procedures:

(a) consignments of mail comprised only of items that are individually 2000 grams or less in total weight and which are carried on all-mail flights within a Member State, for delivery to an address within that Member State; and

(b) for objective reasons, government mail or cargo where security and protection is ensured by that Member State; and

(c) cargo and mail transported on individual ad-hoc flights operated on account of a single consignor;

(d) it has been previously screened or subject to security controls by the point of departure country that is in the list of EU 2015/1998 Attachment 6-Fii and Turkish NCASP Annex 25.

11.3 DESCRIPTION OF MEASURES FOR UNACCOMPANIED BAGGAGE AND PERSONAL EFFECTS CARRIED AS CARGO

Household goods are goods and products used within households. They are the tangible and movable personal property placed in the living rooms, dining rooms, kitchens, family rooms, great rooms, bedrooms, bathrooms, recreation rooms, hallways, attics, and basements and other rooms of a house.

Unaccompanied baggage carried as cargo fitting the above description shall be subjected to appropriate screening and security controls in accordance with point 7.3.

11.4 DESCRIPTION OF MEASURES FOR COURIER AND EXPRESS PARCELS

CAUTION	Express parcels shall not have been accepted to any Pegasus Airlines flight!

11.5 SAFEGUARDING OF CARGO, COURIER, EXPRESS PARCELS AND MAIL

Cargo and mail that originate from a secure supply chain or have been screened shall be held in cages, compartments, rooms or buildings that are secured against unauthorized access or made tamper-proof by using seals or locks or protected by intrusion detection measures for periods when consignments are left unattended. Access points shall be protected through the use of identification permits or biometric access control systems.

11.5.1 Description of Measures

11.5.1.1 Consignment in a Critical Part

Consignments of cargo and mail that are in a critical part shall be considered as protected from unauthorised interference.

11.5.1.2 Consignment in a Part Other Than a Critical Part

Consignments of cargo and mail that are in a part other than a critical part of a security restricted area shall be located in the access-controlled parts of the regulated agent's premises or, whenever located outside of such parts, shall be considered as protected from unauthorised interference if:

(a) they are physically protected so as to prevent the introduction of a prohibited article; or

(b) they are not left unattended and access is limited to persons involved in the protection and loading of cargo and mail onto the aircraft.

A consignment may be stored outside cages or buildings provided that the consignment itself is equipped with tamper-evident seals or locks and remains under the supervision of guards, a security surveillance or closed-circuit television system, or an intrusion detection device, where appropriate, for the entire storage period. If seals or locks are used, their integrity shall be verified.

If seals are used to secure cargo and mail facilities or the consignment itself, proper stock control and auditing procedures shall be implemented to prevent any unauthorized use of such seals.

11.6 PROCEDURES FOR CARRIAGE OF DIPLOMATIC MAIL

The appropriate authority may allow a diplomatic bag to be exempt from screening or to be subjected to special security procedures provided that the requirements of the Vienna Convention on Diplomatic Relations are met.

If a passenger is a diplomatic courier, any diplomatic pouches accompanying that courier, whether as cabin baggage or hold baggage, "shall not be opened or detained" (Vienna Convention Article 27(3)). All other cabin baggage items and hold baggage shall be processed in the normal manner.

Diplomatic baggage, including cabin baggage and hold baggage, shall be identified as such by the sending State. "The packages constituting the diplomatic bag must bear visible external marks of their character"

(Vienna Convention Article 27(4)).

A courier accompanying a diplomatic bag shall possess "an official document indicating his [or her] status and the number of packages constituting the diplomatic bag" (Vienna Convention Article 27(5)).

Annex 17 requires that States establish measures to ensure that cabin and hold baggage are "screened prior to being loaded onto an aircraft" but does not require the screening of diplomatic baggage by X-ray or any other method inconsistent with the Vienna Convention. The sending State may wish to inform the aircraft operator in advance when diplomatic baggage is to be brought on board an aircraft.

If requested to do so, the sending State shall be prepared to verify, orally or by written documentation, that the chain of custody of the diplomatic baggage was maintained at all times by the sending State and that the diplomatic baggage does not endanger the security of the aircraft or its passengers.

In the event that a receiving State, or a State through which a diplomatic bag is transiting or transferring, has specific information that a sending State's diplomatic baggage intended for transportation on an aircraft poses a threat to the security of that aircraft or its passengers, the receiving State or the transiting or transferring State, by decisions at the appropriate level, may refuse to place the diplomatic baggage on board but shall not open it. In such cases, the receiving State shall so inform the embassy of the sending State through the usual diplomatic channels.

States may wish to give serious consideration to applying a seal to their own diplomatic baggage and require States that transport diplomatic baggage to, from or through their territory, to apply their own seal as a deterrent to tampering.

Receiving States may wish to inform the missions of the sending States of their requirements, procedures and expectations with respect to diplomatic couriers and diplomatic baggage.

11.7 TREATMENT OF SUSPECT CARGO OR MAIL

Any suspicion raised by a cargo or mail consignment shall be resolved before it is transported for carriage by air. A suspect cargo or mail consignment shall:

(a) be treated as unsecure cargo or mail and subjected to appropriate security controls, including screening; and

(b) shall be transported by an aircraft operator only if it can be confirmed that the consignment is secure because it does not contain any prohibited articles.

If security controls detect a suspicious item in a consignment, it is important that:

(a) staff members do not touch the suspicious item and immediately contact their supervisor to assist in confirming any suspicion; and

(b) if a suspicion is confirmed, staff members follow the emergency procedures established by their organisation for the handling of such events, which may include the following:

(i) the relevant security, law enforcement and/or Explosive Ordnance Disposal (EOD) organizations are contacted, as appropriate;

(ii) the suspicious item, and the consignment in which it is contained, are handled by EOD personnel only; and

(iii) evacuation and contingency plans are implemented, in coordination with security, law enforcement and emergency services officials.

If a prohibited item has been identified, a threat assessment shall be conducted to determine whether additional security controls (e.g. advanced screening techniques) shall be applied to other consignments bearing similar characteristics (e.g. destined for the same flight or destination or originating from the same consignor or location).

The appropriate authority shall be notified of the discovery, as shall other operational entities (e.g. handling agents or aircraft operators) using the affected and adjacent facilities (in accordance with an established emergency coordination plan). If suspicion cannot be resolved, the consignment shall be refused for carriage by air and shall not be loaded onto a commercial aircraft.

11.8 HIGH-RISK CARGO AND MAIL

High-risk cargo or mail is defined as follows: a cargo or mail consignment is considered high-risk when it is presented by an unknown entity or shows signs of tampering and, in addition, meets one of the following criteria:

(a) specific intelligence indicates that the cargo or mail poses a threat to civil aviation; or

(b) the cargo or mail shows anomalies that give rise to suspicion; or

(c) the nature of the cargo or mail is such that baseline security measures alone are unlikely to detect prohibited items that could endanger the aircraft (i.e. IEDs).

Regardless of whether the cargo or mail comes from a known or unknown entity, a State's specific intelligence about a consignment may render it high-risk.

High-risk cargo and mail shall be subjected to appropriate screening to effectively detect an IED or mitigate the specific threat associated with it. This shall include other detection methods or robust security measures that are not part of the baseline security measures. Such additional screening methods and measures shall be determined by the appropriate authority.

In addition to being presented by an unknown entity or showing signs of tampering, a cargo consignment may be rendered high-risk due to, for example, its dense and/or cluttered nature, which may prevent the detection of IEDs by conventional screening equipment. In such cases, additional screening methods beyond baseline security measures shall be applied.

Even when the application of baseline security measures, which may include the use of routine technology such as conventional X-ray screening or manual searches, seems to indicate that the cargo consignment does not contain an IED, it shall be checked for anomalies that give rise to suspicion. If such anomalies are found, additional screening methods beyond baseline security measures shall be applied.

shall a State receive intelligence information regarding a possible threat caused by a cargo consignment, it shall share that threat information with the States concerned as early as practicable, in order to prevent the loading of such a consignment on a commercial aircraft without, at the very least, the application of high-risk security measures.

The figure below illustrates the decision-making process to be followed in order to determine whether a cargo consignment shall be considered as high-risk cargo or mail and, if so, how to process it.

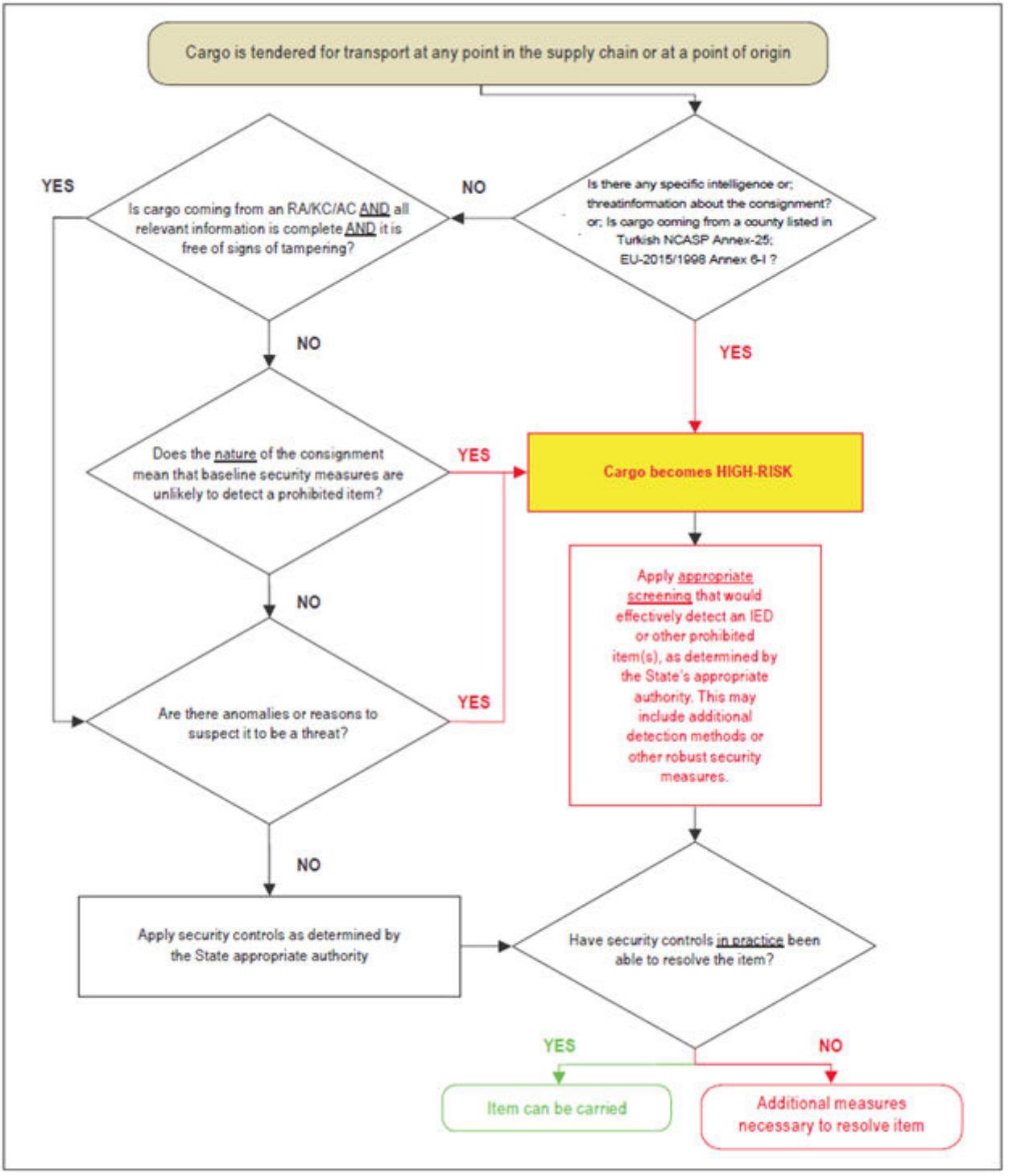


Figure 11-3: High-Risk Cargo Decision-Making Process

11.9 CONSIGNMENT SECURITY DECLARATION

Regulated Entity Category (RA, KC, or AO) and Identifier (of the regulated entity issuing the security status) **1**		Unique Consignment Identifier (if AWB format is nnn-nnnnnnnn) **2**	
Contents of Consignment **3** ☐ Consolidation			
Origin **4**	Destination **5**	Transfer/Transit Points (if known) **6**	
Security Status **7**	Reasons for issuing Security Status		
	Received from (codes) **8**	Screening Method (codes) **9**	Grounds for Exemption (codes) **10**
Other Screening Method(s) (if applicable) **11**			
Security Status issued by **12** Name of Person or Employee ID		Security Status issued on Date (ddmmyy) ..... Time (tttt) **13**	
Regulated Entity Category (RA, KC, AC or AO) and Identifier (of any regulated entity who has accepted the security status given to a consignment by another regulated entity) **14**			
Additional security information **15**			

Figure 11-4:

Completion instructions

(1) **Regulated Entity Category (RA, KC or AO) and Identifier:** The regulated agent, known consignor, or aircraft operator that originally issued the security status, identified by its category (i.e. RA, KC or AO) and its unique identifier, must be entered.

(2) **Unique Consignment Identifier:** The identification of the consignment itself must be entered. This may be an air waybill (format is nnn-nnnnnnnn), a house bill or a mail consignment identifier.

(3) **Contents of consignment:** Identification of consignment details (e.g. goods description) must be entered for a direct air waybill or house waybill shipment. For a consolidation shipment, i.e. a master air waybill with associated house waybill(s), the consolidation box shall be ticked in lieu of the goods description.

(4) **Origin:** The identification of the origin of the consignment must be entered. This is the origin related to the appropriate transport documentation (air waybill or house waybill) as identified in Box 2 (e.g. IATA three-letter airport or city code).

(5) **Destination:** The identification of the final destination of the consignment must be entered. This is the destination related to the appropriate transport documentation (air waybill or house waybill) as identified in Box 2 (e.g. IATA three-letter airport or city code).

(6) **Transfer/Transit Points:** The identification of an en route stopping point where cargo may be transferred to another aircraft or remain on board the same aircraft shall be entered, if known, to the issuer (e.g. IATA three-letter airport or city code). Otherwise this entry may be left blank.

(7) **Security Status:** The coded identification of the security status assigned to the consignment must be entered to indicate whether the consignment is secure for:

(a) passenger, all-cargo and all-mail aircraft (code SPX);

(b) all-cargo and all-mail aircraft only (code SCO); or

(c) passenger, all-cargo and all-mail aircraft, in accordance with high-risk requirements (code SHR).

(8) **Received From:** The coded identification of the category (i.e. regulated agent RA, known consignor KC, account consignor AC or aircraft operator AO) that tendered the consignment must be entered. If no other reason, e.g. “screening method” or “grounds for exemption”, is indicated and the consolidation box is not ticked, then this entry cannot be blank.

(9) **Screening Method:** The coded identification of the screening methods (see below) used by the regulated agent, known consignor, or aircraft operator when securing the consignment may be entered as a reason that the security status was issued, e.g. screening method codes. If no other reasone.g. “received from” or “grounds for exemption” is indicated, and the consolidation box is not ticked, then this entry cannot be left blank. In some cases a single screening method may not be sufficient to inspect all types of consignments, therefore more than one screening method may be listed.

(10) **Grounds for Exemption:** The coded identification (see below) indicating why a consignment is exempt from screening as defined in State national civil aviation security programmes may be entered as a reason that the security status was issued, e.g. screening exemption codes. If no other reason, e.g. “received from” or “screening method”, is indicated and the consolidation box is not ticked, then this entry cannot be left blank.

(11) **Other Screening Method(s):** If the code entered in Box 9 indicates that any other means were applied, then text specifying the other means used must be entered.

(12) **Security Status issued by:** If the consolidation box is not ticked then the individual of the regulated agent, known consignor, or aircraft operator who issued the security status must be identified by name or employee number.

(13) **Security Status issued on:** If the consolidation box is not ticked then the exact date and time when the security status was issued by the regulated agent, known consignor, or aircraft operator employee must be indicated.

(14) **Regulated Entity Category (RA, KC, AC or AO) and Identifier:** The identifier of any regulated agent, known consignor, or aircraft operator that accepts custody of the cargo and accepts the security status originally issued by the regulated agent, known consignor, or aircraft operator identified in Box 1 must be entered. This entry would confirm that the cargo has remained secure and would follow any other entries for other regulated agents, known consignors, or aircraft operators that have also accepted the original security status.

(15) **Additional Security Information:** Any additional security information that may be required by an ICAO Member State, e.g. any national regulation applicable to the responsibilities in the event of a false declaration or any applicable emergency amendment. A signature of the responsible person initially issuing a hardcopy consignment security declaration set out in Box 1 shall be inserted when the supply chain is paper based.

Table 11-1: ***Coded Identification***

Screening Methods

VCK	Visual Check
PHS	Physical Inspection/Hand Search
XRY	Conventional X-Ray
EDS	Explosive Detection System
CMD	Cargo Metal Detection
ETD	Explosives Trace Detection
EDD	Explosives Detection Dogs
AOM	Other screening technologies and methods that could be used to secure cargo and mail consignments and the code AOM shall be followed by an exact description of the method(s) used.
Exemptions	
DIPL	Diplomatic bags/pouches
BIOM	Biomedical samples, vaccines and other perishable medical items.
LFSM	Life-sustaining items such as blood, blood products, bone marrow and human organs.
NUCL	Radioactive materials packaged according to the ICAO Technical Instructions for the Safe Transport of Dangerous Goods by Air (Doc 9284).
SMUS	Consignments or packages which are individually less than 6 mm in thickness and less than 250 grams in total weight, and consolidations composed uniquely of such consignments or packages.

11.10 COMPANY MAIL (CO-MAIL) AND COMPANY MATERIAL (CO-MAT)

11.10.1 Company Mail (Co-Mail)

Co-mails are letters, documents which are sent from Head Quarters to international, domestic stations and offices, from stations and offices to Head Quarters or other stations and offices by the departments of Pegasus Airlines and contracted ground handling companies which ensure internal correspondence and maintain business continuity.

Pegasus Airlines ensures that company mail and materials carried on its own aircraft are subjected to security controls before being placed on board an aircraft and thereafter protected from unauthorized interference from the point of security controls until loaded onto the aircraft.

The Company-mail to be carried by air shall comply with the following:

(a) shall be properly wrapped.

(b) shall not be a document of commercial value.

(c) The Co-Mail Form shall be completed and made available for the Flight/Cabin Crew.

The contents of the Company Mail shall not be:

(a) Documents or material, the transport of which has been forbidden by security or other organizations.

(b) Materials of commercial value which is not the possession of Pegasus Airlines.

(c) shall not have odorous properties.

(d) shall not be irregularly wrapped.

(e) shall not contain jewels.

Co-Mails can be classified as Internal or Confidential. The managers authorized in the signature circular of the relevant department are responsible for the classification of company mails as "Confidential".

The Pilot in Command of the aircraft, if deemed necessary, can open and/or ask to open Co- Mails for checking purposes except if it is classified as confidential.

The acceptance and carriage procedure of co-mail and co-mat are described in each operational department manuel. Please refer to PG-UI-EK-001, PG-KH-EK-001 and PG-DO-EK-001, available in Comply 365.

11.10.2 Company Material (Co-Mat)

Co-Mats are internal supplies and materials sent to domestic and international stations in order to ensure business continuity.

Company materials can never be carried in the aircraft cabin. They must be packaged or placed by the sender in a way that will not damage the aircraft, and the Co-Mat label is tagged on it.

Co-Mat shipments shall only include aircraft spare parts, advertising and promotional materials, Pegasus Magazines, office supplies, in-flight and catering materials, company promotion materials, etc.

The information that the Company Material (Co-Mat) will be transported, together with the quantity and weight, is notified to the Pilot in Command of the aircraft on the Loadsheet and LDM by the Ground Handling Services / Operations Staff.

The number and weight information regarding company materials is transmitted to the operations department where the weight and balance procedures are carried out at least 2 hours before the flight

For further details regarding the acceptance and carriage procedure of company mail and materials, please refer to PG-GU-PR-055 – Company Mail (Co-Mail) and Materials (Co-Mat) Procedure available in Comply365.

For more details regarding the acceptance and carriage procedure of co-mail and co-mat, please refer to PG-GU-PR-055 - Company Mail (Co-Mail) and Company Material (Co-Mat) Procedure.

Procedures relevant for each operational area are also described on PG-UI-EK-001, PG-KH-EK-001 and PG-DO-EK-001 manuals, available in Comply 365.

11.10.3 Air Carrier Mail And Materials Loaded Into Any Part of an Aircraft Other Than the Hold

Before being loaded into any part of an aircraft other than the hold, Pegasus Airlines mail and materials shall be screened and protected in accordance with the provisions on cabin baggage in chapter 4.

11.10.4 Exemptions

The following categories of Pegasus Airlines mail and materials may be exempt from the security controls referred to in point 11.10.:

- Pegasus Airlines mail and materials, which originate in critical parts.
- Spare parts for aircraft, transported as air carrier materials, provided that they are accompanied by documentation attesting airworthiness conformity with applicable ECAC recommendations.
- The documentation shall be checked before loading the spare parts onto an aircraft and kept at a point not on the aircraft for the duration of the flight or for 24 hours, whichever is longer.

11.10.5 Air Carrier Materials Used for Passenger and Baggage Processing

Pegasus Airlines materials which are used for the purposes of passenger and baggage processing (boarding cards, bag tags etc.) and which could be used to compromise aviation security must be protected or kept under surveillance in order to prevent unauthorised access.

After completing of the check-in or boarding process, all related blank documents must be taken from the counters or related places and must be kept in locked or under surveillance in cabinets.

Self-check-in and applicable internet options allowed for use by passengers are to be considered as authorised access to such materials.

11.10.6 Discarded Materials

Discarded (miss-printed etc.) materials which could be used to facilitate unauthorised access or move baggage into the security restricted area or onto aircraft shall be destroyed or invalidated according to the materials nature.

Printed material such as boarding passes, passenger lists, and handling forms may have to be reprinted and are therefore left behind as waste. Dispose of these documents according to data protection rules, as they contain passenger data.

11.10.7 Departure Control Systems and Check-In Systems

Departure control systems and check-in systems must be managed in such a manner as to prevent unauthorized access. Departure Control Systems (check-in systems) shall be controlled to prevent unauthorized access.

Personnel authorized by Pegasus Airlines or related service providers shall use the check-in system. Users shall be checked and revised according to the changes as soon as possible.

- Follow airport procedures intended to prevent unauthorized use and access to unissued (blank) boarding passes.
- Before leaving the counter, remove boarding cards and baggage tags from the respective printers or lock them.
- Before leaving the counter, sign-out, log-off and lock the system.
- Observe regulations concerning the usage of sign-ins and passwords.

Self-check-in allowed for use by passengers is to be considered as authorized access to such systems.

End of Section

12 RECRUITMENT OF STAFF

12.1 DESCRIPTION OF PROCEDURES FOR RECRUITMENT OF STAFF WITH SECURITY DUTIES, INCLUDING BACKGROUND CHECKS

12.1.1 Application

The requirement for a background check shall be applicable to personnel who:

(i) Engage in the implementation of security controls.

(ii) Have unescorted access to the security restricted area of an airport.

(iii) Have unescorted access to other controlled areas and searched aircraft.

(iv) Have access to sensitive aviation security information.

According to PG-PA-PR-001 – Recruitment Procedure (available on Comply365), all Pegasus Airlines candidates (full time or part time) must complete PG-PA-FR-002 – Candidate Interview Form (available in Comply365) prepared by the Chief Human Resource Office; all the recruitment procedure is performed by Pegasus Academy & Talent Acquisition Management. The application form gives full details of the applicant's:

(a) personal data accompanied by a recent and authenticated photograph;

(b) education;

(c) training;

(d) previous employment; and

(e) other relevant information deemed necessary by the State to facilitate a background check to confirm a person's identity and previous experience, including any criminal history.

The application form also includes:

(a) a declaration that the information is complete and accurate;

(b) verification of results of background checks;

(c) a declaration by the candidate accepting that any misrepresentation of the facts is grounds for refusal of employment or for disciplinary proceedings or criminal charges;

(d) the candidate's agreement that personal and professional information may be collected from former employers, educational establishments, government agencies and personal references for the purpose of verification; and

(e) the candidate's signature, if online application approval is involved.

For the purposes of this chapter, a 'state of residence' means any country in which the person has been resident continuously for 6 months or more and a 'gap' in the record of education or employment shall mean any gap of more than 28 days.

The descriptions in this chapter 12 must also comply with Pegasus Airlines contracted services suppliers' staff.

12.2 RECRUITMENT

12.2.1 Persons With Security Duties in Security Restricted Areas

Persons being recruited to implement, or to be responsible for the implementation of screening, access control or other security controls in a security restricted area must have successfully undergone a background check and pre-employment check.

12.2.2 Persons With Security Duties in Other Areas

Persons being recruited to implement or to be responsible for the implementation of screening, access control or security controls other than a security restricted area must have successfully undergone a background or pre-employment check.

12.2.3 Background Checks

Background checks (criminal records) must be completed and checked by Chief Human Resources Officer before the person undergoes any security training involving access to information which is not publicly available.

In accordance with Turkish national rules, background checks are performed by Government Authorities to:

(a) establish the person's identity on the basis of documentary evidence;

(b) cover criminal records in all States of residence during at least the preceding 5 years; and

(c) cover employment, education and any gaps during at least the preceding 5 years.

12.2.4 Pre-Employment Checks

According to the Turkish Social Security and General Health Insurance Law, any person must have undergone a background check.

Before the person is accepted to any security training and allowed to access information which is not publicly available, the Chief Human Resources Officer- Recruitment Management performs pre-employment checks of Pegasus Airlines employees, according to the Reference Control Form PG-PA-FR-006 (covering at least five years).

Pre-employment checks ensure at least to:

(a) Establish the person's identity on the basis of documentary evidence;

(b) Cover the employment, education and any gaps during at least the preceding 5 years; and

(c) Require the person to sign a declaration detailing any criminal history in all states of residence during at least the preceding 5 years.

(d) Additionally: No reference is required from new graduates, inexperienced persons or interns.

(e) The references submitted by the candidate are controlled by the phone by the recruitment entity responsible (IAS); the interviews are conducted in accordance with the Reference Control Form PG-PA-FR-006, available in Comply365.

(f) Answers given by the references are recorded on the Candidate Tracking System (ATS).

(g) Recruitment process details are described on PG-PA-PR-001 – Recruitment Procedure, available in Comply365.

12.3 RECRUITMENT PROCESS

12.3.1 Initial Assessment of Abilities and Aptitudes

The recruitment process for all persons being recruited under points 12.2.1 and 12.2.2 shall include at least a written application and an interview stage designed to provide an initial assessment of abilities and aptitudes.

The Human Resources Vice Presidency - Recruitment Management performs the assessment of abilities and aptitudes and according to PG-PA-FR-021 - Candidate Evaluation Form (available in Comply365) and kept as point 12.3.3.

12.3.2 Mental and Physical Abilities

Persons being recruited to implement security controls must have the mental and physical abilities and aptitudes required to carry out their designated tasks effectively and must be made aware of the nature of these requirements at the outset of the recruitment process.

These abilities and aptitudes shall be assessed during the recruitment process and before completion of any probationary period.

12.3.3 Recruitment Records

Recruitment records, including results of any assessment tests, are kept for all persons recruited under points 12.2.1 and 12.2.2 for at least 5 years after cancellation of their contract by the Chief Human Resources Officer – Talent and Reward Management (please see PG-PA-PR-001, available in Comply365).

12.3.4 Cancellation of the Recruitment Process

Whilst the background is checked by Recruitment Management during the period of acceptance of employment or training, if the persons are identified with the structure, formation or groups determined to constitute a threat to National Security or there is evidence of membership or association with terrorist organizations or related laws or regulations re the recruitment process will be cancelled. The same applies to persons convicted of embarrassing offences such as embezzlement, revolt, extortion, bribery, theft, fraud and forgery according to the following Turkish Criminal Laws:

- Law No. 5237 dated 26.09.2004 on Criminal Record,
- Law No. 5607 dated 21.03.2007 on the Prevention of Smuggling,
- Law No. 4208 dated 19.11.1996 on the Prevention of Money Laundering,
- Law No. 2345 dated 12.06.1933 on the Inspection of Drug Matters,
- Law No. 6136 dated 10.07.1953 on Firearms and Knives,
- Law No: 2863 dated 23.07.1983 Law on the Protection of Cultural and Natural Assets, and
- Law No. 1567 dated 20.02.1930 on the Protection of the Value of Turkish Currency.

Those who have been removed from public service due to their membership, affiliation or contact with the above must not be admitted to training provided in the field of civil aviation security and shall not work as instructors or in any part of Pegasus Airlines.

12.3.5 Repeating of Background Checks

According to the Turkish NCASP, Pegasus Airlines Chief Human Resources officer must carry out for the personal defined under the point 12.2.1 and 12.2.2, at least every 3 years a repeated recruitment process according to point 12.3.3. and the documents shall be kept in personal private files.

End of Section

13 TRAINING OF STAFF

Pegasus Airlines is an TR-DGCA Approved Aviation Security Training Organization. The approval is available for Classroom and e-Learning (Web Based) trainings.

SİVİL HAVACILIK GENEL MÜDÜRLÜĞÜ
DIRECTORATE GENERAL OF CIVIL AVIATION

HAVACILIK GÜVENLİĞİ EĞİTİM KURULUŞU YETKİ BELGESİ
AVSEC TRAINING ORGANIZATION APPROVAL CERTIFICATE

Belge Nu./ Certificate No.
HGD/HEK-8

PEGASUS HAVA TAŞIMACILIĞI A. Ş.

Havacılık Güvenliği Eğitim ve Sertifikasyon Talimatında (SHT-17.2) Öngörülen Şartları Yerine Getirmesinden Dolayı ve Bu Talimatta İstenen Şartlara Uymak Kaydıyla, Yine Bu Talimatta Yer Alan Kurslardan;

Aviation Security Training and Certification Directive (SHT-17.2) Have Been Fulfilled and Providing That The Conditions Required in This Direction Are Satisfied, This Certificate Authorizes That Courses;

(1), (5), (6), (7), (8), (9), (10)

Eğitimlerini Vermek Üzere Yetkilendirilmiştir.
In SHT-17.2 can be given in Trainings.

Bu belge başkasına devredilemez, sahibi tarafından iade edilmediği, geri alınmadığı ve iptal edilmediği sürece verildiği tarihten itibaren geçerlidir.

This certificate is not transferable and it is valid from the issue date unless given back by the bearer, revoked and cancelled.

Düzenlenme Tarihi: 15 Eylül 2022
Date of Issue: September 15, 2022
Geçerlilik Tarihi: 16 Eylül 2027
Date of Expiry: September 16, 2027

Serdar Karabulut
Daire Başkanı / Head of Department

Figure 13-1: Aviation Security Training Center Approval Certificate

NOTE	All training details are described in Pegasus Airlines Security Training Programme, please refer to PG-GU-EK-002, available in Comply365.

End of Section

14 CONTINGENCY PLANNING

Pegasus Airlines is responsible for assessing and categorising any threat to its aircraft. In doing so, it shall consult with any other entity that can provide information relevant to the assessment process and such consultation should respect any specific and different measures or procedures that are mandated by the relevant appropriate authority. It is essential that the process must be defined and implemented in a way that ensures the assessment is carried out thoroughly and expeditiously so that risks are addressed promptly and effectively. The views of the national authorities may be taken into account when a threatening message is being assessed and in determining what further action should be taken.

In the event of threats to more than one aircraft from different air carriers, the air carriers concerned should ideally agree on an assessment. If categorisation cannot be agreed, then the most cautious assessment will be followed.

Pegasus Airlines has at least one properly trained assessor available at all times (IOCC Duty Leader, Aviation Security Leader (RP), Chief Safety and Security Officer).

Pegasus Airlines is responsible, in conjunction with the relevant authorities, for initiating the implementation of an emergency response plan, if appropriate.

Landing permission shoudl not be refused. The Pilot-in-Command is responsible for the safety of his/her passengers, crew and aircraft. Under lawful command, the Pilot-in-Command has the authority to divert to an airfield of choice and for subsequently ordering an evacuation of the aircraft.

14.1 DESCRIPTION OF PLANS TO DEAL WITH THE FOLLOWING CONTINGENCIES

14.1.1 Aircraft Hijack

In a case where hijacking is attempted on board a Pegasus Airlines aircraft, crew members are instructed to follow the hijacker’s commands and not to resist in any way. No definite rules can be laid down for such cases, but the following rules shall as far as possible be followed:

Effective ground security measures are intended to reduce the possibility of potential hijackers to gain access to an aircraft. In the event of a hijacking, both passenger and crew safety and security are primary considerations.

It is Pegasus Airlines’ general policy from the beginning of boarding until the last passenger disembarks the board, that whenever possible the flight deck crew compartment door shall be kept closed and locked, thereby inaccessible for a possible hijacker, and the flight crew will keep control of the flight deck crew compartment at all costs. Refer to 10.3.2 Cockpit Door Procedures.

It is of great importance that crew members shall not leave the aircraft unless it has been so ordered by the responsible authority.

There are two hijacking types according to civil aviation history:

(1) Classical (or traditional) hijacking; this generally occurs for political or personal reasons in pursuit of a crime. In these cases, crew members are instructed to follow the hijackers’ commands and not to resist in any ways.

(2) Hijacking with new demands dimensions; here the Pilot-in-Command has the burden of making all decisions and he may decide to cooperate and/or negotiate with the hijackers’ demands, or land the aircraft as soon as possible in terms of a time and place

14.1.1.1 Flight Crew

14.1.1.1.1 Aircraft on Air

(1) Once the hijacking has been signalled, it is the Pilot in Command's responsibility to evaluate the severity of the threat and decide if it is necessary to perform an emergency landing or if it is safer to fly to the hijacker's demanded destination.

(2) If an emergency landing is required, the Pilot in Command needs to engage in a rapid descent and get clearance from the nearest airport possible. The hijacker will most likely request to divert the aircraft to a particular location.

(3) It should be explained to the hijacker that the destination cannot be reached without landing to refuel.

(4) Once the aircraft has landed, it should taxi to a pre-determined isolated holding area, usually away from the terminal buildings.

(5) Once the aircraft is parked, obstacles such as service vehicles should be put in place to prevent the airplane from taking off again.

(6) Should an aircraft in flight be subjected to unlawful interference, the Pilot in Command shall endeavour to set the transponder to Mode A Code 7500 to give an indication of the situation unless circumstances warrant the use of Code 7700.

(7) When a pilot has selected Mode A Code 7500 and is subsequently requested to confirm his code by ATC he shall, according to circumstances, either confirm this or not reply at all.

(8) Note: The absence of a reply from the pilot will be taken by ATC as an indication that the use of Code 7500 is not due to an inadvertent false code selection.

(9) When unable to change the transponder setting or when not under radar control, transmit a message which includes the phrase “(aircraft call sign) transponder “seven five zero zero”.

(10) The Pilot-in-Command is in command. He has the burden of making all decisions. The Company will initiate no outside interference without permission from the Pilot-in-Command and the flight crew.

(11) The flight Crew members should offer suggestions. The Pilot-in-Command will consider all proposals.

(12) Comply with the hijacker’s instructions. If unable to comply, explain the reason. Keep the hijacker informed as this will ease relations.

(13) The hijacker’s destination may not be feasible, if so offer substitutes.

(14) If the hijacker remains in the flight crew compartment, keep the Cabin Attendants informed. You should initiate the calls so the buzz from the cabin will not disturb the hijacker. Communicate often.

(15) If possible, a PA directly from the flight crew does reassure the passengers that things are proceeding well.

(16) If the hijacker is in the cabin, do not use the call button to signal to the cabin attendants. This might cause distress to the hijacker. Use the PA to announce take-off

(17) Use the radio to contact ATC and/or Company (via ACARS/VHF), if possible, immediately upon the first suspicion of hijacking.

14.1.1.1.2 Aircraft on Ground

(1) When re-fuelling is necessary during the hijacking, explain the process involved. The number of ground personnel will be kept to a minimum. Pilot-in-Commands of other hijacked planes stated their desire to keep in constant contact with ground personnel while re-fuelling was in process. Explain this to the hijacker. Offer him a set of earphones if he has not already taken one.

(2) Pegasus Airlines Flight Crew and Cabin Crew do not leave the aircraft unless it has been ordered by the responsible authority. The flight crew implement the communication techniques which was are defined on the PG-GU-PR-007 Pilot and ATC Communication in Illegal Acts Procedures available in Comply365 or Pegasus EFB Application.

14.1.1.2 Cabin Crew

The following guidelines are offered when dealing with a hijack situation:

- It should be remembered that no two incidents will be the same and you should adjust and adapt your thinking to the situation at hand.
- At first, the hijacker should be discouraged from dealing with the Pilot-in-Command of the aircraft and efforts should be made to keep him/her out of the cockpit. Cabin Crew can try to inform the Pilot-in-Command about the situation and say the word TRIP via the interphone if possible. The Flight Crew will gain time to inform the ATC.
- The Pilot-in-Command must try to be the only crew member dealing with the hijacker.
- Hijackers will try to reach their aims via the Flight and Cabin Crew Members.
- The attitude by the crew towards hijackers and any relationship set-up between the two parties may be vital in helping to resolve the situation and in bringing the incident to a successful termination.
- It cannot be stressed enough how important personal contact is, especially in the case of a single hijacker.
- Only one member of the crew should have any dealings with him/her. Any relationship established could be invaluable in achieving the primary objective: the safe release of the passengers and the crew.

Always remember that there may be others in the hijack team who do not disclose themselves initially, the so-called sleeping-terrorist hijackers, and who will remain seated with the hostages.

- Do not antagonize or argue with the hijackers, especially not on political matters.
- Do not talk to them in a patronizing way and do not appear to be superior.
- If a hijack takes place., Interest should be shown in the hijacker's problems, and he should be encouraged to talk. Do not volume up your voice while dealing and talking with him.
- Do not try to disarm the hijacker(s), because even the accidental discharge of a firearm in the cabin can be extremely dangerous for all on board.
- Sympathize with him by all means, although there are several things that should be avoided whenever possible.
- Do not make him feel nervous and always ensure that only one member of the crew approaches him at any one time.
- Do not become mentally aligned with the hijacker(s). If the hijacker is mentally disturbed, do not refer to insanity or mental disorders.
- Do not make any move unless the hijacker(s) understands the reasons. Inform him about the action you will take or the aircraft actions that will happen. Be honest concerning operational limitations of the aircraft.
- Do not suggest any course of action. If it goes wrong, you may be held responsible.
- Do not supply alcoholic beverages to passenger and hijacker(s) unless demanded by the hijacker(s). (If it is possible, try to pour out these liquids).
- Try to serve him beverage as much as possible, this will cause him to use the lavatory often.
- Try to talk about the subjects for which he can never have the answer.
- Check the quantity of food and beverage. (Try to make storage).
- Crew must rest (as much as possible) by having crew change duties. This will help to keep alert during the hi-jack period.
- Try to convince him that you are on his side and he can only reach his aim with the help of the crew members.

- Talk to him in his mother tongue or a common language.
- If you are unable to make positive communication with him, let the other crew members communicate with him.

If you are able to communicate (in private, such as mobile phone, etc..) with the outside world, try to pass as much information as possible. Keep to the facts and do not give guesses or personal analyses.

Important information can be:

- Number of hijackers.
- Their nationality.
- Their appearance.
- Their clothing.
- The language they use.
- Their position in the aircraft.
- Type and number of weapons, explosives, hand-grenades or flammable substances they have in their possession.
- Number of passengers and their seating.
- Which doors are blocked?
- Any damage to the aircraft.

14.1.1.2.1 Aircraft on Ground

- Try to keep the cockpit door locked as long as possible.
- Try to discourage passengers from becoming directly involved with the hijacker(s).
- On the ground try to obtain permission for food and water to be brought on board. (Do not provide service with a trolley).
- Clear the emergency exits (Try to find out a suitable reason).
- Keep the jump seats closed and the jump seats area clear.
- Try to send any suitable messages out of the aircraft with the freed hostages.
- If someone intends to open the doors from outside, the door automatically moves to the disarm position (for Airbus aircrafts). The doors of Boeing must be disarmed (the Cabin Crew are able to do so).
- Aircraft doors always must be kept fully open or in the closed position.
- If negotiations with the authorities have started, you should try to withdraw yourself from the main negotiating process and put the hijacker(s) in direct contact with the authorities concerned.
- If you are forced to act as a communication link between the hijacker(s) and the authorities, try to avoid answering questions from the authorities on behalf of the hijacker(s) and do not give advice for action by the ground organization.
- The crew is instructed to co-operate and communicate with the Pilot-in-Command all the time.
- Advise passengers to remain seated and to lean down when they hear a command (Cabin Crew must take the same position).

14.1.1.2.2 Aircraft on Ground During Stopover Operation

- Cabin Crew will command the passengers to lean down and hold their head with their arms.
- Cabin Crew will point out the location of the hi-jacker (s).

- Cabin Crew will help the ground staff to calm, to check and control passengers and to move out the injured ones.

14.1.1.2.3 Aircraft on Final Termination

Cabin Crew must avoid any press interview. If this is unavoidable; never give details, do not discuss any defense tactics, and do not give any name. For further action, the Cabin Crew must seek the authorities' approval.

14.1.1.3 Hijacker on the Flight Crew Compartment

If, despite all security precautions, a hijacker should succeed in entering the flight crew compartment, the crew shall, by careful but firm behavior, try to prevent the seat of an active crew member being occupied by the hijacker. The actual takeover of the airplane is the most dangerous phase of a hijacking.

14.1.1.4 Post-Hijacking Procedures

Contact with the head office shall be established directly or via a company station or via national diplomatic channels. Before facing the media, crew members should obtain prior advice from their company representative and ground authorities. Keeping the information or statements, which may assist any future hijacking attempts private is imperative vis-à-vis the media. If continuation of the flight is not possible, the Pilot-in-Command and his crew must stay with the passengers until their onward transportation has taken place.

14.1.2 Bomb Threat

Initially, any bomb threat received shall be taken seriously. Any bomb threat received or discovered before the aircraft has taken off is considered to be a bomb threat to an aircraft on the ground. Bomb threats are normally received in three different forms: by phone, in person (usually hearsay) and in writing, either electronically or handwritten.

The Pilot-in-Command will be informed of a threat received and subsequent security measures suggested/ taken. He shall get in contact with IOCC or the Aviation Security Department and inform the ATC accordingly by using available services described, whichever is practicable.

Since anyone working for Pegasus Airlines can receive a bomb threat, every station employee shall have access to a Bomb Warning Report Form with instructions on what to do in case they receive a bomb threat. Also, Pegasus Airlines should have a capability to trace and to record phone conversations in order to hear to them again for details initially missed and for prosecution purposes. Bomb threats are usually received on Pegasus Airlines phone lines but there have been some occasions where threats were made via other lines.

Bomb threats notification can also be received on board the aircraft during the boarding or taxiing process. They can be found in the lavatories, inside seat pockets or a passenger might make such a threat to a crew member or fellow passenger.

The cabin crew member who receives or sees the bomb threat shall advise the Senior Cabin Crew as well as the flight crew. The flight crew needs to get all the necessary information and relay it to the bomb threat assessor. Along with the bomb threat assessor, the Pilot-in-Command will determine whether there is a need for an evacuation and inspection.

14.1.2.1 Telephone Calls

The person receiving telephone threats shall:

- Listen carefully and make a note of the actual words used by the caller;
- Take such action as necessary to record the call, where this is not done automatically;
- Prolong the call and ask open questions to obtain as much information as possible.

14.1.2.2 Other Threats

The principles of threat assessment shall apply in order to handle the following situations:

- Written threats, including pictures, found on an aircraft.
- Verbal comments that may be received directly, overheard or relayed through a third party.
- Suspicious object: an item only becomes suspicious if it is not normal or if there is no innocent explanation. Suspicious objects shall not be moved without specialist advice.
- Unidentifiable substance: a substance only becomes suspicious if it is not readily identifiable and there is no logical explanation for its presence.

14.1.2.3 Air Carriers' Assessment

Bomb threats are either specific or non-specific. A specific bomb threat targets a specific aircraft. The threat mentions the flight number, the route of the aircraft or is found aboard a particular aircraft. A non-specific bomb threat only signals that a bomb is present on an air carrier's aircraft.

The bomb threat assessor is the Aviation Security Leader (RP). But, once the incident is reported to the local authority or the police, it is their responsibility to evaluate and manage all bomb threats made for airborne aircraft and the ones on the ground involving the facilities. Aviation Security Department and all the staff involved shall assist them throughout the process

Both specific and non-specific threats can present a serious threat. Just because there are no specific details as to which aircraft has a bomb on board, it does not automatically mean that it is a hoax.

Airport Police or the responsible authority and Pegasus Airlines Aviation Security Leader (RP) will use Positive Threat Identification (PTI) to determine whether the threat poses a real danger or not. PTI uses a series of Yes and No questions to determine the seriousness of the threat and also takes into account:

- the recent history of threat against the particular air carrier or airport;
- any industrial dispute within the air carrier;
- other disputes such as environmental or political protests;
- similar events which might prompt a copycat threat;
- high-profile persons at the airport or on board the flight;
- incidents during the checking-in process such as overbooking or a passenger being refused boarding;
- special cargo being carried on board.

PTI will lead the Airport Police and the Aviation Security Leader (RP) to one of the three following conclusions regarding the threat level.

Green	A warning which may not identify a target or a specific group of targets, or which lacks credibility. Present counter measures negate threat.
Amber	A warning that can be related to one or more targets but where there is doubt about its credibility or about the effectiveness of existing counter measures. This may involve danger and may require augmentation of counter measures.
Red	A specific warning where the threat is of a nature which permits identification of a specific target or where the caller has positively identified himself or the organization involved and is judged credible. Likely to involve danger to people, property or commercial activities and therefore merits counter measures.

Landing permission must not be refused. The Pilot in Command is responsible for the safety of his/her passengers, crew and aircraft. Under lawful command, the Pilot in Command has the authority to divert to an airfield of choice and for subsequently ordering an evacuation of the aircraft.

14.1.3 Bomb Threat Assessment in the Air

When a bomb threat is discovered on board an aircraft in flight, the responsibility for performing the assessment will lie with the operating Pegasus Airlines Aviation Security Leader (RP).

Whether a bomb threat is found or, especially, a suspect package, it shall be left in place by the Cabin Crew who finds it. A very detailed description shall be given to the Pilot-in-Command.

The Pilot-in-Command shall then relay the information to the ground and with the appropriate help will determine if the threat is serious. The Pilot-in-Command, with guidance from the Aviation Security Leader (RP), will apply PTI and the Pilot-in-Command will also consider the following:

(1) whether the threat originated before or after take-off and if the threat could have been discovered during the pre-flight search;

(2) whether there are precise details. In the case of a written threat, if the threat is very detailed and if an intention to avoid casualties is present it is more likely to be a genuine threat. If no clear reasons are mentioned, it is less likely that the threat is genuine. If a suspect package is found, the threat shall be considered genuine until proved otherwise;

(3) whether there is a person on board who might attract a threat;

(4) whether there are passengers who might be responsible for a threat;

(5) whether the incident is unique or part of a series of similar threats made to the same air carrier or same location;

(6) whether the Pilot-in-Command doubts the evidence relating to the threat; if so he shall consult with the law enforcement on the ground to get a clear picture of the threat level of the air carrier, States of departure and arrival.

If the threat to an aircraft in flight originates from the ground, this will be communicated to the flight after appropriate assessment by the air carrier. The communication may be in plain language or by discreet code transmission.

14.1.3.1 Red Alert - Aircraft In Flight

14.1.3.1.1 Communication With the Company

On very many occasions bomb threats are received by newspaper offices, Air Traffic Control or Airport Authorities and these threats are sometimes passed to the Pilot-in-Command before the Company has become aware of them.

Whenever possible and when time permits, the Pilot-in-Command shall make an attempt to contact the Company via ACARS/VHF to ascertain if the information has been received by them and agree on the category (Red, Amber or Green Alert) before arriving at his decision to divert or return to the point of departure. Nothing in this instruction shall in any way be construed as removing discretion from the Pilot-in-Command. His authority in this matter is absolute and he may come to any decision which he sees fit under the circumstances. The intention is merely to suggest a course of action which might, on occasions, help the Pilot-in-Command to arrive at his decision.

14.1.3.1.2 Information to Passengers / Security Organizations

In case of a bomb threat against a Pegasus Aircraft in flight with passengers on board, the notification to passengers will be at the discretion of the Pilot-in-Command and based on the circumstances.

If required, make a PA announcement to passengers, informing them that a landing is being made for operational reasons.

The IOCC and Security Organization of the airport of departure and/or destination must be informed and involved.

14.1.3.1.3 Cockpit Procedures

NOTE	If there is a procedure on the FCOM or QRH please apply the procedure on the flight manuals (e.g. Airbus)

14.1.3.1.3.1 Boeing

The Operations Controller, Duty Dispatcher or Senior Station Official, will inform the Pilot-in-Command immediately, either by use of the Company VHF or Air Traffic Control; on receipt of such a message the Pilot-in-Command of the aircraft shall proceed as follows:

- Ascertain as much information as possible about the nature and source of the message to confirm that it meets the Company “Red Alert” criteria.
- In the event the aircraft is in the air, the Pilot-in-Command will endeavour to land at a suitable airport within 30mins. When making this decision the Pilot-in-Command shall, whenever possible, choose an airfield with suitable let-down aids; one with which he is familiar and at which there are reasonable ground handling facilities, e.g. the Company normal destination or approved alternate destination.
- Subject to terrain clearance, weather conditions and fuel reserves, descend to below 10,000ft or MORA and MOCA, whichever is higher, and depressurize the aircraft to minimize the effect of an explosion in the fuselage. In carrying out this procedure, a relatively fast rate of descent (2-3000 feet per minute) shall be used but the full emergency descent procedure shall not be followed. When depressurizing the cabin, care shall be taken to ensure that the cabin altitude is not raised above the altitude existing at the time of receipt of the alert message. This precaution is aimed at minimizing the risk of triggering off a barometric type fuse. If possible, adopt approach configuration (flaps in intermediate position and gear down).
- Declare an emergency and request Air Traffic Control to notify the relevant authorities.
- Make a PA announcement to passengers, informing them that a landing is being made for operational reasons.
- Request ATC to have passenger steps available for immediate disembarkation of passengers in a position well away from all buildings and other aircraft (most airport authorities have a designated area for this event).

After landing the crew will take the precautions as described above for “RED ALERT ON THE GROUND”, taxi to the airport designated bomb disposal area.

When the Pilot-in-Command is satisfied that ALL security measures have been carried out, and the aircraft is CLEAN, the flight may continue.

14.1.3.1.3.2 Airbus

Background

The Duty Dispatcher or Senior Station Official will inform the Pilot-in-Command immediately, either by use of Company VHF or Air Traffic Control; on receipt of such a message the Pilot-in-Command of the aircraft shall proceed as follows:

- Ascertain as much information as possible about the nature and source of the message to confirm that it meets Company “Red Alert” criteria.
- Avoid the activation of an altitude-sensitive bomb; the cabin altitude shall not exceed the value at which the bomb has been discovered
- Reduce the effects of the explosion; the aircraft shall fly as long as possible with approximately 1 PSI differential pressure, to help the blast go outwards. 1 PSI differential pressure corresponds to a 2.500-ft. difference between the aircraft and the cabin altitude.

These conditions are achieved by using the manual pressure control.

Procedures

It is assumed that the following procedure is initiated during climb or cruise:

- First, maintain the cabin altitude using manual pressure mode.
- While maintaining the cabin altitude, descend the aircraft to the cabin altitude + 2.500 ft. and maintain delta P at 1 PSI.

- During further steps of descent, maintain delta P at 1 PSI using the cabin V/S target selector.
- During the approach, use automatic pressure mode in order to reduce the differential pressure to zero at touchdown.

If flight conditions are different, the crew shall adapt the procedure, bearing in mind the above-mentioned principles (see 'Background' paragraph).

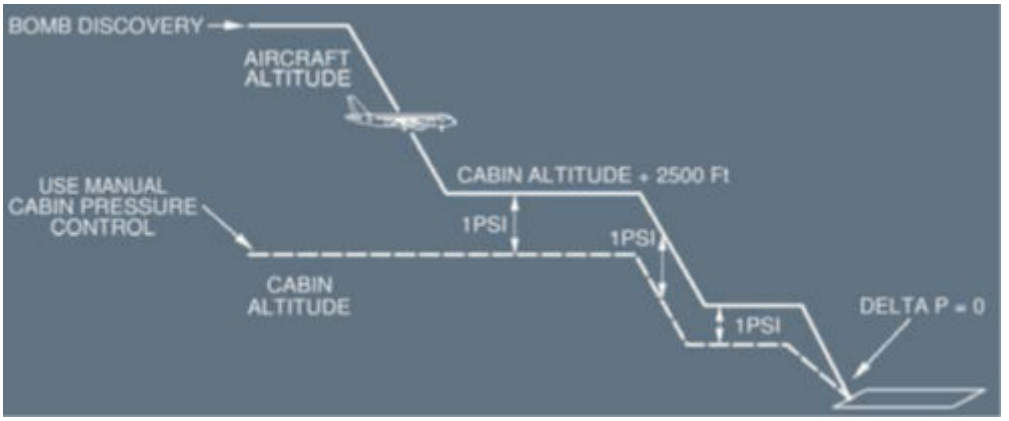


Figure 14-1:

CKPT / CAB COM	**ESTABLISH**

- **If landing and evacuation is possible within 30 min:**

ATC / COMPANY	**NOTIFY**
EVAC	**PREPARE**

- **If landing and evacuation is NOT possible within 30 min:**

AIRCRAFT (IF CLIMBING)	**LEVEL OFF**
CABIN PRESS MODE SEL	**MAN**

The purpose is to immediately prevent the cabin altitude from increasing, in order to avoid the activation of an altitude-sensitive bomb.

MAINTAIN CAB ALT

Use MAN V/S CTL selector to maintain the cabin altitude at the value it had when the bomb was discovered.

ATC / COMPANY	**NOTIFY**

To obtain expert advice from explosive specialists.

TRGT SPEED: PREFER LO IAS

Low speed could reduce the consequences of possible structural damage, if the bomb explodes.

DESCENT TO CAB ALT + 2 500 ft or MEA - MORA	**INITIATE**

Descending to 2 500 ft above the cabin altitude gives a cabin differential pressure of approximately 1 PSI, which helps to ensure that the blast goes outwards, if the bomb explodes.

AVOID SHARP MANOEUVRES which might result in the bomb moving.

MAINTAIN CAB ALT

Use MAN V/S CTL selector to maintain the cabin altitude. Initially brief UP input shall be required; but, be careful not to increase the cabin altitude.

- **When at CAB ALT + 2 500 ft.:**

MAINTAIN 1 PSI ΔP

Use MAN V/S CTL selector to adjust delta P to 1 PSI. Brief DN input shall be initially required to set 0 ft./min cabin vertical speed.

GALLEY	**OFF**
FUEL RESERVES	**DETERMINE**

When flying at cabin altitude + 2 500 ft., fuel consumption in CONF 1, with landing gear down, will be about 2.1 times that consumed in clean configuration.

- **When bomb secured at the LRBL or cannot be moved:**

Least Risk Bomb Location (LRBL) is the centre of the RH aft cabin door.

EMER EXIT LT	**ON**

To recover minimum cabin lighting when the COMMERCIAL pb-sw will be switched OFF.

COMMERCIAL	**OFF**

- **If fuel permits:**

FLAPS	**AT LEAST CONF 1**
L/G lever (except for flight over water)	**DOWN**

The detonation could damage the landing systems. Therefore, if fuel permits, configure the aircraft for landing as soon as possible. Reducing the speed will minimize stress on the aircraft structure.

USE NORMAL CONF FOR LANDING

DURING FURTHER DESCENT: MAINTAIN MAX 1 PSI ΔP

Use MAN V/S CTL selector to DN to adjust delta P to 1 PSI.

- **During approach:**

CABIN PRESS MODE SEL	**AUTO**

This allows CPC to automatically control the cabin altitude to 0 during final approach.

- **When aircraft on ground and stopped in a remote area (if possible):**

Refer to PRO-ABN-MISC [QRH] EMER EVAC.

14.1.3.1.4 Cabin Procedures

If a suspect device is found in the cabin:

WARNING	Do not cut or disconnect any wires and do not open or attempt to gain entry to internal components of a closed or concealed suspect device. Any attempt may result in an explosion. Booby-trapped closed devices have been used on aircraft in the past.
WARNING	Alternate locations must not be used without consulting with an aviation explosives security specialist. Never take a suspect device to the flight deck.
CAUTION	The least risk bomb location for the aircraft structure and systems is the centre of the RH aft cabin door.

EOD PERSONNEL ON BOARD	**CHECK**

Announce “Is there any EOD personnel on board?”. By using the initials, only persons familiar with EOD (Explosive Ordnance Disposal) will be made aware of the problem.

- DO NOT OPEN THE BOMB
- DO NOT CUT BOMB'S WIRES
- SECURE BOMB AGAINST SLIPPING
- PROTECT BOMB AGAINST SHOCKS

Secure in the attitude found and do not lift before having checked for an anti-lift ignition device.

PASSENGERS **LEAD AWAY FROM THE BOMB**

Move passengers at least 4 seat rows away from the bomb location. On full flights, it may be necessary to double up passengers to achieve standoff from the suspect device. Passengers near the bomb shall protect their heads with pillows, blankets.

All passengers must remain seated with seatbelts on and, if possible, head below the top of the head rest. Seat backs and tray tables shall be in their full upright position.

Service items may need to be collected in order to secure tray tables.

PORTABLE ELECTRONIC DEVICES **SWITCH OFF**

The cabin crew must command passengers to switch off all portable electronic devices.

BOMB **CHECK NO ANTI-LIFT DEVICE**

To check for an anti-lift switch or lever, slide a string or stiff card (such as the emergency information card) under the bomb, without disturbing the bomb.

If the string or card cannot be slipped under the bomb, it may indicate that an anti-lift switch or lever is present and that the bomb cannot be moved.

If a card is used and can be slid under the bomb, leave it under the bomb and move together with the bomb.

If it is not possible to move the bomb, then it shall be surrounded with a single thin sheet of plastic (e.g. trash bag), then with wetted materials and other blast absorbing materials such as seat cushions and soft carry-on baggage. Move personnel as far away from the bomb location as possible.

EMERGENCY EQUIPMENT **REMOVE AND STOW**

Emergency equipment (PBE, fire extinguisher, ...) located close to the LRBL must be removed and stowed in an alternative location.

GALLEY/IFE POWER **OFF**

All galley and IFE equipment located close to the LRBL must be switched off.

- **If the bomb can be moved:**

RH AFT CABIN DOOR SLIDE **DISARM**

LEAST RISK BOMB LOCATION (LRBL) **PREPARE**

Build up a platform of solid baggage against the door up to about 25 cm (10 in) below the middle of the door.

On top of this, build up at least 25 cm (10 in) of wetted material such as blankets and pillows.

Place a single thin sheet of plastic (e. g. trash bag) on top of the wetted materials. This prevents any possible short circuit.

CAUTION	DO NOT OMIT THE PLASTIC SHEETS, AS THE SUSPECT DEVICE COULD GET WET AND POSSIBLY SHORT CIRCUIT ELECTRONIC COMPONENTS CAUSING INADVERTENT DEVICE ACTIVATION.

BOMB INDICATION LINE **POSITION**

NOTE	A bomb location indicator line is 6 to 8 ft. (1.8 to 2.4 m) (e.g. neckties, headset cord, or belts connected together) preferably of contrasting colour, that helps the responding bomb squad find the precise location of the suspect device within the LRBL stack once constructed.

Position the bomb indication line from the location on the platform where you will place the suspect device, EXTENDING outward into the aisle.

BOMB **MOVE TO LRBL**

Carefully carry in the attitude found and place on top of the wetted materials in the same attitude and as close to the door structure as possible.

CAUTION	Ensure that the suspect device, when placed on the stack against the door, is above the slide pack but not against the door handle and, if possible, avoid placement in the view port.

LEAST RISK BOMB LOCATION (LRBL) **COMPLETE**

Place an additional single thin sheet of plastic over the bomb.

CAUTION	DO NOT OMIT THE PLASTIC SHEETS, AS THE SUSPECT DEVICE COULD GET WET AND POSSIBLY SHORT CIRCUIT ELECTRONIC COMPONENTS CAUSING INADVERTENT DEVICE ACTIVATION.

Build-up 25 cm (10 in) of wetted material around the sides and on top of the bomb.

DO NOT PLACE ANYTHING BETWEEN THE BOMB AND THE DOOR AND MINIMIZE AIRSPACE AROUND THE BOMB.

The idea is to build up a protective surrounding of the bomb so that the explosive force is directed in the only unprotected area into the door structure.

Fill the area around the bomb with seat cushions and other soft materials such as hand luggage (saturated with water or any other non-flammable liquid) up to the cabin ceiling, compressing as much as possible. Secure the LRBL stack in place using belt, ties or other appropriate materials. The more material stacked around the bomb, the less the damage will be.

USE ONLY SOFT MATERIAL. AVOID USING MATERIALS CONTAINING ANY INFLAMMABLE LIQUID AND ANY METAL OBJECTS WHICH COULD BECOME DANGEROUS PROJECTILES.

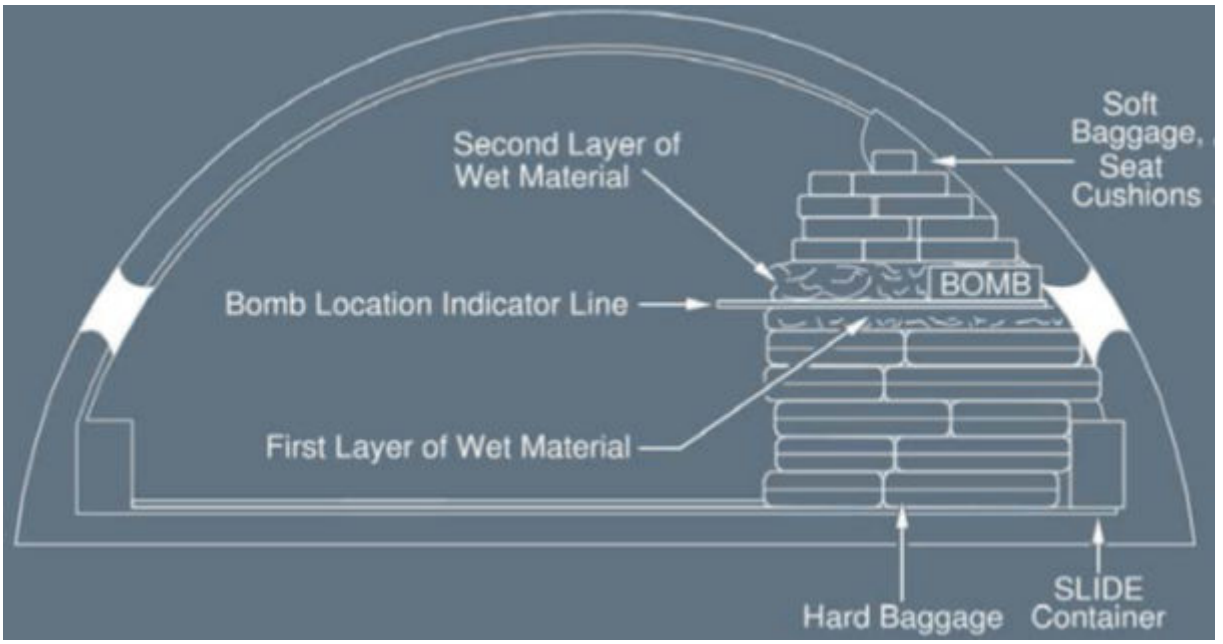


Figure 14-2: LRBL Stack

PASSENGERS **MOVE/ADVISE**

Move passengers at least 4 seat rows away from the least risk bomb location (RH aft cabin door). On full flights, it may be necessary to double up passengers to achieve standoff from the suspect device.

Passengers near the bomb shall protect their heads with pillows, blankets. All passengers must remain seated with seatbelts on and, if possible, head below the top of the head rest. Seat backs and tray tables must be in their full upright position.

CABIN CREW **NOTIFY COCKPIT CREW**

Cabin crew notify the flight crew that the bomb is secured at the LRBL.

EVACUATION/DISEMBARKATION **EXECUTE**

Evacuate through normal and emergency exits on the opposite side of the "bomb" location. Do not use the door just opposite the "bomb".

Use all available airport facilities to disembark without delay.

14.1.3.1.5 In-Flight Search

In cases where a credible threat is made while the aircraft is in flight, it will be necessary for cabin crew members to perform an in-flight search. If a crew member notices an item they consider inappropriate to be carried in the cabin, the PIC shall be notified and the law enforcement authorities alerted in order to rectify the situation and take appropriate actions.

Depending on the gravity of the current security situation and seriousness of the partial threat, at the Pilot-in-Command's discretion, a search of the aircraft maybe undertaken.

The aircraft crew with their specialist knowledge are the most competent search personnel and are most likely to be able to recognize what they are searching for.

Since explosive devices can be disguised in many ways, the general guidelines are:

- An obvious device
- A package or object that fits the description contained in the threat
- A package or object which is foreign to its environment
- A package or object that is in its environment, but which shows signs of having been tampered with. In exceptional circumstances, expert assistance may be obtained from among the passengers.

The extent of the search will be governed by the amount of information contained in the warning and the accessibility of the aircraft at the previous stop(s) on the ground.

The search shall include Crew Baggage, Navigation Bags, Aircraft Equipment, Galleys, Overhead Bins, Toilets, and Coat Spaces etc.

Before the search proceeds with, the Pilot-in-Command shall make a suitable PA announcement, explaining the situation to the passengers, requesting that they remain in their seats and co-operate with the crew. The "Seat Belt/No Smoking" signs shall be switched on.

14.1.3.1.5.1 In-Flight Cockpit Bomb Search

In case where the PIC decides to undertake a security search, the cockpit shall be searched by the Flight Crew according to the checklist PG-GU-BK-001 - Aircraft Security Search Information Card, available in the EFB.

In-Flight Cabin Bomb Search

In the event that the Pilot in Command (PIC) deems a cabin bomb search necessary, each cabin crew member is responsible for conducting a detailed search of assigned areas, following the items mentioned in the ISEC Checklist (for further details, refer to PG-KH-EK-001 - Cabin Crew Manual, available in Comply365).

14.1.4 Threats to Aircraft on the Ground

When dealing with suspect explosive devices incidents it is important to use common terminology so as to minimize misunderstandings. The following definitions are used by many explosive disposal experts and agencies, and it is recommended they shall be adopted internationally when dealing with incidents.

Improvised Explosive Device (IED). An explosive device placed or fabricated by terrorists or criminals. These devices may incorporate military explosives stores (shells, grenades etc.), but are normally devised from non-military components.

Bomb Warning/Threat. The manner in which an Improvised Explosive Device (IED) incident starts. This is usually by telephone, but also covers an alarm raised by the discovery of a device.

Bomb Scare. The Bomb Warning/Threat has been investigated or assessed and discredited. No device was found, any precautionary measures have been relaxed and normal activity resumed.

False Alarm. A suspect IED was discovered and the Explosive Disposal resources tasked. Investigation of the item by the explosive disposal experts reveals the item to be innocent, i.e. left without evil intent, and containing no explosive device or substance.

Hoax. A suspect IED was discovered and the Explosive Disposal resources tasked. Investigation of the item by the explosive disposal experts reveals it to be constructed to resemble a viable IED but containing no explosive or dangerous substance.

14.1.4.1 Red Alert - Aircraft on the Ground

If a RED ALERT is initiated when the aircraft is on the ground, the Station Manager, Airport Representative, or appointed Ground Handling Agent will take the following action:

(1) Consult with the Pilot-in-Command and the IOCC to ensure that the aircraft does not depart from the station.

(2) Notify the Airport Management and Airport Police.

(3) Disembark passengers (if boarded), requesting them to take all their personal belongings from the cabin (if time permits)

(4) Have the aircraft towed to the designated area if required by the Airport Authorities.

(5) Check freight and mail manifests.

(6) All baggage to be identified by the passengers. Unclaimed or unaccompanied baggage shall be removed. Transfer baggage from other airlines that is not claimed by a passenger shall be treated as unaccompanied.

(7) Catering equipment to be searched and any unidentified items removed.

(8) Aircraft to be searched in accordance with Security Inspection procedures detailed in the security programme by the security specialist of the local authority. This duty shall be carried out under the direction of the Station Engineer. However, where none is available, it will be the duty of the Pilot-in-Command and Crew to carry out the search.

The decision on the implementation of any or all of items above shall be made rapidly and communicated clearly by the Station Manager (or Agent) to all relevant parties. The Station Manager (or Agent) is responsible for full coordination of the activity from start to finish.

The senior official present or the Pilot-in-Command shall inform the passengers that a security check is being carried out. All items removed from the aircraft will be subjected to a security search or other agreed procedure for clearance at that station and due provision shall be made for the safe keeping of any baggage, cargo or mail and its eventual return or onward shipment.

14.1.4.1.1 Information to Passengers / Security Organizations

In case of a Bomb Threat against a Pegasus Aircraft on the ground with passengers on board, the Pilot-in-Command shall inform the passengers of the situation and of his intentions. In flight the Pilot-in-Command shall use his judgment regarding the amount of information he gives to the passengers.

In any case the Security Organisation of the airport of departure and/or destination must be informed and involved.

If a bomb threat is associated with an aircraft that is still on the ground, aircraft operators, in consultation with airport authorities and other law enforcement entities responsible shall, once the warning has been assessed:

(1) disembark all passengers and crew with all their cabin baggage by steps or jetties; escape slides shall only be used in extreme emergencies;

(2) move the aircraft to a remote location such as the isolated aircraft parking position;

(3) isolate and re-screen all passengers and their cabin baggage and hold them in a separate area until the crew members, hold baggage and cargo and catering supplies have been inspected and/or screened, searched and declared safe;

(4) unload all hold baggage and require passengers to identify their baggage, which shall then be screened or searched before it is reloaded;

(5) unload all cargo, which shall then be screened or searched before it is reloaded;

(6) check the integrity of catering supplies; and search the aircraft. Such a search shall be conducted only by designated and appropriately trained staff from law enforcement authorities.

14.1.4.1.2 Search on the Ground

(1) Consult with the Pilot-in-Command and the IOCC to ensure that the aircraft does not depart the station.

(2) Notify Airport Management and Airport Police.

(3) Disembark passengers (if boarded) requesting them to take all personal belongings from the cabin (if time permits).

(4) Have aircraft towed to the designated area if required by the airport authorities.

(5) Check freight and mail manifests.

(6) All baggage to be identified by the passengers. Unclaimed or unaccompanied baggage shall be removed. Transfer baggage from other airlines that is not claimed by a passenger shall be treated as unaccompanied.

(7) Catering equipment to be searched and any unidentified items removed.

(8) Aircraft to be searched in accordance with Security Inspection procedures detailed in the security programme by the security specialist of the local authority. This duty shall be carried out under the direction of the Station Engineer. However, where none is available, it will be the duty of the Pilot-in-Command and Crew to carry out the search.

(9) Pegasus Airlines PG-GU-BK-002 – Aircraft Security Search Information Card (available in Comply365 and Pegasus EFB Application) can be implemented as a guidance while search or inspection of an aircraft by the specialist local authority is underway.

The decision on the implementation of any or all of the items above shall be made rapidly and communicated clearly by the Station Manager (or contracted handling agents) to all relevant parties. The Station Manager (or contracted handling agent) is responsible for reporting to IOCC and for full co-ordination of the activity from start to finish.

The senior official of the airport security or the contracted handling agents present, or the Pilot-in-Command shall inform the passengers that a security check is being carried out. All items removed from the aircraft will be subjected to a security search or other agreed procedure for clearance at that station and due provision shall be made for the safe keeping of any baggage, cargo or mail and its eventual return or onward shipment.

14.1.4.2 Sabotage

Sabotage is an act of intentional omission, intended to cause malicious or wanton destruction of property, endangering or resulting in unlawful interference with civil aviation and its facilities.

A sabotage threat, whether anonymous or not, shall be treated as real.

During the period “Doors closed” to “Doors opened”, the Pilot in Command is responsible for taking action against the sabotage attempt. To reduce the potential for sabotage of the aircraft, all crew members and technicians shall be on the highest vigilance when working on or near the aircraft. Any suspicious activity shall be questioned immediately and brought to the attention of the Pilot-in-Command of the flight.

If a sabotage warning has been received, point 14.1.4.1. procedures shall be followed.

14.1.4.2.1 Unlawful Interference With Aircraft in Flight

Acts of unlawful interference are acts such as:

(a) violence against a person on board an aircraft on the ground or in-flight if that act is likely to endanger the safety of that aircraft;

(b) destroying an aircraft in service or causing damage to such an aircraft which renders it incapable of flight or which is likely to endanger its safety in-flight;

(c) placing or causing to be placed on an aircraft in service, by any means whatsoever, a device or substance which is likely to destroy that aircraft, or cause damage to it which renders it incapable of flight, or cause damage to it which is likely to endanger its safety in-flight;

(d) destroying or damaging aerodrome installations, air navigation facilities or interfering with their operation, if any such act is likely to endanger the safety of the aircraft;

(e) communicating information which is known to be false, thereby endangering the safety of an aircraft in-flight;

(f) unlawfully and intentionally using any device, substance or weapon.

Should an aircraft in-flight be subjected to unlawful interference, the Pilot In Command shall endeavour to set the transponder to Mode A Code 7500 to give an indication of the situation, unless circumstances warrant the use of Code 7700.

When a pilot has selected Mode A Code 7500 and is subsequently requested to confirm his code by ATC, he shall, according to circumstances, either confirm this or not reply at all.

NOTE	The absence of a reply from the pilot will be taken by ATC as an indication that the use of Code 7500 is not due to an inadvertent false code selection.

14.1.5 Discovery of a Suspect or Prohibited Article

If any object is located during an aircraft security search and cannot be identified, it must be dealt with as a “suspect” item.

Action by the searcher:

- Do not touch;
- Notify the supervisor;
- Remember the description of the object and its location.

The Appropriate Authority shall be notified immediately so that specialized personnel may deal with the suspect item without delay. Subject to the advice of these personnel, consideration shall be given to towing the aircraft to a safe area to minimize the risk to the public, other aircraft and terminal facilities.

All persons, except emergency responders, will be kept at a minimum distance as decided by the Appropriate Authority.

Fire-fighting services shall be on standby to deal with an explosion or fire until such time as the bomb disposal personnel declare the suspicious item or substance to be safe.

After the suspect item is declared safe, search procedures shall be completed to ensure that no secondary device or substance is on the aircraft.

14.1.6 Dealing with Chemical/Biological Weapon (CBW)

In this section, information will be introduced about Chemical/Biological Weapons (CBW). The situation is similar to the above subject. Principally, almost the same operational procedures will be applied. A critical distinction to be made is the difference between the handling of a bomb and CBW.

14.1.6.1 Aerosol CBW Activation

A primary method of distributing chemical and biological agents inside the aircraft is aerosol dispersion. The action of leaking, exploding or manually pouring the substance into the cabin interior will move the agent through simple airborne transmission onto the skin or into the eyes, lungs and nasal passages. It will be the goal of crew members to contain the weapon's aerosol potential before it spreads through the cabin atmosphere or, if this is not possible, to minimize its effect on passengers and crew.

14.1.6.2 CBW Threats in Cabin - Without Activation

If a CBW is reported to be on the aircraft it shall be noted that exposure to biological or chemical agents may not result in an immediate presence of symptoms or be immediately detectable. The crew must take immediate steps to deal with the situation and attempt to minimize aerosol dispersion. The Flight and Cabin crew have different duties that shall be started simultaneously.

(1) Flight crew shall immediately don masks, goggles, select 100% oxygen,

(2) Cabin crew shall minimize skin coverage with shirt sleeves down or uniform jackets worn.

Some CBW agents are odourless and will not be sensed until it is too late, so this step shall not be delayed. Although an emergency declaration and turn towards an alternate aerodrome is appropriate, an immediate change in cabin pressure shall not be initiated until the inactivated device is secured to the maximum extent possible. Immediately reducing cabin temperature to the lowest practical setting and turning off recirculation fans will decrease most aerosol dispersion characteristics.

Once the suspected Chemical/Biological container is covered and sealed from the cabin atmosphere, a gradual descent of the aircraft can be initiated using a descent that minimizes the rate of cabin change. The slower the descent and increase in cabin pressure, the lower the risk of agent dispersal during the final phase of flight.

14.1.6.3 CBW Threats in Cabin - With Activation

Except for slow-acting biological agents, such as anthrax, airborne exposure to toxic agents may rapidly generate sudden passenger sickness in an epidemic outbreak. Generally, many biological agents will generate symptoms less rapidly than will chemical agents, many of which cause immediate symptoms. Depending on the agent, passengers and cabin crew may exhibit choking, discolouration and fainting, blistering or convulsions that are beyond the means of crew members to effectively deal with while airborne.

Flight crew members must don masks and goggles before any other action.

Turn on the passenger oxygen switch. Secure the cabin door and deny any entry from the cabin. Then decrease the cabin pressure as quickly as possible by raising the cabin altitude, -, which will help evacuate and dilute the aerosol chemical agent. Recirculation fans shall be turned off and the coldest possible temperature shall be selected to aid in minimizing agent aerosol dispersion.

Cabin crew and passengers shall go on oxygen. A rapid descent and an immediate landing are paramount for ensuring the flight crew is physically able to land the aircraft and gain time-critical medical treatment for exposed individuals.

14.1.6.4 CBW Threats in Cargo Compartment

A reported CBW threat in the cargo compartment shall be dealt with much as one would deal with a cargo fire: isolate the cargo bay by removing all sources of ventilation and turn off the recirculation fans. In-flight activation of a CBW may be sensed by smoke detectors in the cargo hold. Normal firefighting techniques will provide optimal protection. During descent, a positive outflow of pressure from the air-conditioning packs will decrease the risk of chemical agents migrating from the cargo bays and into the cabin. Setting the landing elevation lower than the actual destination will keep the cabin relatively over pressurized throughout the landing phase. Manually keeping outflow valves from fully opening upon landing could keep the cabin over-pressurized and protected from cargo area contamination until ready for emergency evacuation through upwind exits.

14.1.6.5 Brief Information for Landing After a CBW Threat

In any CBW threat situation, do not taxi to a terminal area after landing, but instead seek a location downwind of any populated structures. The aircraft shall be parked diagonally to the reported surface winds and disembarking shall be undertaken only on the upwind side of the aircraft. All passengers and crew shall be kept together and quarantined from non-emergency personnel.

14.1.6.6 Flight Crew Checklist For In-Flight CBW Threat Identification

14.1.6.6.1 CBW in Cabin But Inactivated

- Don mask and goggles,
- Inform ATC and declare emergency, squawk 7700,
- Do not change altitude until procedure directs,
- Turn off recirculation fans, decrease cabin temperature,
- Attempt to contain/wrap device,
- Consider turning the passenger oxygen switch on,
- Initiate slow descent to appropriate alternate aerodrome,
- Quarantine passengers upwind of aircraft until assistance arrives.

14.1.6.6.2 CBW in Cabin But Activated

- Don mask and goggles,
- Turn passenger oxygen switch on,
- Inform ATC and declare emergency, squawk 7700,
- Turn off recirculation fans,
- Raise cabin elevation to 10000 feet at the fastest rate possible,
- Decrease cabin temperature to the coolest possible,
- Execute emergency descent procedure,
- Upon landing, evacuate aircraft via upwind side of airplane,
- Quarantine passengers upwind of aircraft until assistance arrives.

14.1.6.6.3 CBW in Cargo Hold

- Don mask and goggles,
- Inform ATC and declare emergency, squawk 7700,
- Turn off recirculation fans,
- Accomplish cargo fire checklist,

- Consider turning the passenger oxygen switch on,
- Maintain positive cabin pressure until landing,
- Stop aircraft with surface wind at 10/2 o'clock position,
- Evacuate aircraft via upwind side of airplane,
- Quarantine passengers upwind of aircraft until assistance arrives.

14.1.6.7 Cabin Crew Checklist For In-Flight CBW Threat Identification

A suspicious package may have oily stains, discoloration or odour. A suspicious substance may be a white, tan or beige coloured powder and have the consistency and texture of talcum powder.

14.1.6.8 Discovery of a Suspicious Spilled Substance

- **Do not try to clean up the substance.**
- Advise the Pilot in Command.
- Turn ventilation down to minimum.
- Breathe oxygen and have the passengers breathe oxygen.
- If contact has been made with the substance, immediately wash hands and forearms repeatedly.
- Don protective equipment; gloves and mask.
- Cover the substance immediately with anything suitable to hand, then create as many barrier layers as possible between the agent and the cabin atmosphere by covering the item with multiple layers of plastic trash bags, dry blankets, more plastic, wet blankets, then more dry blankets to minimize leakage and spreading. Isolate the area.
- Do not allow anyone to approach the substance in a radius of 3 meters.
- Have any individuals exposed to the substance wash their hands and forearms.
- Change clothing that may have been contaminated and place it in a sealed bag.

14.1.6.9 Discovery of a Suspicious Package/Enveloppe

- **Do not shake or empty contents of envelope and package.**
- Advise the Pilot in Command.
- Crew to consider going on oxygen.
- Don protective equipment; gloves and mask.
- Cover all exposed skin.
- Isolate the area.
- Do not move the item.
- Cover the substance as mentioned in the above paragraph.
- Consider passengers to go on oxygen.

14.1.7 Equipment Failure

In the event of any equipment failure involving security at the airport (e.g. x-ray machines, walk-through detectors, hand detectors, etc.) then the Pilot-in-Command will be informed, and the handling agent will be responsible for ensuring that both passengers and their baggage are searched by one of the other methods as stated in point 5.4. In addition, the Pilot-in-Command may request a manual Baggage ID to be carried out prior to flight as directed in 7.2.1.

14.1.8 Enhanced Measures for an Increase in the Level of Threat

Pegasus Airlines increases the company security level on its flight from “Class 1 up to Class 2 “security level when it receives any security threat message from the relevant security authorities.

(1) Pegasus Airlines has the right to refuse uplift of cargo and airmail during times of increased threat level or if it believes that the contents of the cargo and mail shipments pose a risk to safe operation of the aircraft.

(2) Passengers and crew members boarding flights which are considered under increased threat shall be escorted by airport security services personnel if they must leave the confines of the passenger building to board the aircraft. This is to prevent infiltration by potential perpetrators or, in more extreme cases, to guard against attack from surrounding areas. This shall apply whether the passengers are walking or are transported in vehicles.

(3) If a particular flight is under an increased threat, all passengers and their cabin baggage may be offloaded during the transit stop and an inspection of the interior of the aircraft carried out to ensure that no items have been left on board.

(4) In addition, the Pilot-in-Command may request a manual Baggage ID to be carried out prior to flight as per directed in 7.2.1.

14.1.9 Security Alert Signals

These messages will be originated by IOCC at the instigation of the General Manager, Chief Flight Operations Officer, Chief Safety and Security Officer and Aviation Security Leader (RP) or another nominated manager as stated in PG-EM-EK-002 ERM. The IOCC may initiate an alert to meet an immediate threat and such a message will normally be for a specified duration, subject to a re-warning in 24 or 48 hours.

The required security standard will be applied for the time stated in the alert message or until a stand down message is received, whichever is soonest. Every alert message will quote the current standard as well as noting the necessary increase. At the expiry of the validity of that message, revert to the “current” standard quoted.

This procedure does not in any way preclude any official or agent of Pegasus Airlines from applying any or all standards of security at a particular time or to a particular flight, in the event of an urgent need arising. Such actions shall be reported to the IOCC as soon as possible so that an alert may be extended if necessary.

It is imperative that each station acknowledges receipt of Security Messages promptly. All signals will be addressed to the Station Manager or Handling Agent and to the Tour Operator. An acknowledgement from either one will indicate that there has been a check between offices and that both are now alerted.

14.1.9.1 Message Format

The first words of the text will always be “SECURITY ALERT” or “SECURITY STANDDOWN”. The message will follow in six parts.

(a) Duration of alert; next advice or stand down, quoting date and time.

(b) Flights or routes to which the alert is applicable.

(c) Current security standard, followed by required standard using numerical code.

(d) Buildings and installations to which the alert is applicable.

(e) Current security search class, followed by the required search class using the numerical code.

(f) Any plain language message necessary. (See examples of Security Alert message format below)

	Example 1 - Security Alert	**Example 2 - Security Stand Down**

To	Aviation Security Department	Aviation Security Department
From	OPS Units	OPS Units
a.	Until April 30 - 2359	From May 1 0800
b.	All flights Türkiye/Germany and VV	All routes
c.	Present Class 1, apply Class 2.	Present Class 2, revert to Class 1.
d.	All offices and installations	All offices
e.	Present Class 1 Security Level, apply Class 2 Security Checklist.	Present Class 2 Security Level, revert to Class 1 Security Checklist
f.	Due to general unstable situation.	Nil

14.2 SECURITY STANDARDS

14.2.1 Classifications

Security standards are defined for use by those with line responsibility to deal with any known threat. Certain flights or routes may be designated security risks and standards for these will be laid down by the General Manager-EVP-Technical operations. In addition, foreign administrations may require special security measures at a particular time. It is the company policy to comply with such requirements and local management shall immediately notify the CSSO, the Aviation Security Leader (RP) and the CFOO when these arise.

14.2.2 Security Level Class 1

Class 1 is the normal Security Level.

- All checked baggage has to be properly labelled and secured against pilferage.
- Passenger coupons are checked to ensure they are genuine and valid for travel.
- Cargo and mail properly labelled and secured.
- Catering, bars and aircraft stores secured and sealed to avoid pilferage.
- Aircraft steps removed from the aircraft at night and in unattended areas.
- Passengers and hand baggage checked to ensure no firearms; , weapons or explosives are carried. The local standard system for carrying out such checks is acceptable and shall be fully utilized, unless special prior arrangements have been made by the Aviation Security Department
- A final count of passengers boarding is made and the total reconciled with the check-in figures.
- Accompanied baggage reconciliation, including personal identification where necessary to confirm final status.
- Ground handling personnel and crew to be alerted to be vigilant during the turn-around.
- Aircraft to be parked in a secure area.
- Aircraft to be locked and steps removed when not in use.
- Aircraft to be checked prior to departure in accordance with “Clean Aircraft Check” searches under the point 8.2.1. This is done in accordance with the Pegasus Air Carrier Security Programme.
- All catering, galley and aircraft stores to be authenticated.
- No unidentified packages or bags to be boarded.

14.2.3 Security Level Class 2

Class 2 is the increased Security Level.

- No cargo to be shipped, unless opened and physically checked or satisfactorily cleared by X-Ray or other device if available.
- Airport Management and Airport Police to be advised that special precautions are in force.
- Special attention is required to the security of the aircraft and/or passenger assembly areas.

During Class 2, security level conditions are recorded primarily using EFB or, in any case where EFB cannot be used, with PG-GU-FR-001 – Aircraft Security Search Information Form (available in Comply365 and Pegasus EFB Application) and the implementation is described in PG-GU-KB-00014 - Additional Security and Class 2 Security Level Implementation (available in Comply365 and Pegasus EFB Application) and under the point 8.2.1.

In addition, any other measures may be required by the Aviation Security Leader (RP) to meet specific threats.

14.2.4 High-Risk Flights

Whenever there is a permanent or a short-term threat situation requiring a higher level of attention, the related flights can be defined as high-risk flights.

These kinds of flights need additional security measures which must be enforced for the entire timeframe established by the competent Authority.

The required security measures are applied to departing, arriving or transit flights and can affect: aircraft, passengers, crew members, cabin baggage, hold baggage, cargo, mail, in-flight materials, catering, etc.

Flights are considered sensitive whenever particular conditions exist in:

- the overall international situation or in single geographical areas or specific countries;
- the public order and security situation, especially in the case of terrorist and/or criminal acts;
- the situation of the originating or transit airports security systems;
- the type of passengers transported (personalities, authorities, etc.).

The grading of high-risk flights refer to the level, nature and length of the risk and is determined by the Ministry of Internal Affairs – or by the related authorities with the contribution of the Information and Security Services, on the basis of the criminal or terrorist threat or according to the specific public order and security risk situation or national security.

14.2.4.1 Threat Notification

If Pegasus Airlines Aviation Security Department receives intelligence indicating that a specific aircraft may be subject to an act of unlawful interference from a State's services, then air traffic services and any airports at which the aircraft might land must be notified so that they may implement additional security measures, or a crisis management response.

14.2.4.2 Flights Under Increased Threat

Specific or additional security measures and searches under the point 8.2.1. will be applied to specific flights considered to be under an increased threat, including parking the aircraft in a designated area such as an isolated aircraft parking position and deploying security personnel around the aircraft during the time it is on the ground.

The frequency of security patrols on the apron and in the parking areas will be increased, and personnel working on the apron or in close proximity to the aircraft will be cautioned to be vigilant and immediately report any suspicious person or activity. Before the arrival of an aircraft under increased threat, a search will be made of the assigned parking position and its surroundings for any unauthorized persons or potential explosive devices that may be concealed within vehicles or ground service equipment.

If a risk entails a possible attack on a specific aircraft, the aircraft shall be escorted to and from the runway. In addition, areas immediately adjacent to runways and taxiways being used by the aircraft shall be inspected prior to movement of the aircraft to ensure that no potential attackers are in the area. Depending on the nature of the threat, an inspection of the approach and take-off paths outside the airport perimeter may also be required.

14.2.4.3 Suggested Security measures for Baseline, Intermediate and High-Threat Conditions

	Focus Area	Baseline	Intermediate	High
1	Landside and airside boundaries	Establish boundaries between landside and airside areas. Protect and inspect all passages through such boundaries at irregular intervals.	Apply baseline measures plus increased vigilance and patrols.	Apply intermediate measures.
2	Security restricted areas	Control access into security restricted areas at all times. Employ a pass system or other means for vehicles, staff and crew. Check all IDs and passes at access points. Inspect vehicles and supplies on a random basis.	Apply baseline measures plus search at least 20% of staff, items carried and vehicles before access is allowed.	Apply baseline measures plus search 100% of staff, items carried and vehicles before access is allowed.
3a	Passenger screening (where centralized)	Search all departing passengers by hand or screen them with metal detection equipment before access is allowed into the security restricted area.	Apply baseline measures plus search 10% of passengers by hand at the departure gate.	Search all departing passengers again at the departure gate by hand or screen them with metal detection equipment before boarding the aircraft. Search 20% of passengers by hand who have been screened by metal detection equipment.
3b	Passenger screening (at departure gate)	Same as for 3a.	Same as for 3a.	Same as for 3a.

	Focus Area	Baseline	Intermediate	High
4a	Cabin baggage screening (where centralized)	Search all cabin baggage of departing passengers either by hand or by X-ray equipment. 10% of cabin baggage screened by X-ray equipment to be searched by hand.	Apply baseline measures plus search 10% of cabin baggage by hand (or approved advanced technology) at the departure gate.	Search the cabin baggage of all departing passengers again at the departure gate either by hand or by X-ray equipment before being taken on board an aircraft. Search 20% of cabin baggage by hand (or approved advanced technology) which has been screened by X-ray equipment.
4b	Cabin baggage screening (at departure gate)	Same as 4a.	Same as 4a.	Same as 4a.
5	Separation of screened and unscreened passengers	Separate screened departing passengers from inbound passengers. Where physical separation cannot be achieved, application of compensatory measures in accordance with threat assessment by national authority.	Apply baseline measures.	Apply baseline and enhance monitoring of compensatory measures.
6	Aircraft security checks and searches	Check/search (in case of aircraft entering in service) originating aircraft prior to departure and aircraft in transit to ensure no weapons, explosives or other dangerous devices have been placed or left on board.	Apply baseline measures.	Conduct thorough search of aircraft supported by appropriate detection techniques at the discretion of the appropriate authority.
7	Access control to aircraft	Access to aircraft restricted to authorized staff having duties on board, and passengers. Aircraft doors shall be closed, and steps removed when unattended or air bridges withdrawn.	Apply baseline measures.	Access to aircraft to be strictly controlled with guards at each door in use. All staff seeking access to be searched by hand together with items carried.

	Focus Area	Baseline	Intermediate	High
8	Passenger risk assessment	No requirement.	No requirement.	All passengers subjected to a system of passenger risk assessment with selected passengers subject to enhanced screening
9	Reconciliation of hold baggage	Conduct positive hold baggage match with crew and passengers before loading by either manual or automated means. All unaccompanied baggage to be identified.	Apply baseline measures.	Apply baseline measures or positive passenger/bag identification.
10	Hold baggage screening	Screen 100% of originating and transfer hold baggage either by hand, conventional X-ray equipment or explosive detection system (EDS) equipment. With respect to transfer hold baggage, an exception can be made where a validation process and continuous implementation of procedures have been established for screening at the point of origin, and baggage is subsequently protected from unauthorized interference from the originating airport to the departing aircraft at the transfer airport.	Apply baseline measures, plus where conventional X-ray is used, 10% of bags also to be searched by hand or subjected to advanced X-ray technology.	Apply intermediate measures but use best available technology and procedures.
11	Unaccompanied hold baggage	Unaccompanied hold baggage except when its origins and ownership can be verified.	Screen all un-accompanied hold baggage either by hand or EDS equipment, or subject to flight simulation using compression chamber, or do not carry.	Apply intermediate measures.

	Focus Area	Baseline	Intermediate	High
12	Protection of hold baggage	Protect hold baggage from unauthorized interference from the point of its screening or acceptance, whichever is earlier, until departure of the aircraft. If the integrity of hold baggage is jeopardized, it shall be re-screened before being placed on board an aircraft.	Apply baseline measures.	Apply baseline measures plus keep hold baggage under constant supervision by designated security guards or transported in sealed, tamper-evident containers and verified.
13	Air cargo	All items to be subjected to security controls by aircraft operators and/or designated regulated agents and/or any appropriate entity before being placed on the aircraft.	Apply baseline measures with added random screening and increased checks. (Exception for regulated agents).	All air cargo to be subjected to full flight simulation3 and then protected until loaded. Aircraft carrying only cargo apply intermediate measures only.
14	Protection of air cargo	Protect air cargo from unauthorized interference from the point security controls are applied until departure of the aircraft.	Apply baseline measures.	Apply baseline measures plus keep air cargo under constant supervision by designated security guards or transported in sealed, tamper-evident containers and verified.
15	Mail	All items to be subjected to security controls by aircraft operator and/or designated regulated agents and/or any appropriate entity before being placed on the aircraft.	Apply baseline measures with added random screening and increased checks. (Exception for regulated agents).	All mail to be screened or subject to flight simulation in compression chamber, then protected until loaded. Aircraft carrying only cargo apply intermediate measures only.
16	Protection of mail	Protect mail from unauthorized interference from the point security controls are applied until departure of aircraft.	Apply baseline measures.	Apply baseline measures plus keep mail under constant supervision by designated security guards or transported in sealed, tamper-evident containers and verified.

	Focus Area	Baseline	Intermediate	High
17	Aircraft catering supplies and stores	All items to be subjected to appropriate security controls, i.e. to prevent introduction of dangerous items into catering supplies or stores taken on board an aircraft, and there after protected until loaded onto the aircraft.	Search a reasonable proportion of catering supplies and stores and either escort to the aircraft or transport in sealed, tamper-evident containers.	All catering supplies and stores to be prepared under direct aircraft operator security supervision or searched before loading and either escorted to the aircraft or sent under seal.
18	Designate security coordinator	No requirement.	No requirement.	Designate a dedicated security coordinator to ensure all measures are properly implemented.

End of Section

15 INCIDENT REPORTING

An aviation security incident occurs when there is an actual or threatened unlawful interference with aviation. This includes acts associated with an aircraft or airport that involve taking control, damaging, destroying or putting safety, or safe operation, at risk. Accurate reporting of incidents will help to improve operating procedures and to protect Pegasus Airlines and its contracted service suppliers' staff; and to identify areas for further research and/or improvements. It can be said that anyone who works in the aviation industry has a general responsibility to report aviation security incidents.

Pegasus Airlines has an operational reporting system that encourages and facilitates personnel to report security incidents and threats, identify security deficiencies, and raise security concerns. All Pegasus personnel have access to the Integrated Quality and Safety Management System (IQSMS), through which Security e-Reports can be submitted.

All security incident categories are predefined within the IQSMS system to ensure consistent classification and reporting. Submitted Security e-Reports are automatically assigned to the Aviation Security Department for review, analysis, and follow-up actions.

Reports processed through IQSMS and decided to be raised as Assessment should be closed within 30 days by the administrator. When an assessor manages the report, S/he reviews the related risk or creates a new one, modifies the risk if necessary and then gives reference to the risk if an assessment or investigation is raised from the report. If a report is logged for statistics, risk assessment is not necessary.

For further details, please refer to PG-EM-PR-009 - Occurence and Hazard Reporting Procedure, available in Comply365.

NOTE	Safety Department randomly checks some reports to make sure risk assessments are done appropriately. For more details, please refer to PG-GU-EM-EK-001 – SMS Manual, available in Comply365.

An enhanced availability of information ideally allows for information from:

- Industry actors assigned with aviation security responsibilities (e.g., airlines, airports)
- Other entities present at the airport and engaged in security measures (e.g., ground handlers, subcontractors, maintenance operators, retailers, tenants)
- Governmental stakeholders (e.g., law enforcement, aviation authorities, customs)
- Others, if required (e.g., hotels, travel agencies)

15.1 DESCRIPTION OF AIRLINE SECURITY INCIDENT REPORTING PROCEDURES

Pegasus Airlines and its contracted service supplier's personnel shall report all unlawful or suspicious acts which have or may have an impact on Pegasus Airlines. In order to record security related events and warnings or to be able to give information to Security Forces for legal investigations when necessary, Pegasus Airlines ensures that a report is prepared by those who have knowledge about the events and breaches.

CAUTION	Pegasus Airlines and its contracted service supplier's personnel shall inform the security department about the security incidents or threats via using printed forms or sending e-mail to the security@flypgs.com address and using emergency contact numbers under the point 3.4.2.

This Operational security reporting system provides such personnel with a means to report real or potential security threats or any other security concerns, so they may be brought to the attention of the head of security and other relevant managers. The operational security reporting system ensures also;

- To identify the root cause
- To conduct a security risk assessment

- To develop a corrective action
- And, when corrective action is implemented and monitored to ensure effectiveness, to prevent future incidents or occurrences.

Should a serious incident occur the responsibility for reporting and investigating the incident initially will generally become the task of the State of the Occurrence with assistance from the State of Registry (of the aircraft), State of the Operator and State of the Manufacture. All notifiable incidents are required to be reported to the TR-DGCA who have the power of authority vested in them by the Turkish Law which allows sole right of access by the Investigating Authorities, subject to certain exceptions.

Aviation Security Department will send all occurrences and reports to the TR-DGCA and related authorities within a maximum of 72 hours after officially receiving the information about major security related concerns. The Aviation Security Department will inform the authorities before the completing the investigation phase, for example via phone call or e-mail.

15.1.1 Confidentiality

Pegasus Airlines employees must not make any statement to persons outside the company regarding accidents or occurrences involving aircraft operated by the company. The publication of this information in respect of accidents is the responsibility of the CEO or his authorized deputy, and in respect of occurrences is the responsibility of the Flight Operations Post Holder. Any breach of this confidentiality can lead to suspension from duties or, in serious cases, instant dismissal.

Pegasus Airlines staff can also report via the IQSMS confidential e-reports for assessments. By sending this report the name of the sender cannot be seen.

15.1.2 Reportable Security Incidents

In the case of an incident, Company personnel or the contracted service provider shall inform Pegasus Airlines Aviation Security Department as soon as possible. Pegasus Airlines Aviation Security Department has the responsibility to report (initial notification) to TR-DGCA and any other relevant authorities, any occurrence that is defined in this Pegasus Airlines ACSP. This initial notification shall then be followed up by a report by the Head of Security. For isolated minor occurrences, where no imminent danger is present, employees shall notify Pegasus Airlines Security Department. The following are examples of company reportable security incidents and hierarchy of reporting procedures.

Reporting of incidents below does not replace or supersede the need to alert first responders and to initiate relevant emergency responses. Nor, in the case of any suspected criminal activity, does reporting under the NASP replace the need to inform the security authorities or police. ‘Immediate’ in this context means after the necessary operational and legal actions have been taken.

Breach of carriage of prohibited articles:

A full list of prohibited articles is available in point 4.10.3 for cabin baggage and 5.10.3 for hold baggage.

Table 15-1: ***Aviation Security Occurrences Risk Table***

Proposed security descriptors		Proposed explanation of the descriptor	Hierarchy of Reporting
1	Access control into the security-restricted area	Any actual or potential incident or vulnerability with authorized access to the security-restricted area, including not following the airport badge system rules and unauthorized access to air carrier materials or check-in system that could facilitate such an access	Immediately
2	Aircraft access control	Any actual or potential uncontrolled or unauthorized access to the aircraft cabin or hold, including failure to execute required aircraft safeguarding measures	Immediately

3	Aircraft security search/check	Any actual or potential situation where a credible threat (e.g., weapons, ammunition, explosives) has been found on the aircraft (including in the holds) during or after the security search/check has been completed	High Priority
4	Airport supplies protection	Any actual or potential situation where unauthorized access to airport supplies may have occurred	High Priority
5	Airport supplies security controls	Deficiencies or threats reported with regards to security procedures for airport supplies, including identification and screening (where applicable)	High Priority
6	Airside, controlled areas (security-restricted areas)	Any actual or potential threat situation against passengers, crew or airport infrastructure or staff occurring within access controlled and security-restricted areas, including catering, fuel, in-flight and maintenance facilities (if located airside)	Immediately
7	Any audit or inspection carried out by the authorities	Security Search inspections or audit performed by the authorities shall be reported.	Low Priority
8	Cabin baggage screening	Any actual or potential situation where screening rules where not followed or a credible threat (e.g., weapons, ammunition, explosives) has been detected during cabin baggage screening	Immediately
9	Cargo and mail acceptance	Any actual or potential violation of acceptance procedures, especially the verification of the secure supply chain of custody	High Priority
10	Cargo and mail protection	Any actual or potential situation where unauthorized access to cargo or mail may have occurred	High Priority
11	Cargo and mail screening	Any actual or potential situation where screening rules were not followed, or a credible threat has been detected during the cargo or mail screening	Immediately
12	Detection of Prohibited Items in cabin baggage inside Security restricted area.	Any actual or potential situation where screening rules where not followed and detection of an any prohibited items in cabin baggage or by passenger inside security restricted areas.	High Priority
13	Detection of Prohibited Items in hold baggage inside Security restricted area.	Any actual or potential situation where screening rules where not followed and detection of an any prohibited items in hold baggage inside security restricted areas.	High Priority
14	General environment (city, hotel, state)	Any actual or potential threat situation occurring in the city or within a state's territory, including-but not limited to- hotel and public transport infrastructure (e.g., terrorist and lone wolf attacks, insecurity, armed conflicts, availability of surface-to-air missiles and firearms)	High Priority

15	GREEN Warning Assessment - Positive Target Identification	A warning (Bomb Threat) which has been assessed as non-credible using PTI and which requires no immediate action to be taken	Low Priority
16	Hijack/Attempted Hijack	Aircraft whilst in flight or on the ground.	Immediately
17	Hold baggage protection	Any actual or potential situation where unauthorized access to hold baggage may have occurred	High Priority
18	Hold baggage reconciliation	Any actual or potential situation where unauthorized unaccompanied hold baggage may have been transported	High Priority
19	Hold baggage screening	Any actual or potential situation where screening rules where not followed or a credible threat (e.g., weapons, ammunition, explosives) has been detected during the hold baggage screening	Immediately
20	Improvised Explosive Device or components	Detonation of Improvised Explosive Device (IED), Person Borne IED, Vehicle Borne IED or discovery of same or suspected component parts of improvised explosive devices. Also, the discovery of a non-viable or fake device (which may be designed by hostile actors to test security measures).	Immediately
21	In-flight supplies protection	Any actual or potential situation where unauthorized access to in-flight supplies (including catering) may have occurred	High Priority
22	In-flight supplies security controls	Deficiencies and threats reported with regards to catering and other in-flight supplies security procedures, including identification and screening (where applicable)	Immediately
23	Insider threats	Suspicious activity executed by an individual, including a direct employee or a subcontractor	High Priority
24	Landside, airport (airport, parking, public areas, access roads)	Any actual or potential threat situation against passengers, crew or general public or infrastructure at the airport occurring in a public area at an airport terminal or in the area adjacent to the terminal, including parking lots, hotel and airport access roads	High Priority
25	Landside, crew (air carrier crew protection)	Any actual or potential threat situation occurring in the city or within a state's territory that may impact carrier crew and/or local aviation industry employees (e.g., hotels, restaurants, shuttles)	High Priority
26	Landside, perimeter (perimeter airside boundary)	Any actual or potential threat situation against passengers, crew or general public or infrastructure at the airport occurring around the airport perimeter, including ATC, catering, fuel, and in-flight supplies facilities (if not airside)	High Priority
27	Level 1 & 2 Disruptive Passenger Alerts	Where cabin crew communicates with a disruptive passenger of ICAO ‘Level 1-4’ terminology, see Procedures for Dealing with Unruly Passengers.	Low Priority

28	Level 3 & 4 Disruptive Passenger Alerts	Where cabin crew communicates with a disruptive passenger of ICAO 'Level 1-4' terminology, see Procedures for Dealing With Unruly Passengers. Incidents involving disruptive passengers graded Level 3 (life-threatening behaviour) or Level 4 (attempt to breach of flight crew compartment) shall additionally be reported.	High Priority
29	Mixing of passengers (screened/ unscreened)	Any actual or potential situation of contact between screened and unscreened passengers	Immediately
30	Occurrences impacting safety (unruly/intoxicated passenger or person, in-flight theft)	Any situation where a person fails to respect the rules of conduct at an airport or on board an aircraft, including not following the instructions of airport staff or crew members, or disturbing the good order and discipline at an airport or on board an aircraft	Medium Priority
31	Other criminal acts	For example, narcotics trafficking, human trafficking, theft	Medium Priority
32	Other security-related incidents likely to attract media attention	Any security incident or occurrence which has begun to receive, or is likely to receive, media attention and reporting. This will allow respective press offices to co-ordinate media messages about an incident.	Medium Priority
33	Passenger acceptance	Any actual or potential violation of accepted security procedures (e.g., watch-lists matching, submission of required passenger data) or any actual or suspected threat situation during the check-in process, including violation of DEPU, DEPA, INAD transportation procedures, fake documents presented by passengers.	Medium Priority
34	Passenger screening	Any actual or potential situation where screening rules were not followed or a credible threat (e.g., weapons, ammunition, explosives) has been detected during the passenger screening	Immediately
35	RED or AMBER Threat Assessment	Either a credible and specific threat requiring immediate protective measures (e.g. diversion or evacuation) or a threat of doubtful credibility but where it is prudent to consider taking additional protective measures e.g. augmented security checks.	Immediately
36	Sabotage or damage in flight	Any actual or suspected situation where a bomb, device, substance or weapon threat has been received when the affected aircraft was airborne/in flight, including Unmanned Aircraft Systems, CBRN-chemical, biological, radioactive, nuclear agents as well as cyber threats	Immediately

37	Sabotage or damage on the ground	Any actual or suspected situation where a bomb, device, substance or weapon threat has been received when the affected aircraft was still on the ground or towards airport/aviation facilities, including Unmanned Aircraft Systems, MANPADs, CBRN-chemical, biological, radioactive, nuclear agents as well as cyber threats	Immediately
38	Staff and crew screening	Any actual or potential situation where screening rules were not followed or a credible threat (e.g., weapons, ammunition, explosives) has been detected during the staff (including crew) screening	Immediately
39	Theft of ID, or other personal Documents	Theft of Uniforms, airport identification card(s) or liveried vehicles.	Medium Priority
40	Unmanned aerial vehicle	Threat posed by a drone being used to endanger the safety of aircraft, passengers or airport infrastructure	High Priority
41	Weapons and armed individual's transportation	Any actual or potential situation where requirements regarding the transport of weapons or armed individuals has not been followed	Immediately

Immediately	Immediate < 1 Hour	Medium Priority	< 48 Hours
High Priority	< 24 Hours	Low Priority	< 96 Hours

15.1.3 Incident Investigation

Pegasus Airlines' effective investigation process typically includes:

- Threats or acts of unlawful interference;
- Failure of implementation of security controls under the responsibility of the Operator.

Pegasus Airlines has a process for identifying and investigating irregularities, threats, acts of unlawful interference, failure of implementation of security controls, operational occurrences that might be precursors to an aircraft accident or incident. In the event of a major accident, Pegasus Airlines responds to, and possibly participates in, an investigation in accordance with provisions contained in ICAO Annex 13. Such capability requires that Pegasus Airlines maintains an ongoing interface with relevant investigative authorities to ensure preparedness in the event a major accident occurs.

The investigator in charge shall complete the incident report under the following suggested headings:

- **Factual information:** A brief narrative that shall include the following information:
  - Location;
  - Date;
  - Flight number;
  - Route;
  - Type of aircraft;
  - Number of passengers on board;
  - Name and seat number of perpetrator;
  - Number of crew members on board;
  - Name of Pilot-in-Command;
  - Name of senior cabin crew member;

- Names of crew members involved (if it is an in-flight incident).

- **Type of incident:** Indicate what type of incident occurred. If it was an unruly passenger; indicate the nature of the disturbance (i.e., passenger to passenger, passenger to crew, damage to equipment, etc.);
- **Specific cause:** If a cause is obvious, it shall be noted;
- **Injuries** involved
- **Outcome:** Describe the results of the incident. For example: verbal abuse, physical assault, damage to the airplane, destruction of the airplane, damage to terminal, etc.;
- **Measures taken:** Describe what measures were taken to try to limit the incident. For example: off-loaded passengers pre-flight, called police, diversion, emergency landing, etc.;
- Any **witness** accounts shall also be included.

Once the report is complete, it shall be analysed methodically. Only factual information found in the report which is relevant to the determination of conclusions and causes shall be taken into account.

Findings and causes established by the investigation shall be listed. Causes shall include not only the immediate ones, but also deeper procedural causes.

If it is appropriate, recommendations made to prevent further incidents of a similar nature and any corrective actions shall be listed.

TR-DGCA is the final authority for investigations of all aircraft incidents and accidents. TR-DGCA establishes a committee which consists of specialists in aviation for investigating of the causes of accidents and how they happen. The committee performs investigations to prevent the recurrence of incidents/accidents and loss of lives and properties. Internal incident/accident investigations are carried out under the authority of the Responsible Manager on behalf of the Chief Safety and Security Officer. All incidents will be investigated through follow-up of occurrences.

The steps for the corrections and corrective actions are as follows:

- Determination of the need for the correction and corrective actions
- Creation of the request for the corrections
- Assessment and recording of the request for corrections and corrective actions
- Waiting for correction
- Performance of the Root Cause Analysis
- Determination and acceptance of the corrective actions
- Monitoring of the corrective actions
- Assessment of the effectiveness of the corrective actions
- Conclusion of the corrective actions
- Periodical reporting of the correction actions
- Archiving of the relevant records and reporting of the same periodically

All corrections, corrective actions within the organization of the Company shall be managed only through the IQSMS software. The wording of any findings, corrections and corrective actions entered to the IQSMS software must be identical to the wording of the referred document.

For details: PG-KU-PR-002 Correction, Corrective Action Procedure, available in Comply365.

Root Cause Analysis (RCA) uses a specific set of steps, with associated tools, to help find the primary cause of the problem; so that you can:

- Determine what happened.
- Determine why it happened

A key issue is to work out what to do to reduce the likelihood that it will happen again. RCA assumes that systems and events are interrelated. An action in one area triggers an action in another, and another, and so on. By tracing back these actions you can discover where the problem started and how it grew into the symptom you are now facing. Root cause analysis is a tool used to determine the real cause or “root” cause as to why a failure occurred, thus minimizing the risk of a repeat failure. A common mistake in trying to accurately identify the root cause is to identify a casual factor to the failure or to wrongly attribute the failure to a human factor, such as lack of time etc.

All root cause analyses shall be managed only through the IQSMS software.

Please refer to: PG-KU-EK-001 - Quality Compliance Monitoring Manual, available in Comply365.

Submitted reports would typically be subject to an initial review and analysis to assess their validity. An entity shall consider categorizing the severity, likelihood and consequences to determine further steps and potential actions for reported issues. For example, reports on non-issues or issues of negligible or marginal severity, remote likelihood and/or low consequences would be recorded and stored for documentation purposes only, since they fall within an acceptable risk level. Further steps and escalations could be applicable if the analysed risk associated with the issue increases. Risk analysis is usually the responsibility of the Security department and shall be recorded, preferably in a standardized manner, for methodological consistency and trending to the ERA.

Security risk assessments shall also prescribe the authority level required to authorize continued operation at that risk level without mitigation. If the risk assessment reaches an established tolerability threshold, related to an entity's risk “appetite”, appropriate mitigations shall be proposed by the Head of related departments and agreed upon with other stakeholder involved, so the risk could be decreased to an acceptable level. When mitigations include undertaking certain actions, responsibilities and deadlines shall be clearly established and clearly assigned by all entities involved to ensure effective implementation.

As part of a follow-up assessment, an entity shall establish a timeframe for examination of implemented actions to reasonably ensure that the desired effects were achieved and any unintended consequences avoided or adequately identified.

An executive-level governance body (Administrator) shall be established where identified intolerable risks are presented together with actions taken. This is to provide for monitoring of mitigation implementation, enhancing of situational security awareness at the executive level as well as encouraging engagement and a proactive security attitude from business line managers (e.g., ground operations, flight operations, maintenance) with the aim of improving the overall security performance. Results of Risk Assessments are reviewed during Safety Action Group Meetings and Management Review meetings, depending on their importance.

AQD

15.1.4 Analysing of Security Reported Occurrences

All incidents and suspicious occurrences and reports about security related breaches are prepared by the Security Department, sent to related directorates, service provider companies and government agencies and the General Management is informed for corrective and preventive actions to be taken during the SRB Meetings. All records of the security incidents are kept by the Aviation Security Department under the Security Management Recording System, integrated into Airflow.

The recorded security cases during the month are analysed at the end of the month according to the proposed security descriptors in chapter 15.1.2 by the Aviation Security Department. Security reports statistics are reviewed regularly during the Safety and Security Review Board meetings.

15.1.5 IATA Incident Data Exchange Programme

The Incident Data Exchange (IDX) is IATA’s Safety and Security Incident Data Management Programme.

Safety and Security information is shown on Key Performance Indicators to benchmark our performance and establish Safety Performance Targets in accordance with ICAO requirements for Safety and Security Management Systems.

With the IDX Programme, critical trends are highlighted on a regional and global scale, allowing for comparative evaluation, operational challenges at specific airports are anticipated, critical incident trends are determined whilst setting targets for improvement. IATA's Global Aviation Data Management (GADM) department produces safety information that can be used by industry to improve safety performance and operational efficiency.

The Incident Data Exchange (IDX) Programme is IATA's Safety Incident Data Management and Analysis Programme and one of the sources of the Global Aviation Data Management (GADM). Incident Data Exchange (IDX) consists of a world-wide aggregated de-identified database of incident reports, including flight operations, cabin safety, ground safety, engineering and maintenance and security occurrences.

IDX offers a secure password protected platform and provides participants with a seamless experience to view their own safety and security data benchmarked against global aggregated data. The IDX infrastructure has been designed to accommodate operators of varying scale, and the site provides users with three core areas to self-manage activity associated with programme participation:

- User Management
- Data Consumption
- Data Contribution and Quality Oversight

The IDX portal is accessible for users from IDX registered Operators and other industry stakeholders, with valid membership and who have been granted GADM User roles.

For further details, please refer to *PG-EM-EK-001 - Safety Management Manual* and *PG-DO-KD-00016 IDX Program*, available in Comply365.

End of Section

16 SUPERVISION AND PERFORMANCE MONITORING

The objectives of Security Compliance Monitoring activities include, but are not limited to:

- Proactively identifying weaknesses in the management system, corporate documentation, processes, operational procedures, and employee training in support of the enterprise's continuous improvement programme.
- Monitoring compliance with all regulations and standards applicable to Pegasus Airlines. Drawing up and maintaining all documents pertaining to the Compliance Monitoring Programme.
- Providing assurance to senior management and the competent authorities that operations satisfy stated operational requirements.
- Identifying areas requiring improvement as part of the continuous improvement programme.
- Planning, conducting, and reporting audits, inspections, and oversight activities.
- Monitoring identified hazards and risks to operations.
- Determining and ensuring the effective implementation of corrective actions.
- Developing and promoting a working culture that prioritizes compliance, safety, security, and customer focus in day-to-day operations.
- Assessing the effectiveness of safety risk controls.
- Managing records related to the Compliance Monitoring Programme.

Pegasus Airlines has a process to monitor and ensure that relevant contractors and internal and external service providers are aware of and in compliance with the Pegasus Airlines ACSP, its associated SSPs and applicable regulatory requirements of the TR-DGCA.

For the monitoring process auditing is used for internal and external service providers as specified in this paragraph.

Contracts related to security are always copied to Pegasus Airlines Aviation Security Department by the related department to ensure a contract or agreement being executed with external service providers includes the following:

- Measurable performance specifications are monitored by the Aviation Security Department;
- Related requirements for designated performance indicators which are reported to the Aviation Security Department on a specified frequency (if needed or if applicable).

In some regulatory jurisdictions, there may be a regulatory control process that permits certain organizations to meet rigorous standards and become approved to conduct outsourced operational functions for an air operator or other organizations.

A regulatory control process or an industry acceptable certification may be accepted as a means for meeting the specification of an SLA as long as the following takes place:

- Such contract and/or agreement shall identify specific compliance, safety, security and Pegasus Standards The regulatory and/or industry certification can be verified and is approved by the relevant Nominated Person.
- Requirements shall be monitored by Compliance Monitoring Department to ensure the safety, security and Pegasus standards of operations are being fulfilled by the service provider.
- Pegasus Airlines is informed in case the certification expires and / or is withdrawn. In this case the service contractor shall be re-assessed to ensure the reasons for cancellation of the certification do not impact on the safety, quality and security or operational standards of the services delivered to Pegasus Airlines. Examples of regulatory or industry acceptable standards are DGCA-TR, EASA, FAA, UK CAA, IOSA, ISAGO, ISO, IFQP, DAQCP, IDQP, etc. (refer to: PG-YO-EK-001).

There exists a process for conducting periodic or event-driven security surveys that identifies needs and weaknesses of the Pegasus Airlines ACSP. To ensure the implementation of appropriate security measures in response to security threats directed against Pegasus Airlines, audit & performance monitoring applications are handled in special time intervals by the Aviation Security Leader (RP) and/or Delegated Auditors.

Table 16-1: Time Intervals for Audits

Service Provider	Station's Security Level[2]	Audit Intervals [1]
Ground Handling Company	Class 1	Every 2 years.
Ground Handling Company	Class 2	Yearly
Security Service Supplier	Class 1 / Class 2	Yearly
Catering Service Supplier	Class 1	Every 2 years.

[1] Time intervals of audits can be changed according to the Aviation Security Leader (RP) decisions, security needs, risk assessments or any other external/internal requirements.

[2] Refer to "Chapter 14.2" for the security standards.

Details of risk-based audit processes are described in *PG-KU-PR-007 - Compliance Monitoring System Risk Based Oversight Procedure*, available in Comply365. The audits are performed in accordance with published audit checklists (depending on the type of audit) available in Comply365 and IQSMS systems.

16.1 DESCRIPTION OF AIRLINE ARRANGEMENTS FOR MONITORING IMPLEMENTATION OF SECURITY MEASURES AND QUALITY CONTROL

16.1.1 Quality Assurance Audits

In accordance with the National Civil Aviation Security Programme, ECAC Doc. 30, ICAO Annex 17, ICAO Doc 9811 (Manual of the implementation of the Security provisions of Annex 6) and IATA Security Manual, a quality implementation programme has been planned.

Quality Management typically has two major divisions of activities: Quality Assurance (QA) and Quality Control (QC). Quality Assurance is an internal auditing function that is conducted by persons or organizations that must be functionally independent of the technical process being evaluated. This programme will also ensure a means for monitoring the security and quality of services provided by external suppliers or subcontractors.

Quality Assurance audits are performed on behalf of the organization's RESPONSIBLE executive to ensure that the functional areas meet regulatory requirements and established organizational standards. Audit results are presented to the senior management team for periodic review and actions.

In contrast, Quality Control is typically performed by the operating department that “owns” the technical process. These employees are the technical experts who possess the knowledge and authority to redesign internal processes and functions to improve productivity, efficiency, security and quality.

Security Audits are conducted in line with *PG-KU-EK-001 - Compliance Monitoring Manual*, available in Comply365.

The aim of the Quality Assurance Programme is to ensure that;

- Pegasus Airlines personnel, handling agents and contractors are properly implementing the Security Programme;
- the Security Programme is achieving the set objectives.

Security issues are risks to the current and future operation of Pegasus Airlines that need to be managed. Each significant issue or security incident and Level 1 Findings are reported on a regular basis to the Safety Action Group Meetings. Significant issues will be evaluated in the Safety Action Group Meetings for actions.

For example, conducting investigations, risk assessments or reviews to the Safety Review Board/ Management Review Meeting etc. for further evaluation.

Security investigations include the following and, if seen as necessary, the outcomes may be consolidated with root cause analysis.

(1) Threats or acts of unlawful interference

(2) Failure of implementation of security controls under the responsibility of the operator

(3) Security incidents, security occurrences or security threats.

The summaries include strengths and weaknesses and recommendations from the auditors. Also included would be an overall management evaluation of the audit as well as an assessment of the performance of the audited area. To ensure balance, both positive and negative aspects are included.

Audit summaries also include comments regarding the likelihood of changes to security measures based on the audit results and include an estimated time period for the implementation of such changes.

Auditor recommendations contained in a report provide the basis for possible changes within the system. However, for various reasons, the adoption or implementation of recommendations made by auditors may not always be feasible. Therefore, the determination of a need for corrective or preventive action, and the actual implementation of such action, is always a coordinated decision between the Aviation Security Leader (RP) and those operational managers directly responsible for the safety and security of operations.

Correction and corrective action needs that arise as a result of nonconformities and irregularities detected during the audits carried out are managed according to P*G-KU-PR-002 - Correction and Corrective Action Procedure*, available in Comply365.

Pegasus Airlines ensure significant issues arising from quality assurance audits of operational security functions are subjected to a regular review by the Aviation Security Department.

Please refer to: *PG-KU-EK-001 - Compliance Monitoring Manual ,* available in Comply365.

16.1.2 Security Auditors' Requirement

The security auditor qualification and training requirements are described in Pegasus Airlines Security Training Programme, please refer to PG-GU-EK-002 - *Compliance Monitoring Program*, available in Comply365.

16.1.3 Quality Control

The Quality Control (QC) mechanisms of Pegasus Airlines includes:

- Formal performance monitoring audits (both internal and external). These shall be performed at least annually and more frequently when performance issues are highlighted. The audit shall look at compliance with legislation, regulations, operating rules and conformance with the air carrier's own security programme.
- Regular checks. These are usually performed monthly, but are adjustable to the size of the structure and the type of operation, with the objective of collecting statistical data.
- Recurrent testing of processes and staff performance.

One of the key roles of a Security Management System (SeMS) is to facilitate CMM and ensure that the CMM measures are adequate. The key elements of a CMM Programme include:

- Air Carrier Security Programme
- Senior Management's statement of commitment to security
- A procedure for corrective action to ensure identified deficiencies are promptly resolved
- A procedure for preventive action to ensure that potential causes of deficiencies or failures identified are remedied

- A procedure to ensure that the CMM system and the internal quality assurance procedures are subjected to continual, regular and structured review
- An internal audit programmes
- A procedure to ensure that quality indicators, including defect/incident reports are monitored to identify existing or potential problems with the system
- A procedure to capture staff feedback, which is given due consideration to maintain continuous motivation of field staff
- A record system that clearly documents what has taken place and allows for statistical analysis to monitor the continued suitability and effectiveness of security operations; these records shall be used to identify trends to allow the organization to:
- Ensure proactivity
- Define future security policy
- A document control procedure to manage, develop, document, amend and distribute the organization's quality and operational security procedures

16.1.4 Security Audits

Pegasus Airlines or its suppliers, as necessary, will follow domestic and international audits to bring into place national and international security procedures. Security audits are performed involving the internal and external service providers that engage with airports.

Any findings from the audits, whether preventative or corrective will be recorded and tracked by Aviation Security Department or related auditor.

The audits are performed in accordance with published audit checklists (depending on the type of audit) available in Comply365 and the IQSMS system.

Please refer to *PG-KU-EK-001 Compliance Monitoring Manual* and *PG-KU-EK-002 Compliance Monitoring Program*, available in Comply365.

16.1.5 Security Surveys

Airport audits, inspections or surveys cannot be performed by Pegasus Airlines without prior consent from the airport and their respective national authority or regulator. Regulators are the ones that have the ability and responsibility to conduct audits, inspections or tests at airports and airlines which have operations within their State.

It is essential that all stakeholders have the possibility of assessing their respective activities, including airlines at each and every airport of operations.

A Security Survey is an evaluation of security needs, including the identification of vulnerabilities which could be exploited to carry out an act of unlawful interference and the recommendation of corrective actions specifically as regards Pegasus Airlines operations.

Security surveys are conducted on a risk-need basis according to the assessment of the Aviation Security Department.

The surveys are performed in accordance with the published survey checklists available in the Comply365 system.

Surveys of security measures are necessary to ensure the adequacy and continued effectiveness of security programme and further ensure that appropriate measures and procedures remain in compliance with the appropriate legislation. Surveys shall conclude with the production of a comprehensive written confidential report outlining in detail the findings and recommendations of the survey. The depth and scope of the survey shall encompass all features that affect aviation security, to include (but not be limited to):

- the airport security enforcement measures regarding Pegasus Airlines operations can be discussed with the airport authorities and with State regulators to ensure their compliance with National and International rules;

- the training programme (if shared) is examined to ensure national policies and requirements are properly addressed;
- passenger handling procedures are examined to determine areas that may be open to abuse and exploitation;
- security measures applied to hold baggage are evaluated, including passenger/baggage reconciliation and storage measures for mishandled baggage;
- the effectiveness of the pre-board screening of passengers and their hand baggage, and the security integrity of sterile areas can be reviewed;
- the security measures in place, both physical and procedural, to protect cargo and air freight operations, are evaluated;
- security measures in place at in-flight catering centres to protect the integrity of catering supplies to aircraft are examined;
- airport emergency procedures are addressed, including the hijacking of aircraft, destruction of aircraft, sabotage of airport facilities, acts of terrorism at airports, bomb threats against aircraft and bomb threats against airport facilities.
- the effectiveness of the security lighting of critical areas is determined, e.g. if your aircraft is parked overnight;
- the effectiveness of previous security surveys and inspections carried out are evaluated, including how their results and findings have been used and implemented;
- the conduct of security exercises implemented on a regular basis to test security measures and procedures are evaluated;
- the architecture or building layouts and the organization of work seeking to improve the airport security system are studied.

Regular risk-based assessment of security programmes and audit processes are undertaken. The network auditing department performs regular station visits and publishes short e-mail reports.

Details of risk-based audit process are described in PG-KU-PR-007 - Compliance Monitoring System Risk Based Oversight Procedure (available in Comply365).

16.1.6 Security Tests

In accordance with the National Civil Aviation Security Quality Control Programme (MSHGKKP) Pegasus Airlines are not authorized to conduct security tests.

16.1.7 Security Exercises

Chief Safety & Emergency Response Management Officeof Pegasus Airlines arranges various emergency response scenarios and exercises. Pegasus Airlines conducts either a desktop exercise or an on-site exercise for aircraft occurrences once a year.

When the exercise is executed, a detailed debriefing and critique will take place and will be announced by the Emergency Response Manager. Critiques have also been undertaken after actual events with emergency manuals and plans reviewed, and changes made by the Safety Management Department, shall any change be required. Actual events can, of course, be considered instead of exercises.

There are two major requirements in exercising a plan:

- Testing the responses of the crisis management teams
- Testing the procedural elements of the plan

Exercises shall be undertaken against various crisis scenarios. A team of experienced persons shall be involved in setting the exercise, observing the events as they evolve and scrutinizing the exercise's outcomes.

- The control mechanisms of an exercise can involve:
- ‘Table top’ exercises with written scenarios
- ‘Hypothetical’ exercises advancing theoretical critical events
- ‘Restricted’ exercises involving theoretical critical events without the use of manpower and/or equipment
- ‘Real-time’ exercises involving people playing out various roles and the use of aircraft and other services under actual operational conditions.

Briefs must be developed that address the following:

- Scenarios
- Sequence of events
- Control requirements
- Safety issues
- Manpower and resource requirements
- Location aspects
- Monitoring processes while the exercise is in progress
- Debrief processes when the exercise is completed

All exercises are to be controlled by specific written instructions at the beginning and during the exercise.

The instructions shall cover the following:

- Exercise call-sign used to avoid confusion with a real threat
- Dates, duration and location of the exercise
- General outline
- Organizations participating
- Strict communications rules
- Media involvement

Important points to keep in mind when conducting an exercise include:

- Follow the scenario
- Keep to the sequence and timing of events
- Maintain control
- Keep response elements realistic and within their briefs
- Identifying specific events to be initiated by the exercise control staff only

At the end of the exercise, it is important to have an evaluation and debrief. This is the first step in ensuring that the exercise can contribute to improving the emergency response plan. The evaluation shall:

- Determine the achievements or failures to meet objectives
- Determine the effectiveness of plans, procedures, equipment, personnel and facilities being subjected to the exercise
- Compare results with previous exercises or similar incidents
- Identify deficiencies
- Amend policies and procedures, if necessary
- Amend training programmes accordingly

16.1.7.1 Duties And Responsibilities of the Aviation Security Leader (RP) During Exercises

Department Managers are responsible for informing and training their personnel on the contents of this manual for forming an Emergency Team.

Staff who are in position to carry out duties and responsibilities as prescribed in this manual are responsible to the General Manager.

PG-EM-FR-013 – Crisis Management Centre Duties Form (available in Comply365) describes each department's duties. In case of an emergency, the Aviation Security Leader (RP)'s duties are as follows:

- To contact Local Security at the airport,
- To liaise with the Police and/or the Security Company on any security issues,
- To liaise with the appropriate agencies in order to ascertain the level of threat to Pegasus Airlines interests, including any recent threats made to the company.
- To ensure the security of the passengers, crew and aircraft by contacting Local and on-site Security Units.
- To keep in close coordination with Security Units and to up-date the Crisis Management Centre on all developments
- To inform shift members about any accident/Incident and operate own shift
- To keep a daily follow-up form with Emergency Logbook Form in the Crisis Management Centre
- To implement and support orders given by the Crisis Director.

For more details, please refer to ERP Manual PG-EM-EK-002, available in Comply365.

16.1.7.2 Evaluation of Effectiveness of the ERP

Following the debriefing and feedbacks, a draft report is prepared by the Chief Safety and Security Office.

The process is continued with internal and external entities to obtain opinions about the preliminary report and vital information in one month via e-mail or meeting whenever the ERP is activated, whether for an actual event or for an exercise.

After consolidation of the whole data, opinions and recommendations, a final report including findings and suggestions will be published to the related departments via e-mail by the Chief Safety and Security Office within three months at the latest. In the final report, action plans will be defined with relevant departments and action plan monitoring will be performed by the the Chief Safety and Security Office.

Pegasus Airlines Air Carrier Security Programme and other relevant documents will be reviewed and if necessary, revisions will be made by the Aviation Security Department.

For more details, please refer to PG-EM-EK-001 – Emergency Response Manual, available in Comply365.

16.1.8 Station Security Audits

Prior to conducting audits, auditors prepare by researching what they would expect to find on arrival, including but not limited to:

- The nature and level of the local security threat
- Security incidents that may have occurred
- Staff training records
- Previous audit reports
- The type and size of operations

To effectively conduct the audit, cooperation with the regulator and the airport operator will routinely be required.

Therefore, the auditor shall contact the station staff and request their assistance in arranging an opening meeting and a temporary security access control pass.

The audit comprises a mix of reviewing station procedures, observing operational performance and discussing security matters with the staff to assess their awareness of their responsibilities and any challenges they may face discharging them. Ideally, a member of the station staff shall accompany the auditor and contribute to the assessment of findings and the development of remedial actions plans, if they are necessary.

The auditor develops a supportive relationship with the staff that will continue after the audit has been completed; S/he shall continue to provide support to the station, as necessary.

The authorities (airport or states, if applicable) are provided with constructive, specific feedback at the end of the audit process and are invited to participate in any remedial actions that might be recommended.

The auditor verifies that recommendations have been completed as agreed and that security has improved to the extent intended. Thereafter, the auditor shall confirm to relevant personnel that the audit is considered complete. The audit report may contain sensitive security information that is specific to an air carrier operation and location. As such, it is treated with due care and distributed and stored in a secure fashion. Consideration shall be given to providing copies only to those who have a legitimate role in delivering and enhancing aviation security at the station in question.

Quality Assurance/Control is embedded in station security to the same extent as any other operational aviation activity. It is also one of the critical elements in SeMS development.

Station security quality control is recognized as a method for providing internal confidence in the organization by reassuring that:

- Station security standards are implemented correctly
- The station can manage aviation security in an effective manner
- There is an awareness and understanding of aviation security roles and responsibilities throughout the station and by all operational managers
- Deficiencies are detected and rectified accordingly, with the goal of improving the station security system through root-cause identification
- Rectification actions are followed-up to verify the improvement and to ensure the most efficient utilization of resources

Station security quality control and assurance is a planned activity usually based on requirements contained in national legislation combined with internal risk assessments. All activities must be documented and recorded.

To provide consistency in station security quality control, a systematic approach to planning, preparation, conducting and reporting is developed (CMM, QAP).

Persons conducting station security audits, inspections, tests and surveys are qualified and trained in the scope of the operational activity to be assessed as well as in quality control methodology to ensure objectivity and consistency in all activities. Simultaneously, an appropriate level of functional independence between the person conducting the assessment and the area being assessed needs to be provided.

The audits are performed in accordance with published audit checklists (depending on the type of audit) available in the Comply365 and IQSMS systems.

A necessary element for regular risk-based continued effectiveness of security programs risk-based oversight audit process has been created. Network auditing department is performing often station visits and publishing the short e-mail reports. This report is also including the security issues. According to the e-mail reports a premiere audit will be planned by Aviation Security Department.

Details of risk-based audit process are described in *PG-KU-PR-007 - Compliance Monitoring System Risk Based Oversight Procedure,* available in Comply365.

16.1.9 Security Inspection

A security inspection is an examination of the implementation of relevant national civil aviation security programme requirements by an airline, airport or other entity involved in security. This will normally be

conducted over a short period (e.g., a few hours or a day). Only relevant authorities (DGCA) performg the security inspections on a random basis.

16.1.10 New Destination Risk Management Study

New Destination Risk Management Studies will be undertaken according to *PG-EM-EK-001 - Safety Management Manual* and *PG-EM-PR-001 - Management of Change Procedure*, available in Comply365. The procedure has specific conditions for New Destination Risk Management Studies and their processes are as follows:

(1) **Starting New Destination Risk Management Study**: A Safety and Risk Management Specialist starts the process after being informed by Commercial Department about a new destination/route request. If an airport visit is not possible or required, a Remote New Destination Checklist is requested by the Safety and Risk Management Specialist. If the airports involved have already scheduled flights operated by the Company, a review of the current study will be conducted and published as a revision.

(2) **Choosing Subject Matter Experts**: A Safety and Risk Management Specialist chooses the Subject Matter Experts (SMEs) from the departments below to identify and analyse the risks completing *PG-EM-FR-026 - Remote New Destination Checklist,* available in Comply365, before/without visiting the airport;

(a) IOCC

(b) Flight Operations

(c) Ground Operations

(d) Technic

(e) Security

(f) Cargo (If there will be cargo operation)

(g) Cabin Operations

(h) Crew Planning

(i) Safety

(j) Commercial

(k) Legal

SMEs choose other relevant associates from their departments if unavailable elsewhere. Observers from various departments may also be chosen for information purposes only.

(1) **Data Entry** : SMEs enter the data on the checklist with highlighted summary and provide it to the Safety and Risk Management Specialist for the final safety review

(2) **Safety Review**: The Safety and Risk Management Specialist, SMS Manager and/or Flight Safety Manager review the finalized document and determine the risks.

(3) **Risk Assessment**: RA methodology is applied to each determined risk.

(4) **Preliminary report** including checklist and identified risk(s) is published by the Safety and Risk Management Specialist to relevant units and the Commercial Department.

(5) **Airport Visit**: The Safety and Risk Management Specialist asks SMEs if an airport visit is necessary via e-mail and the SMEs decide by communicating via e-mail or other means. If necessary, an airport on-site visit is planned to identify blind spot risks. Required representatives from departments attend the airport onsite visit. The following are taken into account in the decision-making process for the airport visit:

(a) Identifying whether an operation has been carried out before,

(b) Receiving feedback from other operators,

(c) Checking whether airport facilities meet high standards,

(d) Reviewing of security standards,

(e) Ensuring the external service providers availability

(6) **After visiting the airport:** SMEs fill in *PG-EM-FR-001 - New Destination Checklist,* available in Comply365 if and when an airport visit is accomplished and send it to the Safety and Risk Management Specialist. The related documents on the airport and the used checklist are combined with the preliminary report. After the risk management study is over, if there is an uncompleted operational necessity listed in the checklist and if it does not cause a risk, it will be monitored by the related SME to be informed to the Safety and Risk Management Specialist once it is completed. If the need to revise the checklist arises, SMEs notify the Safety and Risk Management Specialist. Risks related to identified hazards and threats are specified in the explanation section of the checklist.

(7) **Risk Mitigation:** Refer to *PG-EM-EK-001 - Safety Management Manual Chapter 4.9*, available in Comply365.

(8) **Announcement to Operational Personnel:** SMEs announce the related risks of the airport to the operational personnel of their departments.

(9) **First Flight:** Crew qualification rostering for new destinations flights will be minimum C3 for Captain and P2 for F/O for the first three consecutive flights and no LIFUS / check flight, unless a higher crew composition is required as determined according to *PG-EM-FR-001 - New Destination Checklist.*

For further details about risk analysis process of charter and scheduled flights, please refer to *PG-EM-PR-011 - New Destination Procedure*, available in Comply365.

16.1.11 Compliance Monitoring of Safety and Security Outcomes

Compliance monitoring of reported safety and security outcomes are aiming to provide confidence to Pegasus Airlines corporate goals under safety and security audits.

Data tracking, analysis and investigations, audits and evaluations support the essential function of the Safety and Security Management Systems by ensuring that safety and security objectives have been met.

The SMS and security audits have been integrated and are carried out by the Compliance Monitoring Program.

- Audit initiation, including scope and objectives.
- Planning and preparation, including audit plan and checklist development.
- Observation and gathering of evidence to assess documentation and implementation.
- Analysis, findings, actions.
- Reporting and audit summary.
- Follow-up and close out.

The final outcome of this step is the identification of safety and security issues emerging from related audits. Safety and security issues are risks in the current and future operation of Pegasus Airlines, that need to be managed.

All level 1 findings and all findings whose risks are determined in the red area in the matrix are represented in SAG meetings by Compliance Monitoring representative and are added in Monthly Actvity Reports. In addition, finding failure item trends are followed up and are represented in SAG each quarter.

Please refer to *PG-KU-EK-001 - Compliance Monitoring Manual*, available in Comply365.

End of Section

17 LOCAL AIRPORT PROCEDURES

Please refer to the Airport Security Plans & Instructions *PG-GU-PR-Doc.No* (reference number changing according to the station) and/or Station Local Notification Lists PG-MK-BK-Doc.No (reference number changing according to the station) available in Comply365. Or contact security@flypgs.com.

17.1 LIST OF CONTRACTED SERVICE PROVIDERS

If any local procedures exist at that station, it will be the responsibility of the person mentioned below to inform Pegasus Airlines prior to operations.

Local Notification Lists include all stations' contact information; the lists are available in Comply365 and Pegasus Online Library and EFB under the reference *PG-MK-BK-Doc.No* (reference number changing according to the station). Or contact security@flypgs.com.

17.2 ADDITIONAL SECURITY SERVICE PROVIDER SELECTION PROCESS

Pegasus Airlines also has additional security services on its flights, when necessary, The additional security service provider selection process is performed according to security-relevant criteria. This service shall be received from a private security service provider company which is authorized by the TR-DGCA or relevant authority.

In Türkiye, a Private Security Service Company shall have a license from the Ministry of Interior according to Law No. 5188 concerning Private Security Services and is compatible with Turkish NCASP (National Civil Aviation Security Program & National Security Training Program or Pegasus Airlines Security Training Program).

Most of the additional security implementation requests are published by the relevant authorities to the Aviation Security Department directly or determined according to the risk assessment results performed by Pegasus Airlines Aviation Security Department. The risk results are periodically reviewed according to the risk assessment process established by the Chief Safety and Security Office.

If there is a need for additional security service provider implementation, the security service providers companies in relevant location will be assessed by Aviation Security Department in coordination with Support Procurement Leadership Management according to national, international and Pegasus Airlines requirements.

For further details, please refer to *PG-YO-EK-001 Corporate Manual* and *PG-KU-EK-001 - Compliance Monitoring Manual*, available in Comply365.

After the assessment process the Support Procurement Leadership signs the agreement with the appropriate company. Aviation Security Department must perform the audit process mentioned under the Chapter 16.

End of Section

18 STAFF SECURITY

The following Chapter aims to provide guidance to all staff in order to make their stay at an outstation as secure as possible. Some of the guidance might seem overly cautious for low-risk stations. Pegasus Airlines strongly emphasize that all guidance shall be strictly followed at all stations, a feeling of complacency might set in the mind of those who travel frequently. In order to avoid staff overlooking precautionary measures when staying at a higher risk location, they should be reminded by the station manager of the higher risk level and briefed to adhere to the air carrier's recommended guidelines closely (including any items specific to that station).

18.1 VIGILANCE, INSTINCTS AND COMMON SENSE

Staff should not get involved in any sort of activity that they would usually refrain from doing at their home base. By following this basic principle, staff can avoid most of the problems that can present themselves while away from home. In combination with adherence to recommended security measures and training, vigilance, common sense and some reliance on instincts can help steer staff away from potentially dangerous situations.

If going somewhere feels wrong, then it is probably best avoided. Firstly, a lack of confidence could affect the ability of staff to react quickly and instinctively. Secondly, staff that do not feel at ease with something will seem more nervous and might appear as an easier target for people with malicious intentions. The combination of training, adherence to security guidance and vigilance, common sense and instincts should help avoid most dangerous situations. And it should also help staff respond effectively to those situations if they do arise.

18.2 STATION BRIEFING INFORMATION

The Security Department should provide specific advice to their air crews and ground staff when a threat becomes apparent at a particular location. Ad hoc notices regarding new or specific threats should be communicated to staff in a timely fashion and using available communication channels (e.g. staff bulletins etc.).

Such advice shall include any special security measures that may be required in addition to the standard operating procedures that are contained in the air carrier's security programme and instructions.

The station brief should include customs and local practices. A ‘Do's and Don'ts’ section is a good approach, especially at stations where there is an increased threat level or where the culture is very different from the home base. Where action is required by air crews, the brief could also describe the security measures relating to the aircraft, airport and ground transport operations that are specific to the station (e.g. aircraft overnight security measures). It is then important to ensure that the briefing sheets are handled, and disposed of, in a way that protects their contents.

Staff should pay particular attention to local circumstances and requirements. They might need to register at an embassy or consulate, obtain visas or abide by any curfews. Staff should avoid civil unrest by paying attention to any notices that call for demonstrations or protest, monitoring local media, remaining in close contact with local air carrier and hotel management and actively avoiding any affected neighbourhoods/ regions.

It is good practice for visiting staff to be provided with useful telephone numbers and contact information for the station in which they are staying. Such information can be included on the station briefing sheet. In an emergency, local air carrier or hotel staff should be able to lend practical support to the individual (e.g. finding a local doctor).

18.3 STATION MANAGER

Pegasus Airlines contracted ground handling service providers Station Manager plays an important role as the ‘eyes and ears’ for the Security Department. The Station Manager should relay information relating to changes in the local security environment to the IOCC & Security Department via the 24H contact numbers or e-mail. IOCC must be informed first as regards all communication. IOCC will then inform the Aviation

Security Leader (RP). Critically, the Station Manager should have links to the relevant local security authorities and agencies and will act as the interface between them and the air carrier's head office when needs dictate.

At sensitive locations where crews or other staff layover, the Station Manager also has the important role of briefing the IOCC, Aviation Security Department and the crew regarding safety and security considerations for their stay.

The Station Manager, with expert support from the Security Department, should evaluate and monitor the local conditions for the security of the crew and other visiting staff and should:

(a) check that crew transport to and from the hotel is secure. This includes noting factors, which may affect the security en-route;

(b) ensure secure handling of crew baggage to prevent contamination and uplift of explosives or any unauthorized interference, which may endanger safety of the aircraft;

(c) ensure, if necessary, that the hotel has facilities for safe custody of official monies. In addition, the hotel shall be located in a safe neighbourhood.

Moreover, should there be events that could jeopardize the security of crew or other staff during a layover; the Station Manager should relay this information as soon as possible to the air carrier's IOCC & Security Department. A decision should then be made as to whether and how they shall increase security measures for layovers or if it is more advisable to relocate the layover to another station in the area. In extreme cases, it might be appropriate to suspend the layover altogether.

While the Station Manager should provide all the necessary local information and support to ensure the security of staff, the ultimate responsibility for keeping safe and secure remains with the individuals themselves and depends on how vigilant and responsible they are.

18.4 CREW GROUND TRANSPORTATION

As required, ground transportation should be arranged by the air carrier to move crew and their baggage between the airport and the hotel. The Station Manager, supported by the Administrative Affairs Management, will help identify suitable transport and ensure it is both secure and safe. Where dedicated ground transportation is not arranged by the air carrier, hotel transportation or reliable public transportation should be the primary option for crew members to get to their hotel. If available, the hotel's own transportation shuttle should be used as the means of transport and the pick-up for the return trip to the airport should be confirmed.

At high-risk locations, additional measures may be necessary to protect crew transportation, and these should be determined by the Security Department on a case-by-case basis. They might include using a local escort with appropriate communications (mobile telephone or radio), varying routes taken and so on. Consideration should also be given to ensuring that crew are collected and dropped-off at the airport in a location and manner that reduces their exposure to higher-risk public spaces.

18.4.1 Taxis

Whenever a taxi is used, it is recommended that crew and other staff should:

- always use approved taxis;
- be aware of the identifications (logos, car colour, etc.) of registered taxis and where they can be found;
- make sure the meter is turned on when departing unless a price has been agreed on;
- avoid riding for a fixed price if alone, unless it is clearly stated in the taxi that there is a fixed price between the points of departure and arrival; .
- beware of taxi drivers offering their service within the airport terminal, quite often these are not registered taxis;
- avoid sharing a taxi with someone they do not know;

- at the destination, wait until luggage has been removed from the trunk before paying the fare;
- have some money ready for the fare separate from their wallet;
- exercise caution in what they discuss with the taxi driver;
- have the name and address of their hotel on a printed card, possibly in the local language, to ensure the taxi driver knows the destination.

18.4.2 Public Transportation

Whenever public transportation is used, it is recommended that crew and other staff should:

- check with hotel staff if any public transport stations or stops could present a hazard. For example, in many cities, stops in the business district are crowded during the day but can be deserted at night and might not be safe;
- try to have a sense of which bus or train to take;
- write directions on a piece of paper rather than carry a tourist map;
- ask a public transport employee or a passenger who looks trustworthy for directions if lost;
- not panic if they are lost;
- stay in a well-lit area when waiting for a bus or train at night;
- stay towards the middle of the platform, where most people wait for the train;
- avoid boarding train carriages where there are no or very few passengers;
- try sitting or standing as close to the bus driver as is permitted;
- exit the bus or train or leave the waiting area the moment they feel threatened.

18.5 HOTEL SECURITY

Pegasus Airlines provides to their crew accommodation in a safe, secure and reputable hotel after due assessment of the establishment and its location. Where appropriate, other staff on duty travel should consider making use of the crew hotel to benefit from the assessment and from any other facilities made available to employees.

In assessing the suitability of a crew hotel, the Security Department should formulate a set of standards that can be used in an objective manner and that ensures there is sufficient security at the hotel.

The areas to review would include the location of the hotel, perimeter protection, access controls, room security facilities, surveillance procedures and equipment, the standard of the hotel security team and the security management approach demonstrated by hotel senior management. A checklist for the review of the hotel should be prepared and made available for hotel inspections and can include the following items:

- the hotel is located in a safe neighbourhood;
- the hotel perimeter is subject to security controls;
- the hotel building is subject to access and other security controls;
- there is adequate surveillance equipment within the hotel;
- the hotel engages a security team who are on duty 24/7; .
- the hotel has a proactive approach to security management, including good links with local police and security agencies;
- the hotel is able to provide effective and timely local security advice to guests;
- the hotel has a good access control system that records all entries into guest rooms;
- hotel rooms are physically secure from unauthorized external access (e.g. balconies);

- hotel rooms have double locks;
- hotel room doors have a safety door chain/bar and a spyhole or entry camera;
- hotel rooms are equipped with a mini-safe;
- the hotel can provide a secure holding facility for cash and other valuables;
- the hotel operates, or has access to, secure ground transportation.

This is not a finite list of requirements and may be built upon to meet the demands of the individual airline based on their security risk assessment for the location in question. Where necessary, expert advice on the physical, technical or procedural security measures required to manage the risk in higher threat environments should be sought. Amongst other things, this could include enhancements to perimeter security, access controls and ground transportation arrangements.

18.5.1 Check-in

Pegasus Airlines ensures that the management of the hotel recognizes the importance of providing secure accommodation for air crew and other staff and, as a minimum, the hotel should be able to provide staff with:

- rooms that do not face a street or parking lot;
- rooms on the lowest available floor above the ground floor;
- rooms in the vicinity of each other and on the same floor;
- rooms not directly next to, but convenient for, emergency exits or elevators;
- a secure holding facility (e.g. hotel safe) to store all valuable documents (e.g. passports, crew identification, etc.) and large sums of money. Documents that are left at the front desk for safe storage should be put in a sealed envelope and signed in order to protect against tampering.

When staff check-in, they should be aware of the security requirements of the air carrier and should ensure that the hotel provides them with facilities that meet those requirements.

18.5.2 Securing the Hotel Room

Upon entering the hotel room, it is recommended that staff should familiarize themselves with the surroundings:

- carefully study the hotel evacuation plan (usually on the room door) and note the emergency meeting point;
- visually note where the nearest emergency exit is and determine the quickest way to get to it. The route should be memorized in case there is reduced visibility during evacuation;
- make sure there is no evidence of tampering in the room. If there are signs of tampering, it could mean that someone else has access and this should be reported to the hotel reception immediately and another room should be assigned, especially if the hotel does not use electronic keys;
- make sure all the locks on the main door are working properly. All locks should be used when going to bed;
- verify that the telephone is working properly and take note of the hotel and local emergency numbers;
- make sure that you have air carrier contact numbers;
- verify that the hotel reception can be contacted quickly and easily;
- make sure that any valuables or security-sensitive items are stored in the room’s mini-safe.

18.6 PREVENTIVE ACTIONS

A few guidelines and procedures for staff to follow to minimize the risk of becoming a victim during a visit away from base are:

- if you do not feel safe getting in an elevator with a stranger, wait for the next one;
- try to vary your routine when returning to the hotel room;
- be discrete with the room number; do not disclose it to anyone;
- use caution if someone calls asking you to leave your room to go to reception - call reception to confirm;
- verify that the person knocking is really who S/he claims to be by using the spyhole. If the person claims to be a hotel employee and they were not requested, call the hotel reception to confirm their presence;
- upon returning to the room, have a quick look around to ensure there is no evidence of intrusion;
- leave valuables, purse/wallet, room key, mobile telephone and a jacket next to the bed in case of need
- be ready to evacuate in an emergency;
- keep a small torch/flashlight available in your room for use in the event of a loss of hotel lighting;
- keep the room key secure.

18.6.1 Fire and Evacuation

If the hotel fire alarm sets off while the crew or other staff are in their room, they should:

- never use the hotel elevators;
- collect the room key and head for the room door. If there is smoke in the room, roll down your bed and crawl to the door always staying as close as possible to the ground;
- touch the door before opening it. If it is warm there might be fire on the other side. It shall be kept closed;
- if the door is cool, open it while keeping a foot and shoulder against it which will enable it to be closed quickly if necessary;
- check for smoke and fire in the corridor;
- follow the emergency exit signs and use the nearest available emergency exit to leave the hotel as quickly as possible. Do not delay. Once outside, go to the emergency meeting point. Remain aware of your surroundings and monitor the development of events;
- only return to the hotel when told it is safe to do so by the authorities or hotel management.

If there is a confirmed fire but crew or other staff cannot exit the room or hotel because of the fire, they should:

- return to their room, close the door, all windows and shut the air conditioner off;
- call the hotel emergency number and advise that they cannot leave their room because of the fire;
- fill the bath, washbasin, rubbish bin and all other containers with water;
- wet all sheets and towels and place them around the room door to prevent smoke from entering;
- if there is smoke or fire in the room, wet another towel and put it over their mouth and nose;
- refrain from breaking any windows unless the room is completely filled with smoke;
- try to attract attention;
- do not attempt to jump or climb out of a window;
- follow the instructions of the rescue personnel when they are rescued;

- confirm the safety of all crew or other staff and report back to the air carrier's base and local management team;
- as soon as possible, call home to report that they are safe;
- only return to the hotel when told it is safe to do so by the authorities or hotel management (e.g. to collect belongings etc.).

18.7 LEISURE TIME

18.7.1 Dressing and Acting Appropriately

Staff should:

- dress in a manner that does not draw attention to themselves and that respects local customs and norms;
- only wear a minimum of jewellery and try to avoid wearing obviously expensive items. Not only can the items be stolen, crew will signal themselves as having money and probably other valuable goods on their person or in their hotel room;
- only carry what will be necessary for the outing. Excessive amounts of money or important documents should be left at the hotel;
- unless specified otherwise (by the Security Department or Station Manager) crew members should always carry their passports when they leave their hotel;
- carry all important documents in a money belt or pouch, preferably under at least one layer of clothing, or in a secure inner pocket;
- try to avoid carrying objects that highlight them as tourists or outsiders. If possible, do not carry belongings in a knapsack or backpack, use a purse or a bag with a shoulder strap instead. Make sure to wear the shoulder strap across the body to avoid the bag being easily snatched away by pickpockets;
- when walking on the street, as far as possible, walk facing oncoming traffic and carry handbags and belongings on your side facing away from the vehicle traffic or in front of you;
- have the necessary keys ready when approaching a residence or car.

18.7.2 Know the Area

Before going out, staff should familiarize themselves with the city using a map. As far as possible, avoid having to open large maps in public areas and/or on the street. It is preferable to carry a small map or pocket street index.

In addition to any brief received from the Station Manager, crew members and other visiting staff should also check with the hotel staff at reception as to which neighbourhoods should be avoided. Hotels selected by Pegasus Airlines are usually in safe areas of the city; ask the staff for the attractions, restaurants and bars in the area.

In the event that you do get lost, the most important thing is not to panic and to still act as if you have a sense of where you are. Ask a suitable passer-by for directions, call the hotel or consider taking an approved taxi to a safe/known location. Try to avoid walking near shrubbery, deserted/dark alleys and other isolated areas.

Never accept an offer for a ride from a stranger (including unapproved taxi operators) or attempt to hitchhike.

Staff should try to familiarize themselves with local customs like tipping, behaving with the proper etiquette, etc.

18.7.3 Use Caution When Talking with Strangers

When meeting new people, crew and other staff should:

- always use common sense. Part of the training for crew members covers how to read passengers for signs of nervousness or malicious intent. Use those skills along with other instincts when approached by strangers;
- try to work out if the person is genuinely alone. Look for non-verbal cues or communication with other people in the surrounding area;
- if drinking alcoholic beverages is locally acceptable, refrain from consuming large quantities, especially when alone;
- never leave a drink unattended even for a few seconds. Do not drink beverages that have been left unattended;
- avoid accepting drinks from strangers, unless ordering straight from the bar;
- be aware of the characteristics, use and effects of Rohypnol and other date rape drugs;
- do not discuss politics, ideology or religion with strangers;
- do not become spectators where there are protests or demonstrations. By-standers can quickly become embroiled if the protest turns violent.

The decision of staff to offer resistance if attacked should remain at their discretion. Pegasus Airlines briefs their staff, especially crews, on the most appropriate way to behave to ensure that the protection of the person is clearly placed well ahead of protection of possessions in order of priority.

18.7.4 Avoid Being Alone

As far as possible, crew members and other staff should try to avoid going out alone, especially at night.

However, if they do decide to venture out alone they should:

- keep to the main streets and roadways which should be more populated, even late at night. Also, try to use well-lit areas even if it means walking for a few more minutes;
- avoid walking near shrubbery, deserted/dark alleys or other isolated areas;
- walk confidently and with a sense of purpose. It is important not to become an easy target;
- do not isolate themselves from the outside world. For example, using a personal music device prevents them from gathering important information about their surroundings, and those around them, when walking or jogging. Also, it makes it easier for attackers to sneak-up on their victims;
- inform colleagues staying at the hotel or the hotel reception before going out. Provide an itinerary and an approximate time of return. When you do return to the hotel, inform them that you have arrived back safely.

18.8 CREW BAGGAGE

18.8.1 Packing and Securing Baggage

It is recommended that crew and other staff keep the following guidance in mind for packing and securing their baggage:

- only bring what is necessary for the duration of the trip to minimize the opportunity for theft or loss;
- prevent personal electrical items from being tampered with - any items that require modification or repair should be taken home for attention rather than sent to an unknown local supplier;
- avoid accepting items from people they have not known for a long time;
- all gifts received must be opened and checked before being packed to ensure they do not contain unauthorized or dangerous items;

- all items or gifts purchased away from base must only be wrapped or packaged in the presence of the staff member;
- always pack their own bags while confirming to themselves that the contents are secure (e.g. have not been tampered with). Some hotels offer a baggage packing service - decline this offer;
- ensure that any packed bags are made secure and are then kept protected from unauthorized interference (e.g. supervised by a crew member, stored in a secure cage etc.);
- any packed bags that have been left unattended (e.g. in a hotel room, in public areas of the hotel, in the custody of a porter, in an office etc.) should be checked by their owner before leaving for the airport to ensure that they have not been interfered with;
- theft of crew or other staff uniforms or identification cards (IDs) should be reported immediately to the Station Manager and the head office of the Aviation Security Group Department. Stolen uniforms and IDs could be used by unauthorized persons to access air carrier and airport facilities and operations.

18.8.2 Crew Baggage Transportation, Check-in and Screening

Crew members differ from normal staff in that they often travel in a group. When crew travel together, either one crew member should be in charge of supervising the on and offloading of baggage at the hotel and airport or each individual crew member should remain responsible for their own baggage throughout the journey. Crew bags should be locked and not left unattended at any stage during the transit from hotel to airport check-in. Protecting the baggage in this way should prevent any unauthorized interference and provide a safeguard against terrorist or criminal activity. Such interference could take the form of attempting to insert an item in a bag, attempting to add a bag to the load or attempting to substitute a bag. Individual crew members should then personally account for their hold baggage at the time of check-in or loading at aircraft side (as appropriate). Similarly, all items of cabin baggage should be protected and accounted for.

Crew members shall not look after the bags of strangers and shall not expect to have others look after their bags. They shall not accept anything for carriage on a flight from a stranger.

When going through the airport security checkpoint, crew members should be mindful of the potential for the theft of electronic items (such as mobile telephones, PDAs, etc.) and other items of value (e.g. coins). Crew should be aware of what they remove from their pockets when going through the archway metal detector and make sure they have all their possessions before leaving the screening area.

In some locations, crew members should also be aware of the potential for attempted bribery and corruption by customs and immigration officials as well as by screeners. Any such attempt shall be reported to the Station Manager or a senior official immediately.

Crew members travelling on duty but with no operational role on the flight (e.g. positioning crew) shall comply with the same security procedures and follow the same check-in and boarding process as other passengers. They shall take the same care to protect their baggage and to be aware of security requirements.

In general, all staff should be mindful of their surroundings at the airport and should remain vigilant. They should try and avoid crowded or vulnerable areas, particularly in the landside part of the airport. The threat of terrorist attacks against such areas has to be recognized and measures put in place by the local authorities and airport management to mitigate the risk. In higher threat locations, the air carrier's Security Department might become involved in assessing the best location for the crew check-in operation and the route that crew should take through the airport (on arrival and departure).

Pickpockets and petty thieves can often be found in airports and crew members and other staff should remain vigilant.

18.9 HIGH-RISK SITUATIONS AND OTHER EMERGENCIES

18.9.1 Civil Unrest, Armed Conflicts and Similar Events

At high-risk stations or when there is an increased threat because of an armed conflict, civil unrest or similar events, the following added measures should be implemented:

- the company should defer duty travel unless it is absolutely necessary;
- a list containing local management/representatives and emergency numbers should be given by the local air carrier representative to every staff member upon arrival. It is recommended that they keep the list with them as well as their passport and company ID;
- except for essential work-related issues, staff must avoid leaving the hotel or going to places considered dangerous when a situation of conflict exists;
- for crew, the Pilot-in-Command should account for the whereabouts of all staff and keep the company informed accordingly;
- if allowed to leave the hotel, crew members or other staff should record their destination and planned time of return on a list to be kept at the hotel reception. This will help locate and account for them in the event of an emergency;
- in general, staff should seek and follow the advice of the hotel management and local authorities in such situations;
- when it is deemed appropriate and safe, the air carrier management should consider making arrangements to evacuate crew and other staff from the station. This will be done in coordination with the relevant local and national authorities.

18.9.2 Tornadoes and Hurricanes

In cases where there is a major storm, tornado or hurricane, staff shall obey instructions given by the hotel management. If no specific guidance is given, crew should:

- stay inside and in the most protected part of the room, usually the bathroom, or take cover under a strong table. If time permits, find an emergency stairwell which would provide more protection;
- protect themselves from flying debris, using mattresses or blankets;
- anchor themselves to a strong structure such as the main water pipe;
- beware of the “calm eye” of the storm – a period lasting from minutes to an hour where the storm seems to calm down before getting strong again;
- remain indoors until given the all-clear by the authorities and/or hotel staff;
- stay informed by watching television and/or listening to the radio for emergency bulletins;
- stay out of damaged buildings;
- confirm the safety of all crew members and report back to the air carrier as soon as it is possible - call home to report that they are safe.

18.9.3 Earthquakes

Earthquakes can rarely be predicted. As with any other emergency, the most basic thing to do is to remain calm.

As soon as staff realize that they are experiencing an earthquake they should:

- If indoors:
  - take cover under a desk, table, door frame or stay against a wall;
  - stay away from all windows, mirrors and glass;

- refrain from using matches, candles and any other open flame in case there is a gas leak;
- once the shaking stops, turn off all appliances except radios and television;
- if there is a smell of gas, open a window and evacuate if it is safe to do so.
- Report any gas leak to the hotel reception or authorities;

- If outdoors:
  - refrain from re-entering the building until permission has been given by the authorities;
  - stay in the open, away from buildings and power lines.

- If in a car:
  - stop and stay inside;
  - be aware of aftershocks;

- In general:
  - stay informed by watching television and listening to the radio for emergency bulletins;
  - stay out of damaged buildings;
  - confirm the safety of all crew members and report back to the air carrier as soon as it is possible
  - call home to report that they are safe.

18.9.4 Defending Yourself

Crew members are always encouraged not to intervene physically when confronted with disruptive passenger behaviour. They should try to talk down the situation. This will have the added benefit of warning other crew members and able-bodied persons (or pre-selected passengers) of the possible problem.

However, if a cabin crew member is physically attacked, S/he has every right to defend him/herself and restrain the passenger. The emphasis of physical intervention is that it should always be defensive (either for the crew member, a passenger or the aircraft itself) and never offensive. Crew members should be taught basic evasion and separation techniques as well as basic blocking movements in case there is an attempt to strike them. Crew members should also be taught that, by acting as a team using simple techniques, they have the ability, regardless as to their size and gender, to restrain a violent passenger.

Training and usage of sophisticated martial arts or hand-to-hand combat is to be strongly discouraged. In order to master and maintain these tools, frequent and intensive training is required, something which cannot be provided to staff by an air carrier. Moreover, inadequate training in martial arts can cause crew members to cause more harm than necessary to themselves and possibly to the perpetrator.

The ultimate goal of self-defence is to ensure your own safety and gain control of the disruptive passenger in order to apply restraints and neutralize the perpetrator for the rest of the flight.

End of Section

19 CYBER THREATS TO CRITICAL AVIATION INFORMATION AND COMMUNICATION TECHNOLOGY SYSTEMS

The civil aviation operation environment is changing rapidly and significantly, with the deployment of new advanced technologies and communication systems, shifting from manual processes to more efficient automated processes, communications, and storage, in order to enhance security and facilitation.

Pegasus Airlines is certified with the standard of ISO/IEC 27001 Information Security Management Systems.

ISO 27001 (formally known as ISO/IEC 27001:2005) is a specification for an Information Security Management System (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes.

Pegasus Airlines IT Security Management has identified critical information systems software and hardware used in their operations, which may include, but are not limited to:

(a) access control and alarm monitoring systems;

(b) departure control systems;

(c) passenger and baggage reconciliation systems;

(d) screening systems and/or explosive detection systems, whether networked or operating in a stand-alone configuration;

(e) regulated agent and/or known consignor databases;

(f) air traffic management systems;

(g) aircraft operator reservation and passenger check-in systems;

(h) closed-circuit television surveillance systems; and

(i) security command, control and dispatch systems.

The use of such systems, the increased connectivity or links between ground systems and aircraft, as well as the use of commercial off-the-shelf software and hardware, constitute an array of potential vulnerabilities.

The safety of passengers, crew and ground personnel would be endangered in the event that such systems were tampered with. Additionally, passenger and employee personal information shall be protected against unauthorized access and use.

States should therefore include appropriate provisions for the protection of such critical aviation information and communication technology systems, including hardware and software, against cyber-attacks and interference, in their NCASPs and other relevant national programmes.

NCASPs should indicate that the nature of these systems and the information contained therein is critical to the safety and security of civil aviation operations.

The objectives of these measures should be, at a minimum, to:

(a) protect the systems against unauthorized access and use;

(b) prevent tampering with the systems; and

(c) detect attacks on the systems.

The physical protection of such systems should begin at the design stage or as early as practicable to ensure that they are as robust as possible against cyber-attacks. This may be achieved using a multi-layered approach, which includes, but is not limited to:

- administrative controls, such as:
  - security standards, policy and procedures;
  - appropriate recruitment, selection and training of staff, particularly persons with administrator rights, including background checks;
  - threat and risk assessment to determine the vulnerability of a system and the likelihood of attack;

  - quality control, including inspections and tests; and

- virtual or logical controls, such as:
  - firewalls
  - data encryption;
  - network intrusion detection systems;
  - anti-virus systems; and

- physical controls, such as:
  - ensuring system hardware, particularly servers, are appropriately secured and located in areas to which access is controlled;
  - implementing authentication systems verifying that only those authorized to have access are accessing the system, such as biometric login methods and/or passwords;
  - limiting the number of persons with authorized access;
  - requiring more than one person for approvals within systems, for example, an airport identification permit may only be produced with two persons authorizing its production;
  - continuously monitoring and controlling of access to systems;
  - using remote backup systems in the event of loss of the primary system; and
  - maintaining activity logs which can be useful in auditing and evaluating, as well as providing alerts when there is activity outside of normal operating parameters.

The protection of critical aviation information and communication technology systems, including their hardware, software and data, shall be included in threat assessment processes established by the appropriate authority. This may be achieved by including critical aviation information and communication technology systems in assessments of likely methods of attack.

The appropriate authority shall also require operators to conduct vulnerability assessments of their aviation information and communication technology systems, establish measures to mitigate potential cyber-attacks and verify the implementation of such measures as part of their regular compliance monitoring activities, such as inspections and audits.

19.1 SECURITY MEASURES FOR INFRASTRUCTURE

Pegasus Airlines shall ensure security measures in the design, implementation and operation of new aviation information and communication technology systems, including the disposal of hardware and software.

Modifications to existing systems shall also take into account security to the extent practicable. For example, the design and construction of airport and aircraft operator facilities (e.g. check-in and boarding counters, ticket counters, screening checkpoints, etc.), cargo and logistics centres for airport supplies, are best served when security is taken into consideration at the earliest stage of the process. This offsets the costs and negative operational impacts of having to retrofit facilities or equipment.

The specifications for, and procurement of, new aviation information and communication technology systems shall include security provisions. Suppliers shall provide details as to how information on and operation of the system is secured, including arrangements for ongoing support and maintenance, whether on-site or from remote locations.

Preventative maintenance shall be scheduled and managed and if support and maintenance is outsourced, the number of individuals permitted access to system software and hardware shall be limited. Such a measure will help prevent unauthorized access to the system and minimize the opportunity for individuals to interfere with the integrity of the system. Similarly, routes for cables shall be designed so that critical aviation information systems cannot be easily infiltrated.

19.1.1 Network Separation

Pegasus Airlines shall ensure that networks used for critical aviation information and communication technology systems are separated from networks to which the public has access.

The software and hardware of a modern aviation information and communication system are inoperable without the necessary cables and connectivity to another operational system network to facilitate data transmission and exchange. For that reason, systems shall be examined to ensure that security objectives are not compromised by exposing them to uncontrolled or open access communications networks, and appropriate policies and practices shall be in place to reduce the number of connections to the minimum required. This practice is often referred to as 'hardening'.

Connections to networks shall take place under controlled conditions, where the type of information and frequency or method of data exchange between the system and the network is known. An effective management system for these network interfaces shall be established to ensure that all connections to a system are documented, reviewed, and upgraded as necessary and that adequate virus and malware protection is in place, where applicable.

Additionally, a layered approach to software management shall be considered. A limited number of individuals shall have administrative rights to a critical aviation information and communication technology system. Access to such a system shall be based on the principle of legitimate need. For example, some individuals may only be granted read-only rights, while others may be granted access only to parts of the system relevant to their specific tasks.

For further details, please refer to *PG-BG-TL-007 Network Access Control*, available in Comply365.

19.1.2 Remote Access

Pegasus Airlines shall ensure that remote access to critical aviation information and communication technology systems is only permitted under pre-arranged and secure conditions, and that suppliers do not have unauthorized access to such systems after they have been procured and/or installed.

In most instances, remote access requires that suppliers have a means of accessing a system. Operators shall ensure that this access route is known to them, and that the method and conditions of entry are agreed upon. For example, the supplier shall be required to notify a designated official from the operator whenever access to the system is needed. Alternatively, an automatic e-mail message shall be generated to notify the designated official from the operator each time access is sought.

Maintenance of systems shall be performed by authorized personnel only, and at pre-arranged and approved times. Operators shall request suppliers to limit the number of persons authorized to provide support and maintenance to the system. Background checks shall be conducted on such persons, including criminal history to the extent legally permissible.

The above measures shall be complemented with an appropriate audit and exception reporting system generating an automatic report whenever there is abnormal activity in the system, such as access to the system outside the normal operating hours. For example, shall entry be sought outside the pre-arranged hours, an exception report shall be sent to a supervisor with responsibility for the system. This person shall follow up with the supplier to determine why entry was necessary without prior agreement. Similarly, audit logs shall be reviewed regularly to identify and follow up on exceptional access.

Unofficial pieces of code within software, also referred to as "back doors", may be used by suppliers and others to enter and use a system undetected. This vulnerability is almost impossible to mitigate against, but certain measures may assist in detection. Implementing software behind a firewall not provided by the same supplier and regular system audits, shall identify any unusual activity on the system.

Pegasus Airlines shall request a certificate from suppliers stating that no such back-door access exists and guaranteeing the integrity of the system. This could be helpful in the event that prosecution is necessary.

For further details, please refer to *PG-BG-PR-014 - Remote Working Procedure*, available in Comply365.

19.1.3 Supply Chain Security for Hardware and Software

Aviation information and communication technology systems need to be upgraded from time to time due to changes in operating requirements or software upgrades, and often require modifications in software

and/or hardware. In each of these circumstances, there is a possibility for the unauthorized introduction of software or hardware that can attack, infiltrate, or compromise the integrity of the system.

Measures shall be in place to ensure that only reputable and legitimate suppliers are used to procure hardware and software for aviation information and communication technology systems. The concept of supply chain security shall be applied to the extent practicable. The objective of this measure is to ensure that the integrity of software and hardware is protected against unauthorized interference throughout the supply chain. Suppliers shall be required to provide details of their security measures, not only at the installation stage, but also over the lifetime of the system.

For further details, please refer to *PG-BG-PR-013 - Supplier Data Protection Procedure*, available in Comply365.

19.1.4 Cyber-Attack Incident Records

Understanding the threat and the likely methods of attack is a key element in developing appropriate security measures to safeguard aviation information and communication technology systems against cyber-attacks.

One source of information that is helpful in this process is the review of incident reports.

There are several steps that appropriate authorities shall take for this to be effective which include, but are not limited to:

(a) develop and implement a template for reporting cyber-attack incidents. This would facilitate the collection and analysis of information, including threat assessment, and the implementation of appropriate counter measures,

(b) establish an alert system to facilitate communication with operators and other stakeholders; and,

(c) establish provisions in State NCASPs to require operators to implement a reporting regime in their organizations, and to include such regimes in operator security programmes.

For further details, please refer to *PG-BG-PR-024 Information Security Incident Procedure*, available in Comply365.

End of Section