



**SEM - SUBCONTRACTOR VERSION  
SECURITY MANUAL**

---

---

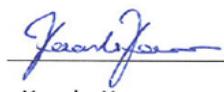
**FINNAIR  
SECURITY MANUAL - SUBCONTRACTOR VERSION**

The Content Of This SEM Subcontractor Version Is Confidential

This version is based on SEM revision 19, 21.9.2023.

List of Effective Pages:

Pages 1 - 72

  
\_\_\_\_\_  
Kaarle Karvonen  
Head of Security

Approval date: 21.9.2023

**COPYRIGHT ©**

Copyright © Finnair Oyj 2023. All rights reserved. The contents must not be reproduced without prior permission from the owners of the copyright.

Accountable Manager, Operations Division, ZO/503  
P.O. Box 15, 01053 FINNAIR, Finland.  
Tel: +358 9 818 5252



## **SECURITY MANUAL**

### **Revision 19**

#### **Record of Revision**

**Copyright © Finnair Oyj 2023**

All rights reserved. The contents must not be reproduced without prior permission from the owner of the copyright.

Head of Security, AL/69 P.O. Box 15, 01053 FINNAIR, Finland.  
Tel: +358 9 818 5600

<b>Rev No</b>	<b>Effective Date</b>
8	01.2.2013
9	20.1.2014
10	19.5.2014
11	18.9.2015
12	5.11.2015
13	15.1.2016
14	22.10.2017
15	04.7.2018
16	01.8.2019
17	22.6.2021
18	29.12.2021
19	21.9.2023

#### **Temporary Revision Record**

<b>Rev No.</b>	<b>Effective Date</b>	<b>Chapter</b>
-	-	-

## **0. DEFINITIONS**

**Accompanied hold baggage:** Baggage accepted for carriage in the hold of an aircraft, on which the passenger who checked it in is on-board.

**Airside:** The movement area of an airport, adjacent terrain and buildings, or portions thereof.

**Aircraft not in service:** Aircraft not in service shall mean an aircraft that is either parked for a period for more than 12 hours or is not under surveillance sufficient to detect unauthorised access.

**Aircraft Security Search:** A thorough inspection of the interior and the exterior of the aircraft for the purpose of discovering prohibited articles.

**AOSP - Aircraft Operator Security Programme:** Security Manual is description of AOSP.

**Background check:** A check of a person's identity and previous experience, including any criminal history, as part of the assessment of an individual's suitability for unescorted access to security restricted areas.

**Cabin baggage:** Baggage intended for carriage in the cabin of an aircraft.

**Commercial Flight:** A scheduled or non-scheduled flight or flight activity rendered for hire to the general public or private groups for valuable consideration.



**Co-Mat:** Abbreviation of air carrier company materials, shipped within its network of stations.

**Co-Mail:** Abbreviation of air carrier company mail, shipped within its network of stations.

**Continuous Random Checks:** Checks conducted during the entire period of activity, whilst those checks are to be conducted on a random basis.

**General Aviation:** Any scheduled or unscheduled flight activity not offered or available to the general public.

**GOM:** Ground Operations Manual.

**EDS - Explosive Detection System.** A 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, irrespective of the material from which the bag is made.

**EDDS - Explosive Device Detection System.** A 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, irrespective of the material from which the bag is made.

**High Risk Cargo and Mail:** Cargo and mail, which has been identified by airline, relevant authority, law enforcement or intelligent service as posing a risk to aviation safety or security or cargo and mail from specific countries listed in Cool Cargo security program or cargo and mail tampered in a way that it would have been possible to conceal the prohibited article or which are otherwise suspicious.

**Hold Baggage:** Baggage intended for carriage in the hold of an aircraft.

**Known Consignor:** (a) For Cargo: The originator of property for transportation by air for his own account and who has established business with a regulated agent or air carrier.(b) For Mail: The originator of mail for transportation by air for his own account and who has established business with a regulated postal authority/administration.

**LAGs:** Liquids, Aerosols and Gels.

**Landside:** The area of an airport which is not airside and includes all public areas.

**Mail:** Despatches of correspondence and other objects tendered by and intended for delivery to postal administrations. A postal authority/administration is defined by Member States.

**Operational Ground Staff:** Ground staff with security related duties as mandated in SEM, e.g. loading staff, customer service personnel, catering staff.

**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. An indicative list of such prohibited articles is found in the Annex 1.

**PEDS:** Primary Explosive Detection System. A 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, irrespective of the material from which the bag is made.

**Operational Ground Staff:** Ground staff with security related duties as mandated in SEM, e.g. loading staff, customer service personnel, catering staff.

**Regulated Agent:** An agent, freight forwarder or 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, courier and express parcels or mail.

**Secure clean:** process where cleaning company performs security search in Cabin in addition to standard cleaning

**Security:** A combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference.

**Security Restricted Area:** Airside areas of an airport into which access is controlled to ensure security of civil aviation. Such areas will normally include, inter alia, all passenger departure areas between screening points and aircraft, ramp, baggage make-up areas, cargo sheds, mail centres and airside cleaning and catering premises.

**Security Controls:** Means by which the introduction of prohibited articles can be prevented.

**Service panel:** Service panel means aircraft external access point used for providing aircraft services; such include water, lavatory, ground electrical outlets and other service compartments that have external clip-down panels.



# SEM

## FINNAIR SECURITY MANUAL

Effective date  
21.09.2023, Rev 19

Page  
3

**Screening:** The application of technical or other means which are intended to identify and/or detect prohibited articles.

**STEB:** Security Tamper Evident Bag.

**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

**Terminal:** The main building or group of buildings where the processing of commercial passengers and freight and the boarding of aircraft occurs.

**TIP:** Threat Image Projection, a software programme, which can be installed on certain x-ray machines. The programme projects virtual images of threat articles (e.g. a gun, knife, improvised explosive device) within the x-ray image of a real bag under examination, and provides immediate feedback to the x-ray machine operator on the operator's ability to detect such images.

**Trace Detection Equipment:** Technology system or combination of different technologies which has the ability to detect very small amounts (1/billion of a gram), and so to indicate by means of an alarm, explosive materials contained in baggage, or other articles subjected for analysis.

**Unaccompanied hold baggage:** Baggage accepted for carriage in the hold of an aircraft, on which the passenger who checked it in is not onboard.

### Acts Of Unlawful Interference

An act of:

- (a) Violence against a person on board an aircraft in flight if that act is likely to endanger the safety of that flight;
- (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 causing damage to it which renders it incapable of flight, or causing damage to it which is likely to endanger its safety in flight;
- (d) Destroying or damaging air navigation facilities or interfering their operation, if any such act is likely to endanger the safety of aircraft in flight;
- (e) Communicating information which is known to be false, thereby endangering the safety of an aircraft in flight; or
- (f) Unlawfully and intentionally using any device, substance or weapon:
  - 1. Performing an act of violence against a person at an airport serving civil aviation which causes or is likely to cause serious injury or death;
  - 2. Destroying or seriously damaging the facilities of an airport serving civil aviation or aircraft not in service located thereon or disrupting the services of the airport;

if any such act endangers or is likely endanger safety at that airport.

## 1. GENERAL

### 1.1 FINNAIR SECURITY POLICY

#### 1.1.1 Statement

This is to certify that Finnair Security Manual is issued in accordance with relevant regulations. It complies with applicable EU security regulation and the National Civil Aviation Security Programme of Finland.



Finnair Oyj  
Topi Manner  
President and CEO

Finnair Oyj  
Jaakko Schildt  
Senior Vice President, Operations  
Accountable Manager

## **1.1.2 Policy**

Security is a fundamental operational priority for Finnair. The Company and its organisation is committed to

- the provision of resources necessary for the successful implementation of this Policy,
- compliance with applicable regulations and standards of Finnair,
- promotion of security awareness and the establishment of a security culture,
- the establishment of security objectives and security performance standards,
- continual improvement of the security management system, and
- periodic review of this Policy to ensure continuing relevance to the organisation.

This Policy shall be communicated throughout the organisation by the Head of Security.

All Finnair operations shall be conducted in compliance with the procedures and limitations contained in the Company Manuals and current regulations of the authorities.

Finnair protects its operations, activities, staff and property against acts of unlawful interference by following international and national laws and aviation security regulations and by developing its own precautions against such acts.

This is achieved by developing and maintaining the Finnair Security Programme, in the form of this Manual.

Security in Finnair consists of all measures that aim to protect the Company's business, operations, customers, crew, personnel and property against acts of unlawful interference.

This Manual is based on EU Regulation 2015/1998 and other applicable EU regulations, ICAO Annex 17 and the Security Manual, Finnish Law, the National Civil Aviation Security Programme of Finland and the general interests of Finnair.

The Manual consists of procedures and measures to provide guidance for essential security matters, and to ensure their appropriate implementation and practice. This Manual (and associated Manuals) also aims to ensure applicable personnel have the direction necessary to implement security measures and to provide additional security measures that can be implemented during a time of increased threat determined by the state, as well as to meet the requirement of the civil aviation security programme of all states served by the Operator. The Finnair security organisation, duties and responsibilities are also described in this Manual.

The Manual is reviewed and approved by the Finnish Civil Aviation Administration (CAA). The Manual also forms the aviation security programme required by ICAO Annex 17. Furthermore, the Manual is a precondition for a valid Air Operator Certificate.

The Manual must be observed in all Finnair operations. If the Manual contradicts the national law of a country where Finnair is operating, the national law shall be observed. If the manual requirements defer from the law in the country where Finnair is operating, the more demanding shall be complied with. Security instructions published in other official Company documentation (e.g. manuals, technical instructions) shall be approved by the Head of Security.

This Manual is maintained, developed and revised by the Head of Security (HEL-AL).

## **1.2 USE OF MANUAL**

The English version of the manual is the only official version.

The Security Manual is published in an electronic form only. The main distribution channel is Finnair Sharepoint. Subcontractor version of the manual is available via Company Hub.

At the beginning of the manual there is a list of effective pages. Each user of the manual shall ensure, as necessary, from the issuer, which revision is the official up-to-date version.

Each page has a header which indicates the acceptor of the text, effective date, and chapter and page number.



The Security Manual must be available to persons listed in the distribution list.

### **1.2.1 Maintaining and Revisions**

When the manual is amended, new Security Manual files are updated and published in an electronic form and a notification of revision is sent to each person having access to the electronic Manual. A list of persons having access to the Manual shall be maintained by the Head of Security.

The latest revised, new or deleted information is indicated by a vertical line in the margin and/or with different colour in the text.

The Head of Security is responsible for maintaining and for accepting changes to the Manual. He shall be informed about all discrepancies or errors in this manual as well as of any changes that require revision to the list of persons having access to the Manual.

NOTE:

Nominated persons are responsible for the distribution, maintaining distribution lists and revision control as well as other requirements mentioned in this chapter for SEM Subcontractor Version that they have forwarded to relevant recipients.

### **1.2.2 Temporary Revision**

A Temporary Revision of this manual shall be published by the Head of Security when there is an immediate need to amend or give new or additional instructions to personnel.

### **1.2.3 RESERVED**

### **1.2.4 Information Leaflet**

Information leaflets are published to inform personnel about regulations, instructions, changes etc. which are not/cannot be included in the permanent manual. The persons in the distribution list shall read the leaflets and make themselves familiar with the contents, even if the leaflets are intended for one time use only.

### **1.2.5 Finnair Security Manual, Subcontractor Version**

Finnair Security Manual, Subcontractor version is an extract of the Security Manual and is developed in aim to communicate security relevant information for Finnair subcontractors. The subcontractor version is issued to subcontractors by the nominated persons.

### **1.2.6 Document Management**

The purpose of document management is to ensure that all new or revised controlled security documents are:

- Exact description of the function, recorded action or specification,
- Standardized by form,
- Individually identified,
- readily identifiable and accessible to applicable operational personnel,
- contains legible and accurate information,
- presented in a format appropriate for use by operational personnel,
- In compliance with Authority requirements,
- Appropriately prepared, inspected and approved,
- Appropriately distributed to applicable personnel,



- Retained as required and
- Disposed or deleted according to Company information security guidelines.

### **1.2.7 Operational Security Records**

Operational security records are records that include objective evidence about the operational security system and conformity with security requirements.

Operational security documents shall be retained for 2 years and be readily available and be protected from unintentional deletion and unauthorised use.

Such security records that contain sensitive or restricted information shall be handled in accordance with Company information security guidelines. It shall be ensured that when such a document is not in a physical possession of an authorized person, records are stored in a secure place (e.g. locked file cabinet or drawer). A review shall be conducted once a year to identify records that are no longer valid. Records that are not valid shall be destroyed in a manner that precludes recognition or reconstruction of the information.

### **1.2.8 Copyright**

Copyright © Finnair Oyj 2012. All rights reserved. The contents must not be reproduced without prior permission from the owners of the copyright. Finnair Operations Division, P.O. Box 15, FIN-01053 Finnair, Finland. Tel. +358 9 81881

## **1.3 GENERAL RESPONSIBILITIES**

Government authorities are in principle responsible for maintaining adequate security measures to safeguard operations at airports under their jurisdiction and to ensure undisturbed activities. Each nation shall have a valid National Civil Aviation Security Programme.

In countries with more than one international airport, governments shall establish a National Civil Aviation Security Committee. Both government and the aviation industry should be represented. The committee will advise on security policy and ensure a uniform and effective application of the National Civil Aviation Security Programme.

At each airport, a security committee, preferably headed by the Airport Manager and composed of representatives of various authorities and users, will be responsible for developing and implementing general security measures and procedures at the airport in conformity with the National Civil Aviation Security Programme. The committee should be open to participation by one or more representative of the airlines, selected from the members of the Airline Operators Committee.

In most countries, government authorities are responsible for security measures at airports, including passenger and baggage screening. Airlines operate under the security protection of authorities and are obliged to follow general and local security regulations in their operations and must maintain their own security procedures. In some countries, airlines are held responsible for airport security in a more extensive area, including passenger and baggage screening, access control etc.

## **1.4 COMMUNICATION**

Effective communication of security related issues is essential to ensure the appropriate level of security. Communication is also an integral part of the Company Security Management System.

Nominated persons and heads of various departments shall inform the Head of Security of security related issues.

### **1.4.1 Communicating Security Relevant Information**

The Head of Security shall communicate security relevant information to the management, crew, operational personnel and stations.

The methods used for communicating may include, but are not limited to following:

- telephone, email
- ACARS



- in person
- Finnair Crew Information System
- Finnair Company Hub
- Manuals, Information Leaflets

The Head of Security shall initiate the communication through relevant channels. When using the Crew Information System the Head of Security shall ensure that the information is inserted to the system to be available for crew members and also deleted when not applicable any more.

Cockpit door related security sensitive information (e.g. procedures and door codes) shall be distributed to Finnair crew members in person in aim to verify the recipient's identity and eligibility for receiving the information as well as to gain a written receipt of acknowledgment. Distribution of cockpit door codes to other persons or entities than crewmembers shall be approved by the Head of Security and made in accordance with Finnair Information Security Principles.

Cockpit door procedures as well as all other security related information is strictly confidential.

## **1.4.2 Informing Company Management of Security Issues**

The Company management is informed of security issues on a regular basis by the Head of Security through the Safety Review Board.

## **1.4.3 Reporting**

The objective of security reporting is to continuously improve security and mitigate possible threats. Security occurrences related to Aviation Security shall be reported using Air Safety Report (ASR), Ground Safety Report (GSR) or Personnel Disturbance Report (PDR). Company/Personnel, Cyber/Data Security, Fraud and other security occurrences shall be reported using generic Security Report (SR).

All security concerns that have or may have an impact on Finnair shall be reported. Typically, these could be suspicious acts, non-compliances to security directives, violations to company rules/regulations, unsecure practices, failed security controls or other applicable occurrences.

Security occurrences shall be reported to Safety and Compliance Management Application (Q-Pulse), which is available in Company Hub (Intranet). Security Report handling follows principles, which are valid also for Safety reports. These principles are described in SCMM Appendix 5. All Security occurrences shall always be investigated (level D), classified and risk rated. If the risk is high enough, then corrective/preventive action shall be taken.

It is also possible to submit a report anonymously. If employee wants to report something confidentially without name, it can be done by filling a "Confidential report" paper form available in Crew Center and delivering it directly to Head of Security.

Confidential issue can also be reported informally using direct e-mail to Head of Security. Feedback concerning confidential report is provided by Head of Security.

See also Operations Manual part A, chapter 11.

## **1.5 Reserved**

## **1.6 SECURITY RESPONSIBILITIES IN FINNAIR**

### **1.6.1 Overview**

Security in Finnair is based on a decentralised model. The Head of Security is responsible for evaluating the security and threat situation and to determine appropriate security measures accordingly. All Finnair business units, subsidiaries and individual departments are responsible for implementing and maintaining these security measures within their fields of activities and areas of responsibility. When applicable or requested by the Head of Security, security contact persons shall be appointed to assist the heads of the business units and subsidiaries in the planning, execution and follow-up of security matters and also in contacts with Head of Security.



---

The Head of Security shall be informed of the appointments and subsequent changes. Appointed persons shall be acceptable by the Head of Security.

See Annex 5 for “Security Key Personnel”.

---

### **1.6.2 Accountable Manager**

The Accountable Manager shall approve the Finnair Security Programme. He is also responsible for ensuring that adequate resources are allocated in the field of security.

---

### **1.6.3 Executive and Senior Vice Presidents**

The Executive and Senior Vice Presidents are responsible for evaluating the need for appropriate and reasonable security measures and for maintaining these within their respective areas of responsibility. All security measures and their maintenance shall be in conformity with this Manual, and shall be accomplished in co-operation with Head of Security.

#### [1.6.4. Nominated Postholders](#)

---

### **1.6.4 Head of Security**

The Head of Security is accountable for security and is in charge of leading and managing security activities within the Finnair Group. He is also responsible for leading and managing the Security Management Unit.

The Head of Security has direct access to the Chief Executive Officer and the Accountable Manager. The Head of Security reports to Vice President Safety, Security and Compliance. The deputy for Head of Security is Manager, Business Resilience.

The Head of Security is responsible, and has respective authority, for:

- the Security Management Unit
- Finnair Security Programmes and Policies (including development, maintenance and implementation);
- Accountable for SeMS (Security Management System);
- assisting and advising the President, Senior Vice Presidents and line organisation in areas within his remit;
- Follow-up and evaluation of the security and threat situation of all Finnair operations and route network, and to act accordingly;
- the development and promulgation of security standards and practices to provide line management with direction and control;
- Reviewing and updating company security training programmes for continuous improvement and to reflect regulatory and operational changes;
- ensuring the effective implementation of security procedures and measures with regular evaluations, inspections and audits;
- following international and national developments in security (e.g. new or revised security directives and regulations) and communicating such issues to relevant departments within Finnair
- Ensuring an effective risk analysis, threat assessment and response capability;

He shall also:

- Have overall accountability for ensuring operations are conducted in accordance with conditions and restrictions of the AOSP and in compliance with applicable regulations and standards of the Operator.
- follow international and national developments within his area of responsibility (e.g. new or revised directives and regulations) and to communicate them to relevant departments within Finnair
- approve security instruction issued by other departments in Finnair as well as keep records of such approvals
- co-operate with authorities and various relevant organisations
- represent Finnair in the National Civil Aviation Security Committee of Finland
- share information between relevant authorities, airports, air traffic service and external service providers to enable effective risk assessment process



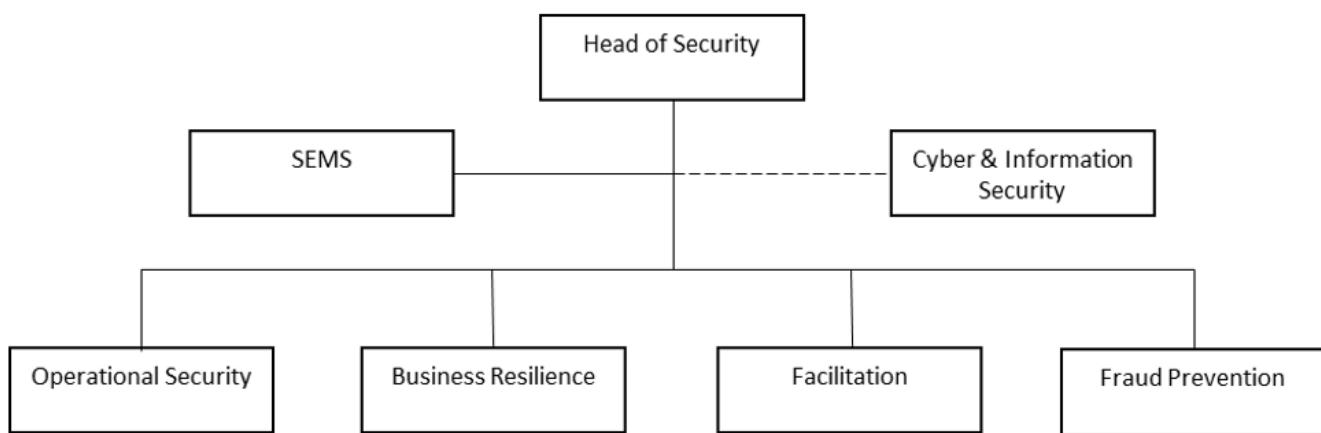
- represent Finnair in national and international bodies (e.g. IATA, AEA, ICAO, ECAC) in matters within his area of responsibility,
- maintain contacts with other airlines, especially oneworld partners
- act as a member of Safety Review Board

If security is threatened or may be threatened as a result of a specific incident, the Head of Security is responsible for deciding all the security measures needed. The implementation of these measures should be carried out in co-operation with the departments concerned. If the threat is aimed towards a specific flight or part of flight operations or crew members, Flight Operations shall be involved.

## **1.6.5 Security Management Unit**

The Security Management Unit is responsible for the development, management and continuous improvement of group security (aviation, corporate, cyber, information), facilitation, fraud prevention, resilience and insurance. The unit is headed by the Head of Security and it consists of security managers with specific roles and responsibilities as described below.

### **1.6.5.1 Organisation Chart**



## **1.6.6 GENERAL MANAGERS, REGIONS AND AREA MANAGERS, STATIONS**

General managers and Area Managers are responsible for Finnair security matters within their respective area of responsibility.

General managers and Area Managers are responsible for liaising and co-operating with local authorities and for the development of local security procedures. This is to ensure that Finnair security procedures are in accordance with local legislation, aviation regulations and the local security situation.

General managers and Area Managers shall continuously evaluate the threat and security situation in their region and keep the Head of Security informed of changes and problems.

## **1.6.7 Finnair Airport Service Managers and In-House Airport Service Managers**

Finnair airport service managers and In-house Airport Service Managers are responsible for Finnair security matters at their respective stations.

Finnair airport service managers and In-house Airport Service Managers are responsible for continuously evaluating the threat situation against Finnair and civil aviation in general, and for monitoring the effectiveness of security measures concerning Finnair operations.

Finnair airport service managers and In-house Airport Service Managers shall ensure that individual Finnair security procedures and measures are in accordance with local legislation and aviation regulations.



Finnair airport service managers and In-house Airport Service Managers shall maintain contact with local security authorities and the airport security committee. They shall keep the Head of Security informed about local security directives and regulations as well as other security related issues.

If the level of threat is increased, it is the responsibility of the Finnair airport service managers and In-house Airport Service Managers to implement the necessary actions in co-operation with the local authorities, the Commander (if applicable) and the Head of Security.

---

## **1.6.8 Reserved**

---

## **1.6.9 Operations Control Center (OCC)**

Finnair Operations Control Center is responsible for acting as a 24-hour information and co-ordination centre for security matters that require urgent forwarding to the Head of Security or his deputy.

OCC shall also inform applicable aviation authority in case of unlawful interference or a preparatory act against the Finnair has occurred.

In rapidly increasing threat situations OCC Duty Manager has the authority to initiate and control the immediate security actions.

---

## **1.7 COMPETENCE AND EXPERIENCE OF PERSONNEL**

---

### **1.7.1 Head of Security**

See SeMS manual Appendix 4

---

### **1.7.2 Other Personnel**

See chapter 5, Finnair Aviation Security Training Programme.

---

### **1.7.3 Subcontractors and Service Providers**

Nominated persons shall ensure that all subcontractors and relevant service providers have established security training programmes that are similar to that of Finnair and/or consistent with civil aviation programme of the State.

---

## **1.8 EXERCISING CARE AND AWARENESS**

All Finnair personnel, regardless of their duties, have an overall obligation to exercise care and awareness in security and safety matters concerning Finnair and aviation in general.

Security instructions shall be carefully followed and all discrepancies should be reported to supervisor, who shall forward this information, if necessary, to the Head of Security.

---

## **1.9 SECURITY EXERCISES**

Operational security exercises shall be performed to practice and evaluate the

- Effectiveness of procedures designed for response to security incidents,
- Implementation of security procedures by applicable personnel, and
- Usefulness and serviceability of security equipment.

The security exercises shall as a minimum be conducted annually. The exercises can be performed in conjunction with other Company exercises, e.g. emergency response exercises.



The Head of Security shall ensure the completion of the security exercises. Each exercise shall be evaluated and documented (exercise plan, evaluation, final report) to ensure continuous improvement.

## **1.10 SECURITY INCIDENT INVESTIGATIONS**

The Head of Security is responsible for initiating, oversight and completion of a security investigation.

Incidents involving:

- Threats or acts of unlawful interference, and
- Failure of implementation of security controls shall always be investigated.
- Insider Threat

The security investigation process shall follow the investigation process, as applicable, described in the Finnair Safety and Compliance Management Manual (SCMM) or investigation process described in SeMS manual Appendix 6.

The investigation can be completed in co-operation with the police or other relevant authorities.

An investigation report shall be completed as a result of the investigation.

## **2. STANDARD SECURITY PROCEDURES**

### **2.1 IDENTIFICATION CARDS AND VERIFICATION SYSTEMS**

ID cards are one of the basic elements with which the Company assures a satisfactory level of security in the aviation industry.

Identification verification systems shall be in place in aim to prevent personnel and vehicles from unauthorised access into to the airport airside areas and security restricted areas that are under the control of Finnair. Such identification system shall include designated checkpoints where identification is verified before access is permitted.

Personnel shall prominently display their ID card, issued by the airport authority or by Finnair (if applicable), at all times when on the airside or in other security restricted areas. Unauthorised use of ID cards is strictly forbidden. Local regulations must be followed carefully.

Finnair issues an ID-card for its personnel. Finnair ID cards, including crew ID cards shall as a minimum include name and photograph of the holder, company name, expiry date and word "crew" (for crew ID cards). The ID-card issuance process and other details related to ID-cards are described in the "Finnair ID-card"-Standard.

All operative Finnair employees, persons having access to sensitive aviation security information or critical systems and other personnel groups defined by Security Management will be subjected to a criminal background check or equal check defined by local authorities. This check will be renewed as a minimum every five years in conjunction with the renewal of the Finnair ID-card.

#### **2.1.1 Airside and Other Security Restricted Areas**

All personnel on airside or in other security restricted areas of airports are required to keep their ID cards visible. This shall apply also to vehicles as applicable and as requested, i.e. vehicles shall be equipped with a vehicle pass that allows entering the airside or security restricted area and this pass shall be kept visible when in such an area.

Persons without a visible ID-card shall be challenged to present their ID-card. If the person does not have an ID-card or is not willing to present it the matter shall be immediately referred to the airport security authority,

#### **2.1.2 Aircraft**

All personnel shall keep their ID visible when working on board a Finnair aircraft.

Finnair crew members performing duties on board a Finnair aircraft are not obliged to have their ID card visible during the flight.



## **2.1.3 Company Premises**

All persons working at or visiting any access controlled area of Finnair's or its subcontractor's premise (incl. cargo warehouses) shall always keep their ID-card or visitor card visible. Persons working permanently in Finnair offices shall be subject to a criminal background check. This check shall be renewed every five years as a minimum.

Persons without a visible ID-card or visitor card shall be challenged to present their ID-card or visitor card. If the person does not have an appropriate identification card or is not willing to present it the matter shall be immediately referred to the security function of the premise.

In such Company premises that have direct access to the security restricted area of the airport, security processes, access control procedures and security infrastructure shall follow the requirements set in the Airport Security Programme unless otherwise agreed with the airport operator.

---

## **2.2 SECURITY AT AIRPORTS**

### **2.2.1 Responsibility**

The security at airports is in general the responsibility of the local airport authority in co-operation with the security authorities. Finnair shall operate according to the general and local security procedures to ensure undisturbed operation at the airport.

If the security measures at an airport are the responsibility of the operating airlines, Finnair shall take care of its responsibilities in co-operation with appropriate sub-contractors.

---

### **2.2.2 Background Checks and ID cards**

Prior to receiving permission to perform duties on airside or in other security restricted areas, Finnair personnel and representatives shall be subject to a criminal background check or equivalent as permitted and required by local legislation. Such a background check shall be renewed as a minimum every five years.

---

### **2.2.3 Access Control and Guarding**

Access control and guarding at the airport or in the terminals are usually the responsibility of the airport or the terminal operators.

Finnair representatives at each station shall coordinate with airport authorities to ensure the existence of effective access control to restricted areas of the airport and other facilities so that only authorised personnel gain access to these areas. Prominent display of a security badge by personnel is essential.

If Finnair has been designated certain areas or premises at the airport (e.g. cargo warehouses) or in the terminal area, access control and guarding shall be conducted according to local legislation and Finnair security instructions to prevent unauthorised access to such areas.

---

### **2.2.4 Personnel Screening**

In aim to prevent the introduction of unauthorized weapons, explosives and other dangerous devices or items on board an aircraft by other persons than passengers personnel and their belongings entering the security restricted area shall be subject to security screening. Depending on the risk assessment and the requirements by the state of operations this screening can be on a random basis. Also, exemptions of the prohibited items are defined by local authorities.

At Helsinki-Vantaa airport Finnair operates following security check/screening points: Technical Area (Checkpoint 2), COOL Cargo Terminal, Hangar 11 and Kitchen. Detailed descriptions of checkpoints operating models and procedures are documented in separate "Checkpoint Procedures and Instructions"-documents. Each checkpoint has its own specific document.



## **2.2.5 Awareness**

Finnair personnel, especially at ticket sales, check-in and at boarding gates, shall be aware of security aspects concerning passengers and their baggage and verify their bona fides. If any doubts exist concerning passengers' identity, required travel documents or behaviour, the Finnair station supervisor and appropriate local authorities must be contacted to decide on the necessary actions.

Finnair personnel shall be on the alert for unaccompanied baggage or other suspicious articles in the passenger terminals or in their immediate vicinity. If such baggage or articles are discovered and the owner is not present or cannot be found immediately, the airport security authorities must be notified without delay.

Special attention should also be paid to passengers who purchase a one-way ticket with cash and the purchase, check-in, or boarding happens at the last moment.

---

## **2.3 PASSENGER AND CABIN BAGGAGE SECURITY**

### **2.3.1 Aim**

The aim of this chapter is to state the Finnair requirements for ensuring that

- (a) unauthorised persons do not board Finnair aircraft; and
- (b) prohibited articles are not taken on board a Finnair aircraft by flight crew or passengers either on their persons or in any item of carry-on baggage carried by them.

---

### **2.3.2 Objective**

The objective is to ensure that neither unauthorised persons nor prohibited articles or substances that may jeopardise the safety or security of a Finnair aircraft board or are taken on board.

---

### **2.3.3 Handling and Acceptance of Passengers and Carry-on Baggage**

Finnair passengers shall be handled and accepted only by Finnair or its handling agent. Passenger handling shall be conducted according to the Finnair Ground Operations Manual (GOM).

Finnair will only accept on board its flights persons who have appropriate travel documents, have no malicious intentions, and have been security screened.

---

### **2.3.4 Travel Documents**

#### **2.3.4.1 General**

Every passenger must have valid and authentic travel documents. These travel documents consist of acceptable flight tickets, a valid identification card and other documents needed by the passenger to reach his destination.

It is the responsibility of the ground personnel to check the validity and authenticity of necessary travel documents. This must be carried out with great accuracy, especially if the country of destination and/or transit has special requirements concerning arriving passengers.

If any doubts concerning the nature of the documents arise, they must be resolved before accepting the passenger on board a Finnair flight. The assistance of local authorities should be used if necessary.

If there is any suspicion that a passenger might destroy his travel documents during the flight, it is within the discretion of the station supervisor to decide whether the crew should hold the travel documents during the flight. This should be done only if it is in the interest of Finnair.



#### **2.3.4.2 Abuse of Visa Regulations**

The stations are advised to pay special attention to passengers trying to circumvent any visa regulations by purchasing an ostensible ticket with reservation to a third country. In reality these passengers have no intention of boarding the connecting flight regardless of their pretensions at the departure station. Usually the abusers are nationals of countries who would normally need a visa to enter the country of destination. In order to avoid the visa question, passengers book themselves via e.g. Helsinki to a destination where a visa is not required or is easy to obtain.

In addition to a potential security risk and financial loss due to non-used connecting flights, possible legal measures against Finnair by the authorities could be foreseen.

#### **2.3.4.3 Passenger Profiling in the Case of Suspicious Travel Documents**

To detect potential cases, passenger profiling has to be applied by Finnair representatives at check-in and gate. Observations and an interview may reveal whether the passenger may appear inadmissible or inadequately documented for the destination.

If there are several persons in the group to be profiled,

- passengers should be interviewed separately
- a closer examination of travel documents shall be made.

Also, the following matters below should be considered. Does the passenger

- appear unusually nervous or disoriented?
- have little or no baggage or empty baggage?
- have an unusual or illogical routing?
- have a one-way ticket?
- appear unsuitably attired or not at ease for the class of travel?
- arrive at the check-in or boarding gate at the last minute?
- resemble the nationality of the passport presented and speak the language of that country?
- have someone else checking him/her for the flight?

If some of the conditions mentioned are met and after an interview with the passenger some doubts still persist, boarding can be denied. Finnair station supervisor shall decide on denial.

#### **2.3.4.4 Reporting**

All attempts to board Finnair flights by fraudulent means shall be reported to Manager, Facilitation.

#### **2.3.5 Security at Check-in**

Check-in personnel shall be on the alert especially for the following security items and if doubt exists to communicate the issue with the passenger:

- baggage content and packing,
- prohibited articles in baggage, and
- prohibited dangerous goods.

Passengers shall be informed of prohibited items before completion of check-in. Information of prohibited articles shall be given at the check-in desks and baggage drop desks as well as when passengers check-in via other means (e.g. online, kiosk). At the check-in desks appropriate signage should be used. In online and kiosk check-in the information shall be clearly visible and easily accessible for the passenger.

The check-in personnel should also evaluate the bona fide of the passengers at check-in.



## **2.3.6 Screening**

### **2.3.6.1 General**

All departing passengers and their carry-on baggage must be screened according to local regulations prior to boarding Finnair flights.

No passenger shall proceed beyond the security screening point until all belongings, especially metallic articles, electronic items and restricted articles, are screened and shown not to pose a threat against air traffic and the safety and security of a flight (see Annex 1, List of Prohibited Articles).

### **2.3.6.2 Screening Procedures**

Passenger and carry-on baggage screening may be carried out manually or by using appropriate technical devices. Screening can take place at the departure gate or at the entrance to a security restricted area (i.e. an area with restricted access, where all passengers have been screened before entering).

Passengers or their belongings that cannot be checked with normal screening procedures (e.g. passenger with reduced mobility, ambulatory cases, etc.) must be subject to a manual search. Privacy should be assured when such a search is conducted.

Passengers who refuse screening or who cannot be satisfactorily screened shall be denied entrance to a security restricted area and not allowed to board an aircraft.

When carry-on baggage is screened by x-ray, a minimum of 10% of such baggage shall be subject to manual search. If local security authorities require a higher percentage, this shall be observed.

#### **2.3.6.2.1 Screening of cabin baggage**

Before screening, portable computers and other large electrical items shall be removed from 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.

The appropriate entity at all airports shall screen, upon entry to the security restricted area (SRA), at least LAGs obtained at an airport or on board an aircraft that are sealed in a STEB inside which is displayed satisfactory proof of purchase at airside at an airport or on board an aircraft, as well as LAGs to be used during the trip for medical purposes or a special dietary requirement, including baby food. Before screening, LAGs shall be removed from cabin baggage and shall be screened separately from other items of cabin baggage, unless the equipment used for the screening of cabin baggage is also capable of screening multiple closed LAGs containers inside baggage. Where LAGs have been removed from 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.

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

- (a) a hand search;
- (b) x-ray equipment;
- (c) explosive detection systems (EDS) equipment; or
- (d) explosive detection dogs in combination with point (a);
- (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.

A hand search of cabin baggage shall consist of a manual check of the baggage, including its contents, as to reasonably ensure that it does not contain prohibited articles.

Where x-ray or EDS equipment is used

- each image shall be viewed by the screener or analysed by auto clear software (ACS),



- all alarms shall be resolved to the satisfaction of the screener so as to reasonably ensure that no prohibited articles are carried into the SRA or on board an aircraft, and
- 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.

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.

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

Persons screening cabin baggage by x-ray or EDS equipment should normally not spend more than 20 minutes continuously reviewing images. After each of these periods, the screener should 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 should be a supervisor responsible for screeners of cabin baggage in order to assure optimum team composition, quality of work, training, support and appraisal.

#### **2.3.6.2.2 Screening of liquids, aerosols and gels (LAGs)**

LAGs carried by passengers may be exempted from screening with LEDS equipment upon entry to the airport 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; and
- (b) if the LAG is sealed in a dedicated STEB upon purchase locally at the airport airside.

The dedicated STEBs referred to under point (b) 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.

#### **2.3.6.3 Prohibited Articles**

Prohibited articles are objects which can be used to commit an act of unlawful interference and that have not been properly declared and subject to the applicable laws and regulations. An indicated list of such prohibited articles is found in Annex 1.

Prohibited articles that are allowed to be carried in a baggage hold can be transported as hold baggage. These articles should be placed in hold baggage or in a suitable container, which should be labelled and carried in the baggage hold and they shall not be accessible during flight. Articles that are or cannot be transported by air should be returned to an authorised person or disposed of according to local procedures.

Weapons discovered at security screening must always be reported to local security authorities.

#### **2.3.6.4 Security Restricted Area**

Originating passengers, including their carry-on baggage, who have been security screened shall be held in a security restricted area before boarding an aircraft.

Transit and transfer passengers should be held in the security restricted area after disembarkation. If this is not possible the passenger shall be screened as originating passengers prior to entering the security restricted area and boarding the aircraft. Precautions (e.g. surveillance of transit areas, arrival/departure areas) shall be in place in aim to ensure that transit and transfer passengers do not mix with unscreened passengers.

Transit and transfer passengers that arrive from such stations that have been determined as unsecure by the appropriate authority shall be screened before entering the security restricted area for departing passengers.

Passengers who exit the security restricted area must be subjected to security screening before re-entering the area.

If the passengers in the security restricted area have been contaminated by unauthorised and unscreened individuals who have entered the security restricted area the security restricted area and the passengers and their hand baggage shall be rescreened as determined by the local authorities and/or Head of Security (regarding passengers for Finnair flights).



### **2.3.6.5 Airline Responsibilities**

If local legislation requires airlines to conduct security screening of passengers and their carry-on baggage, Finnair will carry out this obligation by using subcontractors accepted by the local aviation authority. These subcontractors shall perform their duties according to local legislation and Finnair requirements, and the Finnair representative shall control their performance.

### **2.3.7 Passenger Headcount**

Cabin crew shall count the total number of passengers on board the aircraft prior to departure. The Commander shall compare this number to the number of checked-in and boarded passengers. Any discrepancies must be resolved by the CC (Chief of Cabin) and ground personnel in a manner acceptable to the Commander.

At **predetermined stations**, the cabin headcount procedure is not required. The station evaluation procedure related to this is described in Annex 3. The Area Manager, Ground Operations is responsible for completing the station evaluation and for monitoring the station for changes that could reflect the need to perform the headcount. The evaluation and changes shall be communicated to the Head of Security. The Head of Security is responsible for the approval for not to apply the headcount procedure. Such stations where the need for applying the headcount procedure does not exist shall be informed to all persons involved in an appropriate manner. However, a headcount shall always be made if the numbers of passengers checked-in and boarded differ, and this discrepancy cannot be resolved by ground personnel, or if requested by the Commander or ground personnel.

## **2.4 SPECIAL CATEGORY PASSENGERS**

### **2.4.1 Aim**

The aim of this chapter is to state the Finnair requirements for handling special category passengers carried on board its aircraft.

### **2.4.2 Objective**

The objective is to ensure that special category passengers on board aircraft are handled securely.

### **2.4.3 Exceptions from Mandatory Screening Requirements**

If approved by the local authorities the following persons may board an aircraft without screening:

- Head of State, Prime Minister, Minister of Foreign Affairs, the Speaker of the Finnish Parliament and their immediate family;
- Other dignitaries accepted by the appropriate authority and approved by the Head of Security or his deputy;
- a person under the escort of a law enforcement officer where the officer certifies that he has searched the person, his carry-on baggage and personal belongings;
- the escorting police officer; and
- a person authorised to carry a firearm on board a Finnair aircraft.

In any case the Head of Security or the Commander may require screening of any of the above mentioned persons.

### **2.4.4 Diplomatic and Consular Personnel**

Diplomatic and consular personnel and state couriers with their personal baggage are subject to the full range of security measures at the airport of embarkation, if this is not against local law.

Official diplomatic or consular bags shall not be searched. A diplomatic or consular bag is one that

- bears visible external marks identifying its character; and
- is in the possession of a diplomatic or consular courier who presents a valid passport and a certificate signed by an official of the sending state attesting to the courier's status.



## **2.4.5 Risk Category Passengers**

Finnair does not accept potential risk category passengers, i.e. deportees, inadmissible persons or persons in lawful custody to board an aircraft without special security measures.

### **2.4.5.1 Inadmissible Persons**

An inadmissible passenger is a passenger whose admission to a country has been refused by the authorities for reasons that contravene the country's immigration rules and regulations, e.g. not in possession of visa, invalid passport, passenger whose entry to the country is prohibited, etc.

### **2.4.5.2 Deportees**

A deportee (DEPA, accompanied by an escort or DEPU, unaccompanied) is a person who has entered a country either legally or illegally and who has been ordered by the authorities to be removed from that country for various reasons, e.g. discovery of illegal entry, conviction for a criminal offence, expired visa, etc.

### **2.4.5.3 Persons in Lawful Custody**

A person in lawful custody is e.g. a person under arrest, or a prisoner under escort.

### **2.4.5.4 Special Security Measures**

The following additional security measures shall be carried out:

- the competent authorities shall notify Finnair (see 2.4.5.5) in writing 48 (deportees and persons in lawful custody) hours prior to the embarkation of a risk passenger. In exceptional situations this 48 hours prior notification may be reduced to 2 hours;
- the Commander and CC must be notified before the departure;
- the person in question must be escorted if any doubts of disturbance exists;
- security screening of the person, his carry-on baggage and hold baggage by the appropriate authority;
- occupancy of aisle seats or seats next to the emergency exits is not allowed;
- no alcohol is served.

### **2.4.5.5 Notification**

Before an inadmissible person, a deportee or a person in lawful custody is accepted on the flight, the organisation responsible for transportation has to complete and sign the Finnair form 797-A-ADL. Forms containing similar information issued by the local authority can also be used.

The written notification shall contain the following details:

- identity and status of the passenger;
- available travel documents;
- routing and flight information;
- reason for transportation;
- risk assessment completed by the competent authorities;
- identity and status of escort(s), if provided;
- pre seating arrangements required;
- signature and stamp of authority.

The notification shall be sent to Finnair Contact Center (see 2.4.7.9 for contact information).

### **2.4.5.6 Information Procedures**

When the appropriate authority has made the decision to transport a potentially disruptive passenger on a flight, the information on the passenger status shall be entered in the passenger name record (PNR) when making the flight reservation. The flight reservation should be made no later than 48 hours prior to departure.



In addition, the authority responsible for the transportation shall send (by e-mail) a written notification addressed to Finnair Contact Center no later than 48 hours prior to departure. This notification shall be compared with the information in the passenger name record to avoid any discrepancies.

Finnair Contact Center shall forward the written notification to the Finnair representative at the departure station, to Crew Service Desk, and to the Head of Security. Crew Service Desk shall insert the basic information to CIS and maintain the written notification. The Commander of the flight may request the written notification from Crew Service Desk.

It is the responsibility of the Finnair representative at the station to ensure that the seating information of the passenger and escort is delivered to the Commander.

Under special circumstances, such as missing or miscommunication with the pre-notification, the Commander may accept such a passenger on board after consulting with the Head of Security or the escorts.

#### **2.4.5.7 Number of Risk Category Passengers**

The number of risk category passengers is limited to two per flight, unless there is a special permit from the Head of Security.

#### **2.4.5.8 Travel Documents**

The travel documents of a risk category passenger should be in the possession of the passenger himself or his escort.

### **2.4.6 Unruly Passengers**

#### **2.4.6.1 Ground Procedures**

Finnair representatives shall observe the behaviour and mental and physical condition of passengers during check-in and boarding. If any doubts exist concerning a passenger's ability to travel the passenger shall be subject to accurate profiling by the Finnair representatives. See OM-A, 23, Handling of Unruly Passenger.

If there exists reasonable doubt that the passenger may jeopardise the security or safety of the flight, the passenger shall be denied check-in or boarding (see also 2.5 Refusal of Carriage).

#### **2.4.6.2 In-flight Procedures**

See OM-A, 23., Handling of Unruly Passenger.

#### **2.4.6.3 Acts of Violence**

All acts of violence against Finnair personnel shall be immediately reported to the Finnair representative at the station, the Commander (if an incident occurs during the flight) and the police authorities for further action.

The Finnair representative or the Commander shall ensure that all necessary actions are taken to protect Finnair passengers, personnel and property against an unruly passenger.

A report using Passenger Disturbance Report – Ground, (Finnair form 253/1 NKL) shall be sent to the Head of Security.

### **2.4.7 Passenger Escort Procedures**

#### **2.4.7.1 General**

These instructions shall be complied with in the following situations:

- the risk assessment of the passenger and decision to use an escort has been completed by the authorities;
- the risk assessment of the passenger and decision to use an escort has been completed by Finnair. This may occur when Finnair is obliged to carry the passenger to comply with international and national legislation;
- the escorted passenger will be under neuroleptic or sedative medication during the flight.

Finnair may decide to require an escort regardless of the assessment and negative decision of the authorities. The Head of Security shall make this decision.

The Finnair Aviation Medical Director shall always be contacted if medical issues exist.



#### **2.4.7.2 Passengers Requiring an Escort**

Passengers who may require an escort are divided into three categories:

- deportees
- inadmissible persons
- persons under lawful custody.

Deportees or inadmissible persons will not be carried on a Finnair flight without an escort if any doubt of disruptive behaviour exists.

Persons under lawful custody must always be escorted.

#### **2.4.7.3 Escort**

##### **2.4.7.3.1 Escort Requirements**

In principal, two persons must be assigned for each escorted passenger. The escort shall primarily be a law enforcement officer.

Under special circumstances, where the risk is regarded as low, the escort does not necessarily have to be a law enforcement officer. Such an escort must have appropriate training for escort assignments. The Head of Security makes the assessment and decision to accept such an escort.

If the escorted passenger is under neuroleptic and sedative medication during the flight or the behaviour of the passenger indicates that medication may be required during the flight, he shall always be escorted by professional medical staff in addition to normal escorts.

The need for such an escort and their level of proficiency must be determined by Finnair Aviation Medical Director (HELOFM).

##### **2.4.7.3.2 Responsibility of the Escort**

The escort is responsible for the escorted passenger's behaviour and shall prevent the passenger from causing any disturbances.

##### **2.4.7.3.3 Equipment of the Escort**

The escort may have handcuffs in case of a passenger with violent behaviour.

Firearms, teargas, pepperspray, mace or other disabling devices containing an irritant or incapacitating substance and other disabling devices such as electronic stunning and shock devices are prohibited.

#### **2.4.7.4 Evaluation and Decision regarding an Escort Completed by Authorities**

An appropriate and competent officer within the authority shall make the evaluation and the decision.

##### **2.4.7.4.1 Acceptance of Passenger and Escort**

Finnair will accept the passenger and escort to board the aircraft if the requirements in these instructions are fulfilled.

##### **2.4.7.4.2 Information Procedures**

When the appropriate authority has made the decision to escort a person on a flight, the information on the passenger status and escorts shall be entered in the passenger name record (PNR) when making the flight reservation. The flight reservation should be made no later than 48 hours prior to departure.

In addition, the authority responsible for the escorted person shall send (by e-mail) a written notification addressed to Finnair Contact Center no later than 24 hours prior to departure. This notification shall be compared with the information in the passenger name record to avoid any discrepancies.

Finnair Contact Center shall forward the written notification to the Finnair representative at the departure station, to Crew Service Desk, and to the Head of Security. Crew Service Desk shall insert the basic information to CIS and maintain the written notification. The Commander of the flight may request the written notification from Crew Service Desk.



It is the responsibility of the Finnair representative at the station to ensure that the seating information of the passenger and escort is delivered to the Commander.

Under special circumstances, such as missing or miscommunication with the pre-notification, the Commander may accept such a passenger on board after consulting with the Head of Security or the escorts.

#### **2.4.7.4.3 Written Notification**

See 2.4.5.5.

#### **2.4.7.5 Evaluation and Decision on an Escort Completed by Finnair**

Finnair is obliged under certain circumstances to carry passengers who may require an escort.

It is within the responsibility of the Head of Security to determine the necessity of an escort. Co-operation with the Aviation Medical Director is recommended if any doubt about the passenger's physical or mental condition exists.

##### **2.4.7.5.1 Acceptance of the Passenger and Escort**

The passenger and escort can be accepted to board the aircraft if the requirements in these instructions are fulfilled.

##### **2.4.7.5.2 Information Procedures**

The Head of Security informs Finnair Contact Center of the necessary travel information and the status of the passenger and escort. Finnair Contact Center shall make the reservation in the reservation system.

##### **2.4.7.5.3 Written Notification**

The Head of Security shall complete the written notification (see 2.4.5.5).

#### **2.4.7.6 An Escorted Passenger under Medication during The Flight**

If an escorted passenger is to be under medication during the flight, it is within the responsibility of the Head of Security to make the evaluation and decision regarding transportation.

The Finnair Aviation Medical Director shall always be informed and asked for an evaluation.

##### **2.4.7.6.1 Acceptance of the Passenger and Escort**

The passenger and escort can be accepted to board the aircraft if the requirements in these instructions are fulfilled.

##### **2.4.7.6.2 Information Procedures**

The medical information concerning a passenger who may be under medication during the flight shall be sent to the Aviation Medical Director 48 hours prior to departure.

The Aviation Medical Director shall evaluate the information regarding the passenger and his medication and inform the Head of Security.

If the passenger is accepted the requesting authority shall be informed, after which the information procedure will be according to 2.4.7.4.

##### **2.4.7.6.3 Special Notification**

An escort for a passenger who may be under medication during the flight must be provided with a special notification that includes the following items:

- the identity of the passenger
- a detailed description of the medication.

The authority of origin shall provide this special notification.

#### **2.4.7.7 Handling of Travel Documents**

The travel documents of the escorted passenger shall always be in the possession of the escort.



## **2.4.7.8 Additional Security Measures**

### **2.4.7.8.1 Prior to Departure**

The following additional security measures are mandatory when transporting an escorted passenger:

- security screening of the passenger and his/her hand and hold baggage;
- no occupancy of aisle seats or seats next to the emergency exits;
- boarding prior to other passengers.

### **2.4.7.8.2 During the Flight**

The following additional security measures are mandatory during the flight:

- no occupancy of aisle seats or seats next to the emergency exits;
- no service of alcoholic beverages to the escorted passenger or escort.

Special attention shall be paid to the needs of the escorts and assistance shall be offered if required.

### **2.4.7.8.3 Restraining the Escorted Passenger**

If the passenger's behaviour is violent and may affect the safety or security of the aircraft, crew or passengers, the escort shall consider restraining the passenger.

The Commander may order the passenger to be restrained. If the passenger has been restrained during the flight he shall not be released before arrival.

## **2.4.7.9 Contact Numbers**

<b>ORGANISATION:</b>	<b>Tel numbers</b>	<b>Fax</b>
Finnair Contact Center	+358 9 818 31603	+358 9 818 31564
Crew Service Desk	+358 9 818 5250	+358 9 8185239
Customer Team Lead, HEL	+35850 315 3890	
Head of Security	+358 9 818 4125 +358 405589405 (mobile)	
Manager, Facilitation	+358 9 818 8843 +358 40 754 5003 (mobile)	
Aviation Medical Director	+358 9 818 4845 +358 405569459 (mobile)	+358 9 8184825

## **2.5 REFUSAL OF CARRIAGE**

Finnair has the right to refuse carriage of any passenger or passenger's baggage for reasons of safety or security, at the company's discretion, if:

- such action is necessary to comply with any applicable laws, regulations, or orders of any state or country to be flown from, to or over;
- the conduct, age or mental or physical state of the passenger is such as to require special assistance from Finnair, cause discomfort or make himself objectionable to other passengers, or involve any hazard or risk to himself, to other persons or to property;
- such action is necessary because the passenger has failed to observe the instructions of Finnair;
- the passenger has refused to submit to a security check;
- the applicable fare or any charges or taxes payable have not been paid, or credit arrangements between Finnair and the passenger (or the person paying for the ticket) have not been complied with;



- the passenger does not appear to be properly documented;
- the passenger may seek to enter a country through which he is in transit;
- the passenger may destroy his documentation during the flight;
- the passenger will not surrender travel documents to be held by the flight crew, against receipt, when so requested by Finnair;
- the ticket presented by the passenger has been unlawfully acquired or has been purchased from an office other than Finnair or its authorised agent, has been reported lost or stolen, is a counterfeit ticket, or a flight coupon has been altered by someone other than Finnair or its authorised agent, or has been mutilated, and Finnair reserves the right to retain such a ticket;
- the person presenting the ticket cannot prove that he is the person named in the "Name of Passenger" box, and the carrier reserves the right to retain such a ticket.

The Finnair representative or the Commander shall make the refusal decision regarding transportation on the departing or transfer flight. The Head of Security shall make the evaluation and decision to deny future transportation (e.g. return flight) of unruly passengers. This evaluation shall be based on the reports received from the station and/or in-flight reports.

---

## **2.6 SECURITY OF HOLD BAGGAGE**

---

### **2.6.1 Aim**

The aim of this section is to state the Finnair requirements for ensuring that no prohibited articles are taken on board an aircraft in any piece of hold baggage.

---

### **2.6.2 Objective**

The objective is to ensure that hold baggage taken on board an aircraft does not contain any prohibited article or substance that may jeopardise the safety of the aircraft, its passenger or crew.

---

### **2.6.3 Handling of Baggage**

Only authorised Finnair representatives shall carry out baggage handling. Instructions in GOM must be observed.

Access to airport baggage sorting areas shall be restricted to authorised personnel only.

---

### **2.6.4 Acceptance of Baggage**

Finnair will accept baggage to be checked-in only when:

- the passenger is ticketed for the intended flight(s);
- the baggage has been tendered by the passenger, the escorting police officer or the airport security staff;
- it is properly marked externally to enable identification with the respective passenger;
- local security authorities have screened the baggage if the passenger has answered negatively to one or more of the questions (see 2.6.5)

Passengers shall be informed of prohibited items before completion of check-in. Information of prohibited articles shall be given at the check-in desks or baggage drop desks as well as when passenger checking-in via other means (e.g. online, kiosk). At the check-in desks appropriate signage should be used. In online and kiosk check-in the information shall be clearly visible and easily accessible for the passenger.

---

### **2.6.5 Passenger Security Questioning**

The use of passenger security questioning as a company procedure is within the discretion of the Head of Security, unless it is mandatory by local legislation. If the decision is made to use passenger security questioning this shall be informed to the relevant departments by the Head of Security.



---

When the decision has been made to use passenger security questioning following procedures apply:

The passenger shall be asked the following questions, either orally or in writing, at the check-in desk:

1. Do you have only your personal baggage with you?
2. Did you pack the baggage yourself?
3. Are you sure nothing has been put in to your baggage since you packed it?
4. Do you know the contents of the gift parcels in your baggage?

Other questions approved by local authorities may be used instead of the questions above.

If the passenger answers negatively to one or more of the questions mentioned above, his baggage must be subject to screening.

---

## **2.6.6 Transportation of Baggage**

On Finnair flights it is permitted to transport hold baggage which belongs

- to the passengers or the crew on board the aircraft (accompanied baggage);
- to a passenger not on board the aircraft where, for reasons beyond the control of the passenger, the baggage has been misdirected or delayed, provided that the baggage has been subjected to other security controls (unaccompanied baggage).

All hold baggage that has been accepted on a flight shall be recorded (e.g. manually or through a BRS-system) and transportation shall be authorised by the Finnair representative.

---

## **2.6.7 Screening of Hold Baggage**

All hold baggage, including courier shipments checked in as baggage, shall be screened before loading on board a Finnair flight (both on international and domestic flights).

To prevent the transportation of explosives and other prohibited articles in hold baggage, Finnair accepts the use of the screening methods as stated in 2.6.7.2 and 2.6.7.3.

### **2.6.7.1 Transfer Baggage**

If the baggage has been screened at the point of origin and protected from unauthorized interference from the point of screening at the originating airport to the departing aircraft at the transfer airport this baggage does not need to be rescreened at the transfer airport (see exception below).

When the baggage arrives to an EU-airport from an EU Member State, Iceland, Norway, Switzerland or a country that has been accepted by the EU Commission the transfer baggage does not have to be security screened at the transfer airport. Baggage arriving from any other country than an EU Member State, Iceland, Norway, Switzerland or such country that has been accepted by the EU Commission shall be subjected to security screening before loading on board the connecting flight.

### **2.6.7.2 Accompanied Hold Baggage**

All items of accompanied hold baggage shall be screened by one of the following methods before being loaded onto an aircraft:

- Hand search; or
- Conventional x-ray with at least 10% of screened baggage being subjected to either:
  - Hand search; or
  - EDS or EDDS or PEDS
  - Conventional x-ray equipment with each bag being viewed from two different angles by the same operator at the same screening point; or
- Conventional x-ray with TIP installed and employed; or
- EDS or EDDS; or



- PEDS; or
- Trace Detection Equipment on open pieces of baggage.

#### **2.6.7.3 Unaccompanied Hold Baggage**

All items of unaccompanied baggage shall be screened by one of the following methods, before being loaded onto an aircraft:

- Level 2 EDS; or
- Conventional x-ray equipment with each bag being viewed from two different angles by the same operator at the same screening point; or
- Hand search supplemented by the application of Trace Detection Equipment on open pieces of baggage,

unless the unaccompanied baggage, which has been previously screened to Level 3 EDS, the security screener re-inspects the images and Finnair representative has completed an appropriate risk assessment, has been separated due to factors beyond passenger's control, and the unaccompanied baggage has been within the care of Finnair. The result of the risk assessment shall be documented.

Accompanied hold baggage that has become unaccompanied need not to be re-screened before carriage provided that:

- the baggage has already been screened in accordance with the National Civil Aviation Security Programme to the standards for accompanied baggage; **and**
- the baggage and the passenger were separated in the following circumstances and could not have been contrived by the passenger or an accomplice:
  - the passenger has been denied boarding to an overbooked flight by Finnair. This shall not apply when passenger volunteers to give up their seat.
  - the passenger was rerouted onto another flight solely by Finnair and not at the passengers request
  - the baggage was delayed in transfer between two flights due to unforeseen reasons and missed the departure flight
  - there was a breakdown of the baggage system causing the baggage to be delayed and miss the departure flight
  - the baggage was loaded on the wrong aircraft by Finnair or ground handling agent.

in addition, it shall be established that the passenger did travel on the flight on which they were checked in unless the circumstances detailed in the above round bullet points 1 and 2 apply.

---

#### **2.6.8 Protection of Hold Baggage**

Hold baggage to be carried on an aircraft, shall be protected from unauthorised interference from the point at which it is accepted into the care of Finnair until departure of the aircraft on which it is to be carried. The following measures shall be taken in protecting hold baggage:

- 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 authorised persons may have access.
- Any person entering a baggage make-up or storage area without authorisation shall be challenged and escorted out of the area.
- Originating and transfer hold baggage shall not be left unattended on the ramp or aircraft side prior to being loaded on the aircraft.
- Tail-to-tail transfer hold baggage shall not be left unattended on the ramp or aircraft side prior to being loaded.
- secure areas shall be established for mishandled baggage. The mishandled baggage shall be kept in such area until forwarded, claimed or disposed.

Access to lost-and-found offices in the terminal shall be restricted authorised persons only in aim to prevent unlawful access to baggage and materials.

When the hold baggage is located in the critical parts of the security restricted area it is considered to be adequately protected and no additional security measures are needed.



---

## **2.7 PASSENGER AND BAGGAGE RECONCILIATION**

---

### **2.7.1 Aim**

The aim of this section is to state the Finnair requirements for ensuring that no such baggage is carried on board a Finnair aircraft where the passenger with hold baggage does not board the flight

### **2.7.2 Objective**

The objective is to ensure that reconciliation procedures are completed prior to the departure of a flight.

### **2.7.3 Reconciliation Procedures**

A passenger/baggage reconciliation procedure shall be established at each Finnair station for each flight. This procedure applies to all flights as well as to originating, transit and transfer passengers.

Hold baggage shall not be placed on board an aircraft unless the following measures are taken:

- Hold baggage shall be properly marked externally to permit identification with relevant passengers; and
- The passenger to whom such baggage belongs shall be checked in and boarded for the flight on which it is to be carried; and
- Prior to loading, hold baggage shall be held in an area of the airport to which only authorised persons have access; and
- All items of baggage taken into the custody of Finnair for carriage in the hold of an aircraft shall be identified either as accompanied or unaccompanied.

This procedure is to ensure that the baggage belonging to passengers who are not on board the aircraft will not be transported unless it has been security screened or subjected to other security control and found to be acceptable for transportation.

A hold baggage manifest or an alternative means of providing evidence which confirms the identification and screening of unaccompanied hold baggage shall be drawn up.

The reconciliation shall be completed before the departure of the flight.

---

### **2.7.4 Accepted Procedures**

The following reconciliation procedures are acceptable:

- Semiautomatic, fully automated or manual passenger and baggage reconciliation systems;
- a physical identification by the departing passengers of their hold baggage before boarding the aircraft; or
- a comparison of the number of baggage counted on flight coupons with the number of counted pieces of hold baggage loaded on board the flight.

---

### **2.7.5 Baggage Count**

The number of checked-in pieces of baggage loaded on an aircraft must be counted and compared with the number of baggage checked-in. If any discrepancies occur the reasons for this must be determined. The Commander shall always be informed.

When an automated baggage reconciliation system (BRS) is used and each piece of baggage for a flight is reconciled, it is not necessary to count the number of baggage manually.

---

### **2.7.6 Unloading of Baggage**

If a passenger checked in for a flight, who has placed baggage in the custody of the air carrier, is not on board the aircraft, such hold baggage shall be removed from the aircraft and shall not be carried on that flight.



When passengers checked in and boarded match, but the number of hold baggage loaded on the aircraft exceeds the number of pieces checked-in for that flight, discrepancies must be resolved before departure.

When a baggage has been removed from the flight, and the intention is to transport it with another flight, it shall be processed according to 2.6.7.3 before acceptance for the new flight.

Baggage related additional guidance (OM-A 10.1.6)

If a passenger with baggage has checked in but does not board the aircraft, the Commander shall be informed. As general guideline, it is mandatory to remove the baggage from the aircraft before departure. However, the commander can, at his own discretion, decide not to remove the baggage when the following applies:

- the departure station is in the EU, UK, Norway, Switzerland or Iceland, and
  - (a) The passenger and/or his luggage was transferred to another flight for a reason other than his own request; or,
  - (b) Finnair decides not to unload the baggage for operational reasons and the passenger has not influenced that decision by changing his flight. The commander should contact ground handling company for more information about the missing passenger to support his decision.

## **2.7.7 Baggage Identification**

Physical baggage identification must be carried out if

- there is no other way to identify the baggage of a passenger who checked in but did not board the aircraft;
- the comparison of the number of checked-in pieces of baggage does not give a reliable result and the passenger and baggage reconciliation is based only on that comparison; and
- the commander decides that it is necessary for the security of the flight.

## **2.8 OFF-AIRPORT CHECK-IN**

### **2.8.1 Acceptance and Approval**

Off-airport check-in is accepted for Finnair flights when the arrangements fulfil the same level of security and the same security procedures are carried out as at airports.

The local authorities must approve off-airport check-in procedures and any additional security measures required by these authorities must be complied with. The approval of the Head of Security is also required before implementing off-airport check-in services.

### **2.8.2 Off-airport Security Procedures**

Finnair requires the following security measures to be followed in regard of off-airport check-in for Finnair flights:

- The Head of Security shall approve each off-airport check-in location;
- Personnel performing the check-in must be qualified for the duties
- normal computerised check-in facilities must be available, unless otherwise approved by the Head of Security;
- baggage and boarding passes must be marked with off-airport tags/stickers;
- hold baggage must be stored in facilities accessible only to authorised persons;
- hold baggage shall be transported to the airport separately from other baggage and in a vehicle or vehicle lockers loaded and sealed by authorised personnel;
- at the airport the hold baggage must be handed over to authorised personnel by the driver;
- An airline representative shall check the seals of the vehicle lockers before opening. If the seal is incorrect or has been tampered with, the hold baggage must be subject to security screening;



---

## **2.9 AIRCRAFT SECURITY**

---

### **2.9.1 Aim**

The aim of this section is to state the Finnair requirements for searching, checking and controlling access to Finnair aircraft at airports.

### **2.9.2 Objective**

The objective is to ensure that there are no prohibited articles or unauthorised persons on any Finnair flight.

### **2.9.3 Protection of Aircraft**

Finnair aircraft, while parked in ramp, maintenance or other parking areas, shall always be under the control of Finnair or its representatives. Responsibilities are as follows:

- HEL: Technical Operations and / or Ground Operations
- other stations:
  - schedule and charter destinations:
    - Handling agent
    - Crew (turnaround flight)
  - ad-hoc destinations:
    - Handling agent, or
    - aircraft crew if no handling agent is available

Access to Finnair aircraft is restricted to authorised persons. Authorised persons can be considered persons who have a valid ID card (or other permits granted by airport or local authority) that authorises them to be in the aircraft and who have duties to be performed in the area. Finnair personnel must be alert to prevent unauthorised access to an aircraft. To ensure this, security guarding may be used if the security level at an airport so requires.

Authorised personnel shall remove unauthorised persons from the aircraft and this shall be reported to the Head of Security and to local security authorities.

Regardless of where an aircraft is parked at an airport, it shall be protected against unauthorised access by:

- ensuring that persons seeking to gain unauthorised access are challenged promptly; or
- having its external doors closed. Where the aircraft is in a critical part, external doors that are not accessible 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; or
- having electronic means which will immediately detect unauthorised access.

The above mentioned protective procedures shall not apply to an aircraft parked in a hangar that is locked or otherwise protected from unauthorised access.

#### **2.9.3.1 Aircraft in Critical Parts of the Security Restricted Area**

No additional protection measures apply. See 2.9.3 for basic protection measures.

#### **2.9.3.2 Aircraft in other than Critical Parts**

Where external doors have been closed and the aircraft is in a part other than a critical part, each external door shall also:

- Have access aids removed (this shall not apply for a door that is accessible from the ground); or
- Be sealed; or
- Be locked; or
- Be monitored.



Where access aids are removed for doors that are not accessible from the ground, they shall be placed sufficiently far from the aircraft as to reasonably prevent access.

Where external doors are locked, only persons with an operational need shall be able to unlock these doors.

Where external doors are monitored, the monitoring shall ensure that unauthorised access to the aircraft is immediately detected.

#### **2.9.3.3 Crew**

The Commander and CC are responsible for monitoring access into the aircraft when it is manned.

Crew members must check that all persons (excluding passengers) entering the aircraft have a visible ID card and duties to be performed in the aircraft.

#### **2.9.3.4 Ground Personnel**

Ground personnel shall monitor and control access to the aircraft when working at the aircraft.

### **2.9.4 Aircraft Security Sealing**

The aircraft shall be sealed with special security seals when considered necessary. The necessity of sealing is determined by the Head of Security. Local authorities may also request aircraft sealing. Detailed sealing procedures and instructions are described in GOM and Operations Manual, Part A.

Where security seals are used:

- They shall be tamper-evident; individually numbered and controlled;
- Seal numbers shall be recorded and kept at the station for 24 hours or the duration of the flight, whichever is longer;
- Prior to entering an aircraft into service, the seals on that aircraft shall be inspected for signs of tampering. If tampering is detected or suspected, an aircraft security search shall be conducted prior to entering the aircraft into service.
- They shall be protected from unauthorised access and distributed in a controlled way

### **2.9.5 AIRCRAFT SECURITY SEARCH**

An aircraft security search shall be conducted as follows:

- Aircraft interior (e.g. flight deck and cabin) the crew or other personnel with appropriate training,
- Aircraft exterior (excluding cargo holds): flight crew as part of pre-flight inspection,
- Cargo holds: ground handling or other personnel with an appropriate training.
- Where no ground handling or other personnel with appropriate training is available the Commander is responsible for ensuring that also aircraft holds are searched..

Airport security authorities should be requested to inspect and remove any suspicious articles.

Left-behind belongings shall be delivered to the Finnair ground personnel or to other company representatives to be forwarded to the lost and found office.

All Finnair aircraft shall be searched as follows, unless more stringent measures are required. Such requirement will be informed by the Head of Security.

The aircraft is exempted from the aircraft security search if it arrives to the airport critical parts from an EU member state or from a state appearing in Attachment 3-B of Regulation (EU) No 2015/1998.

If the aircraft arrives to, or departs from, another than critical part, it shall be subjected to an aircraft security search. An aircraft security search shall also be conducted when an aircraft is moved to the critical part from other parts of the airport.



An aircraft in transit may be exempted from an aircraft security search. If it arrives from a third country not listed in Attachment 3-B of Regulation (EU) No 2015/1998 and one or more passengers disembark the aircraft then the following shall be undertaken:

- reconciliation of the remaining passengers and baggage, and
- verification that no articles were left in overhead bins and seat pockets by the disembarking passengers

Security search shall always be done if there is a reason to suspect unauthorised persons may have accessed the aircraft.

Finnair crew or other designated person/entity approved by the Head of Security is responsible for conducting the aircraft security search.

The search shall be made by hand. Such areas that are empty can be searched visually.

All-Cargo flights may be exempted from the cabin security search at out stations, since cabin is either sealed or under supervision of Finnair during turnaround.

#### **2.9.5.1 Aircraft Security Search Areas**

An aircraft security search shall include examination of the following accessible areas in the interior of the aircraft:

- Overhead bins,
- Closets,
- Lavatories,
- Galleys,
- Storage bins,
- Seat backs and seat pockets,
- Areas under seat, between seats and between seats and walls,
- The cockpit if unattended,
- Crew equipment bins and compartments,
- Other compartments in the passenger cabin and flight deck,
- Aircraft service panels,
- Wheel wells,
- Service compartments,
- Hold and adjacent areas,
- Stores contained within the cargo compartments,
- Minimum 5% of the lifevest pouches.

#### **2.9.5.2 Record keeping**

Upon completion of an aircraft security search, a record shall be kept for 24 hours or the duration of the flight, whichever is longer. The record shall contain the following information:

- Flight number,
- Departure station of previous flight,

When the aircraft security search is completed by several parties the information of the completed search shall always be made known to Pilots. Completed cabin security search shall be notified to Pilots by the SCC. The completed security search of holds is indicated in the Loading Instruction Report (LIR) signed by the loading supervisor.

If the aircraft security search has been completed, also following information shall be contained in the record;

- Date and time of the aircraft security search,
- Name and signature of the Commander.

An aircraft security search may be conducted on an aircraft in service during turn-around or during a transit stop whilst service providers are on-board the aircraft, provided that the service providers and their items carried have been screened according to local requirements and are under supervision of Finnair personnel or its representatives.



## **2.9.6 Protection of Flight Deck**

All Finnair aircraft with a maximum certificated takeoff mass in excess of 45,500 kg or with a seating capacity greater than 60 passengers are equipped with an approved flight deck door that is: i) capable of being locked and unlocked from either pilot station, ii) designed to resist penetration by small arms fire, grenade shrapnel or forcible intrusions by unauthorized persons.

## **2.10 CARGO SECURITY**

### **2.10.1 Aim**

The aim of this section is to state the Finnair requirements for ensuring that no prohibited article is taken on board an aircraft in any piece of cargo or mail.

### **2.10.2 Objective**

The objective is to ensure that cargo and mail taken on board an aircraft does not contain any prohibited article.

These instructions shall be followed as a minimum. Outside the EU-area the local legislation may differ or set additional requirements. In case of conflict with local legislation acceptable procedures shall be agreed with Head of Security. Finnair Cargo's security-function is part of the Finnair Group security governance and management model and provides expertise in all cargo security related issue (e.g. airline, terminal operations).

Detailed description of Finnair Cargo Cool terminal can be found from specific Cargo Cool terminal Security program approved by Traficom.

### **2.10.3 Security Controls**

All cargo and mail shall be screened or subjected to other security controls prior to being loaded on an aircraft. Transit cargo and transit mail may be exempted from security controls if it remains on board the aircraft.

Cargo and mail to be loaded on an aircraft shall be screened, unless:

- (a) security controls have been applied to consignment by a regulated agent and the consignment has been protected from unauthorised interference from the time that those security controls were applied; or
- (b) security controls have been applied to the consignment by a known consignor and the consignment has been protected from unauthorised interference from the time that those security controls were applied; or
- (c) security controls have been applied to the consignment by an account consignor, the consignment has been protected from unauthorised interference from the time that those security controls were applied, and the cargo is carried on all-cargo aircraft or the mail on all-mail aircraft;
- (d) security controls have been applied to transfer cargo and transfer mail as referred in 2.10.9.

All cargo and mail shall be screened by a regulated agent before being loaded on to an aircraft, unless:

- (a) the required security controls have been applied to the consignment by a regulated agent and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or
- (b) the required security controls have been applied to the consignment by a known consignor and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or
- (c) the required security controls have been applied to the consignment by an account consignor and the consignment has been protected from unauthorised interference from the time that those security controls were applied and until loading; or
- (d) the consignment is exempted from screening and has been protected from unauthorised interference from the time the it became identifiable air cargo or identifiable air mail and until loading.



Where there is any reason to believe that a consignment to which security controls have been applied has been tampered with or has not been protected from unauthorised interference from the time that those controls were applied, it shall be screened by a regulated agent before being loaded on to an aircraft.

A person with unescorted access to identifiable air cargo or identifiable air mail to which the required security controls have been applied shall have successfully completed either a background check or a pre-employment check.

If the required security controls have not been applied to the consignment of cargo or mail, it shall always be screened before being loaded on to an aircraft.

#### **2.10.4 Approval of Regulated Agents**

Regulated agents shall be approved by the appropriate authority. The approval as a regulated agent is site specific.

All actors participating in the controlled logistics chain must be regulated agents or under their supervision. In case an undertaking that handles or transports known cargo is not a regulated agent or a subcontractor to a regulated agent, known consignor or account consignor, the cargo delivered by that undertaking shall be screened.

A subcontractor who works in the regulated agent's premises and carries out e.g. security screening under its supervision is not required to be a regulated agent. The regulated agent is responsible for its subcontractors.

The haulier shall give a haulier declaration to the regulated agent, known consignor or account consignor for whom it works, and on request also to that regulated agent to whom the consignment is delivered.

Finnair Cargo is a regulated agent.

#### **2.10.5 Acceptance of Cargo**

Finnair accepts for transportation only cargo and mail received from a regulated agent and that have been subjected to appropriate security controls.

#### **2.10.6 Security Controls by Regulated Agents**

Air cargo shall always be security screened before loading on board an aircraft, unless it has been ascertained during reception that the consignment has arrived from or has been collected either:

- (a) from a regulated agent and the sender is a known consignor or security measures are performed by regulated agent;
- (b) directly from a known consignor; or
- (c) directly from an account consignor

and that the consignment has been protected from unauthorised interference during transport.

Where there is reason to suspect that a consignment has been tampered with, it shall always be screened.

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" 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.

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.

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.

When accepting a consignment, the regulated agent shall verify the status of the sender company from CAA website or in the EC database. If the consignment has been sent by a regulated agent listed in the database and the air waybill shows a security status, the consignment need not to be screened but it must be protected.

If the regulated agent accepts the security status issued by the previous regulated agent, it shall add its own identification number on the document before handing it over to the next regulated agent or Finnair.



The person delivering the consignments to the regulated agent or Finnair shall present his or her identity card, passport, driving license 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.

When accepting consignments to which not all required security controls have previously been applied, the regulated agent shall ensure that they are appropriately screened and accompanied with an appropriate document showing security status before being loaded on to an aircraft.

After security controls have been applied, the regulated agent shall ensure that:

- (a) access to these consignments is controlled; and
- (b) these consignments are protected from unauthorised interference until they are handed over to another regulated agent or Finnair.

After the security controls have been applied, the regulated agent shall ensure that any consignment tendered to Finnair or another regulated agent is accompanied by appropriate documentation, either in the form of an airway bill or in a separate declaration and either in an electronic format or in writing.

The documentation shall be available for inspection by the appropriate authority at any point before the consignment is loaded on to an aircraft and shall provide the following information:

- (a) the site specific name and address of the regulated agent that issued the security status and/or its unique alphanumeric identifier as received from the appropriate authority;
- (b) a unique identifier of the consignment, such as the number of the (house or master) air waybill;
- (c) the content of the consignment;
- (d) the security status of the consignment, stating "SPX" or "SCO";
- (e) the reason that the security status was issued, stating "KC", "AC", the means of method of screening used or the grounds for exempting the consignment from screening;
- (f) the name of the person who issued the security status, or an equivalent identification, and the date and time of issue;
- (g) the site specific name and address, or unique identifier received from the appropriate authority, of any regulated agent who has accepted the security status given to a consignment by another regulated agent.

In the case of consolidations, the requirements c), e), f) and g) as stated above will be considered as met, if the regulated agent is able to establish the nature of the contents, the reason that the security status was issued and/or the name of the person who issued the security status and the date and time of issue, respectively, by a verifiable audit trail at any time before the consignment is loaded on an aircraft and afterwards for the duration of the flight or for 24 hours, whichever is the longer.

When accepting consignments to which not all required security controls have previously been applied, the regulated agent may also elect not to apply the security controls, but to hand the consignments over to another regulated agent to ensure the application of these security controls.

When accepting a consignment from a known consignor or account consignor, the regulated agent shall verify the status of the delivering company, or the company from which the consignment is collected, in the EC database. If the known consignor is not yet listed in the database, the status can be verified in the company's own list of known consignors. The identity of the person delivering the consignment must be established e.g. from his/her driving license.

Every cargo consignment to be loaded on to an aircraft shall be accompanied with a document providing the information required below. Such a document can be an air waybill, MAWB or HAWB, or a separate attachment containing the required information. This document can be either in physical or digital form.

## **2.10.7 Marking the Security Status**

An SPX or SCO marking may only be made after the regulated agent has ascertained that the consignment has securely passed from the known consignor or account consignor through the entire controlled logistics chain, or has been security screened. If the marking is made before the consignment is handed over to the air carrier, the regulated agent shall monitor the consignment until the moment when it is handed over and make sure that no irregularities occur. In case any irregularity is detected, the security marking shall be made void by striking it through and the consignment shall be subjected to screening. After screening a new marking shall be made.

Consolidated cargo can only be made up of consignments with the same security status (SPX/SCO).



The markings must show:

- The unique identifier for the regulated agent as issued by the appropriate authority, i.e. the regulated agent's approval number, which can be found in the EC database or, before the database is brought into service, on CAA Finland's web-site.
- The unique transaction identifier of the consignment, e.g. the air waybill number.
- The content of the consignment, which means its trade name. In case of a consolidated consignment, where the contents are marked e.g. only as "consolidated cargo" in the main waybill, a manifest indicating the content of each individual consignment shall be attached to the main waybill. The manifest can also be sent to the receiver as an electronic file.
- The security status of the consignment, SPX or SCO.
- Justification for the assignment of security status: KC if the consignment was received from a known consignor or AC if the consignment was received from an account consignor.
- If the security status is issued on the basis of screening, the screening method or procedure shall be indicated: hand search, visual check, x-ray, EDS, dogs, ETD or simulation chamber, or "combination of".
- If the consignment has been exempted from security screening on other grounds, the reason for the exemption shall be indicated.

## **2.10.8 Security Screening**

When screening cargo or mail:

- (a) the means or method most likely to detect prohibited articles shall be employed, taking into consideration the nature of the consignment; and
- (b) the means or method employed shall be of a standard sufficient to reasonably ensure that no prohibited articles are concealed in the consignment.

Where the screener cannot be reasonably sure that no prohibited articles are contained in the consignment, the consignment shall be rejected or be rescreened to his satisfaction.

To be able to determine the most appropriate method, the person who carries out the screening or the person who decides which screening method is used shall have a document showing the content of the consignment at his/her disposal.

### **2.10.8.1 Methods of Screening**

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

- (a) hand search;
- (b) visual check
- (c) x-ray equipment;
- (d) explosive detection systems (EDS) equipment;
- (e) explosive detection dogs;
- (f) explosive trace detection (ETD) equipment;
- (g) metal detections equipment.

A hand search shall consist of a thorough manual check of the consignment, including all its contents.

Screening by explosive trace detection (ETD) equipment shall consist of the analysis of samples taken from both the inside and the outside of the consignment and from its contents. The contents may also be subjected to a hand search.

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 the parts of the consignment can actually be seen, with or without aids; or
- (c) for live animals.



The following means or methods may be applied only where it is not possible to apply any of the other means or methods owing to the nature of the consignment:

- (a) a simulation chamber combined with a visual check, if agreed by the appropriate authority; or
- (b) other appropriate security controls, if agreed by the appropriate authority notified to the Commission.

#### **2.10.8.2 Exemptions from Screening Requirements**

The following consignments may be exempted from screening:

- (a) time-critical consignments of life-saving materials, provided that they come from a reliable source and are accompanied by appropriate documentation;
- (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;
- (c) nuclear materials, provided that they are protected in accordance with the Convention of the Physical Protection of Nuclear Materials, New York and Vienna, 3<sup>rd</sup> of March 1980;
- (d) consignments which are individually less both than 6 millimetres in thickness and than 250 grams in total weight;
- (e) consolidations composed uniquely of consignments exempted under d); and
- (f) without prejudice to the security controls that have been applied in accordance with Council Regulation (EEC) No2913/92 and in particular article 36a thereof, transfer cargo and transfer mail arriving by air provided that they are not subjected to detailed Community implementing rules and are protected from unauthorised interference from their arrival until the departure of the aircraft on which they are to be carried, and
- (g) cargo arriving from non-EU countries listed at Annex 6-F of Regulation (EU) No 2015/1998.

Consignments containing radioactive materials are required to be appropriately packed and documented. The consignments shall always be accompanied with relevant documentation attesting their content and origin.

Consignments referred to in paragraph d) can be e.g. letter mail.

Reliable sources include established medical and charitable organisations, for which the regulated agent or appropriate authority has confirmed:

- the address; and
- the nature of business of operation; and
- contact details of a person accepting responsibility for the consignment; and
- VAT reference number or company registration number.

The documentation shall indicate the source of the consignment, details of intended recipient and a description of the contents.

Appropriately labelled diplomatic mail need not to be security screened.

The persons conducting the screening shall be qualified as security screeners for air cargo.

#### **2.10.9 Transhipment Cargo**

The protection of transhipment cargo arriving by air shall be done in accordance with applicable directions in 2.10.12.

The transhipment cargo that remains in the custody of Finnair and is protected from unauthorised access does not need to be security screened at the transit station.

In case transhipment cargo arriving by land or rail is loaded on to an aircraft at the transit point without screening, the consignor shall be able to demonstrate where the cargo has been subjected to required security controls.



## **2.10.10 SCREENING OF HIGH RISK CARGO**

When shipment is subjected to High Risk Cargo and Mail category (see detailed description from ACC3 program, chapter 8), it must be screened

- by explosive detection system (EDS equipment) that complies at least with Standard 2 or
- a combination of two or more screening methods, one of which shall be:
  - explosive detection dogs (EDD); or
  - explosive trace detection (ETD).

For mail and cargo below 500g, unless exempted in accordance with point 6.3, dual view x-ray equipment or single view x-ray equipment provided every item is examined from at least two different angles with at least 60 degrees and no more than 90 degrees rotation by the same screener. Where the screener cannot be reasonably sure that no prohibited articles are contained in the consignment the consignment shall be rejected or be rescreened to his satisfaction.

## **2.10.11 Account Consignors**

An account consignor is a known consignor whose consignments can be positively identified for carriage on all-cargo aircraft. If consignments shipped by an account consignor are transported on board an aircraft with passengers, the cargo consignment shall always be security screened before loading.

Account consignors shall be designated by a regulated agent.

In order to be designated as an account consignor, the following procedure shall apply:

- (a) the regulated agent shall provide the entity with the "Aviation security instructions for account consignors" and "Declaration of commitments — account consignor" as contained in Annex 4. These instructions and declaration shall be provided to the regulated agent by the appropriate authority of the Member State in which its site is located;
- (b) the entity shall submit a signed "Declaration of commitments — account consignor" as contained in Attachment 6-D to the regulated agent, unless the entity is a holder of an AEO certificate referred to in point (b) or (c) of Article 14a(1) of Commission Regulation (EC) No 1875/2006 amending Regulation (EEC) No 2454/93. The entity shall also designate at least one person responsible for security at its premises and shall inform the regulated agent of this person's name and contact details. Where applicable, the signed declaration shall be retained by the regulated agent and made available on request to the appropriate authority concerned. Where the requirement to complete a Declaration of Commitments has been waived on the basis of an AEO certificate, an account consignor shall immediately inform the regulated agent if it is no longer a holder of such a certificate;
- (c) the regulated agent shall make a validation by establishing the following details of the prospective account consignor:
  - the company details, including the bona fide business address, and
  - the nature of the business, and
  - contact details, including those of the person(s) responsible for security, and
  - VAT reference number or company registration number, and
  - where the exemption under 2.10.11 b) is applied, the AEO certificate number;
- (d) if the regulated agent is satisfied with the information provided under points (b) and (c), then the regulated agent may designate the entity as an account consignor.

The regulated agent shall maintain a database with the information referred to in point c) above. The database shall be available for inspection by the appropriate authority.

If there is no activity relating to movements of cargo or mail by air on the account of the account consignor within a period of 2 years, the status of account consignor shall expire.

If the appropriate authority or the regulated agent is no longer satisfied that the account consignor complies with the instructions as contained in Annex 4, the regulated agent shall immediately withdraw the status of account consignor.

When, for whatever reason, the security controls specified in the "Aviation security instructions for account consignors" have not been applied to a consignment, or where the consignment has not been originated by the account consignor for its own account, the account consignor shall clearly identify this to the regulated agent.



Account consignors shall be designated by regulated agents, and the regulated agent shall keep a record of them. The records must contain the information listed above and a signed declaration of commitments must be attached. Details of account consignors shall be presented to the aviation authority on request. The data can also be in electronic form.

The appropriate authority in each EU member state will perform inspections to evaluate whether the designation of the account consignor by the regulated agent is appropriate and whether the entity designated as an account consignor complies with national instructions.

"Activity on the account" means the shipping of a cargo consignment. In case a customer is designated as an account consignor again after the status has expired, a new declaration of commitments and a new validation are required.

If an account consignor fails to comply with the national instructions or has not shipped any cargo in two years, the entity having made the designation shall withdraw the status of account consignor.

## **2.10.12 Protection of Cargo and Mail**

Cargo and mail to be carried on an aircraft shall be protected from unauthorised interference from the point at which security controls are applied until the departure of the aircraft on which it is to be carried.

Cargo and mail that are not adequately protected from unauthorised interference after security controls have been applied shall be screened.

The regulated agent, known consignor and account consignor shall, for their own part, be responsible for the safety of the premises used for receiving, handling and storing cargo and mail, and for the security control of these premises. Access to and movement in such premises shall be controlled so that only those persons duly authorised by the company are allowed to enter. All doors leading to the premises shall be kept locked, unless the premises are in constant use or under continuous surveillance. The premises shall be protected so that they cannot be entered without being noticed. The protection can be arranged e.g. by camera surveillance, crime reporting system, patrolling or a combination thereof.

In order to ensure that consignments to which the required security controls have been applied are protected from unauthorised interference during transportation:

- (a) the consignments shall be packed or sealed by the regulated agent, known consignor or account consignor so as to ensure that any tampering would be evident; and
- (b) the cargo load compartment of the vehicle in which the consignments are to be transported shall be locked or sealed or curtain sided vehicles shall be secured with TIR cords so as to ensure that any tampering would be evident, or the load area of flat bed vehicles shall be kept under observation; and either
- (c) the haulier declaration as contained in Attachment 6-E shall be agreed by the haulier who transports on behalf of the regulated agent, known consignor or account consignor, unless the haulier is itself approved as a regulated agent. The signed declaration shall be retained by the regulated agent, known consignor or account consignor for whom the haulier provides transport. On request, a copy of the signed declaration shall also be made available to the regulated agent or air carrier receiving the consignment or to the appropriate authority concerned; or
- (d) the haulier shall provide evidence to the regulated agent, known consignor or account consignor for whom it provides transport that it has been certified or approved by an appropriate authority.

This evidence shall include the requirements contained in Attachment 6-E and copies shall be retained by the regulated agent, known consignor or account consignor concerned. On request, a copy shall also be made available to the regulated agent or air carrier receiving the consignment or to another appropriate authority.

Points b), c) and d) shall not apply during airside transportation.

The transportation shall be arranged so that the consignments are protected from unauthorised interference. The consignments shall be packed or sealed for transportation so that any signs of tampering can be detected, or the consignments shall be protected by locking the cargo load compartment or keeping it under surveillance and the haulier shall either sign a haulier declaration, which shall be made available to the above mentioned entities on request, or present an approval certificate issued by the appropriate authority.



---

If the haulier wishes to obtain the approval of the appropriate authority in Finland, it must seek for approval as a regulated agent. Information about approvals issued by authorities in other EU member states can be requested from CAA Finland on a case by case basis.

After accepting a consignment for carriage, the air carrier and/or its ground handling agent shall be responsible for ensuring that cargo or mail is not left unattended on loading platforms or other areas outside the terminal, but is immediately transferred to the security restricted area.

Every consignment of cargo or mail which is found to have been stored without supervision shall be screened before being loaded on to an aircraft

Cargo or mail located in the critical part of the airport need not be specifically protected.

If the airside of an airport has not been entirely defined as a critical part, cargo must be protected also on the airside either by loading it e.g. into containers so as to prevent unauthorised access or by physical surveillance.

---

## **2.10.13 ACC3**

See Annex 4 for Finnair ACC3 Programme.

---

## **2.11 COMPANY MAIL AND MATERIALS**

---

### **2.11.1 Aim**

The aim of this section is to state the Finnair requirements for ensuring that no prohibited article is taken on board an aircraft in any piece company mail or materials.

---

### **2.11.2 Objective**

The objective is to ensure that company mail and materials taken on board an aircraft do not contain any prohibited article.

---

### **2.11.3 Application**

Finnair company mail and materials carried on Finnair aircraft shall be subjected to security controls before being placed on board an aircraft.

---

### **2.11.4 Definitions**

Mail and materials shall mean internal dispatches of correspondence and materials, such as but not limited to, documentation, supplies, maintenance spares, catering and cleaning supplies and other articles, intended for delivery to Finnair own or contracted organisation for use within Finnair operation. The transportation of dangerous goods in company mail is prohibited.

---

### **2.11.5 Security Controls**

Any shipment of company mail (co-mail) or company materials (co-mat) shall be subject to following measures:

- It shall be controlled and security screened to ensure that no prohibited article has been introduced into company shipment; and
- It shall not be left unattended prior to being loaded on board an aircraft.

Co-mail and co-mat to be loaded into the hold of the aircraft shall either be screened as hold baggage or subjected to the same security controls as for cargo and mail.

Co-mail and co-mat to be loaded into any part of an aircraft other than the hold shall be screened as cabin baggage.



---

Any other co-mail or co-mat shipment made on behalf of Finnair by a contract organisation such as, but not limited to, catering equipment and stores, cleaning supplies and other materials handled by contracted service providers, is screened prior to loading on board aircraft.

Once security controls have been implemented sterility of the company mail and material shall be maintained until such time as it is placed onboard aircraft and maintained until departure of the aircraft.

---

## **2.11.6 Company Materials used for Passenger and Baggage Processing**

Company materials which are used for the purposes of passenger and baggage processing and which could be used to compromise aviation security shall be protected or kept under surveillance in order to prevent unauthorised access.

Self check-in and applicable internet options allowed for use by passengers are considered as authorised access to such materials.

Discarded materials which could be used to facilitate unauthorised access or move baggage into security restricted area or onto aircraft shall be destroyed or invalidated.

Departure control systems and check-in systems shall be managed in such a manner as to prevent unauthorised access.

Self check-in allowed for use by passengers shall be considered as authorised access to such systems.

---

## **2.12 IN-FLIGHT SUPPLIES**

---

### **2.12.1 Aim**

The aim of this section is to state the Finnair requirements for ensuring that no prohibited article is taken on board an aircraft in any in-flight supplies.

---

### **2.12.2 Objective**

The objective is to ensure that in-flight supplies taken on board do not contain any prohibited article that may endanger the safety of the aircraft, its passengers or crew.

---

### **2.12.3 General Provisions**

In-flight supplies, including catering, intended for carriage or use on board a Finnair aircraft shall be subjected to security controls and thereafter protected until loaded onto the aircraft in order to prevent prohibited articles from being introduced on board an aircraft.

All in-flight supplies delivered directly to Finnair aircraft shall be security screened unless they originate from a regulated supplier approved by the appropriate authority.

These instructions shall be followed as a minimum. Outside the EU-area the local legislation may differ or set additional requirements. In case of conflict with local legislation acceptable procedures shall be agreed with Head of Security.

---

### **2.12.4 Regulated and Known Suppliers**

---

#### **2.12.4.1 Regulated Suppliers**

Regulated suppliers of in-flight supplies shall be approved (if applicable) by the appropriate authority.

The approval as a regulated supplier is site specific.

Any entity that ensures the security controls listed below and delivers in-flight supplies directly to Finnair aircraft shall be approved as a regulated supplier. This shall not apply to Finnair in-house deliveries for Finnair aircraft.



#### **2.12.4.2 Known Suppliers**

Known supplier means a supplier who is allowed to deliver in-flight supplies to the airport, from where they can subsequently be delivered to a non-predetermined flight. Known suppliers are approved by the airport operator, Finnair or the company to whom the supplies are delivered at the airport. The approving entity shall notify the airport operator of any known suppliers it has approved.

In order to be designated as a known supplier of in-flight supplies, Finnair or the entity to whom it delivers shall ensure that the prospective known supplier provides information on aviation security standards and shall make a validation.

Known suppliers of in-flight supplies shall be designated by Finnair or entity to whom it delivers. In order to be designated as a known supplier, the entity shall submit a "Declaration of commitments – known supplier of in-flight supplies" to Finnair or Finnair's supplier. The declaration shall be signed by the legal representative or by the person responsible for security. The signed known supplier declaration shall be retained for the period of the contract.

If there are no deliveries within a period of two years, the status of known supplier shall expire. The status may also expire if the appropriate authority or Finnair is no longer satisfied that the known supplier complies to its commitments.

#### **2.12.5 Security Controls**

Suppliers of Finnair in-flight supplies shall implement security controls to prevent the introduction of prohibited articles into such supplies intended to be carried on board aircraft. These measures shall include the following:

- Appoint a person responsible for security in the company; and
- Ensure that persons with access to in-flight supplies receive security awareness training before being given access to these supplies;
- High standards of reliability when employing staff; and
- Prevent unauthorised access to its premises and in-flight supplies; and
- Reasonably ensure that no prohibited articles are concealed in in-flight supplies; and
- Apply tamper evident seals to, or physically protect, all vehicles and/or containers that transport in-flight supplies, This shall not apply during airside transportation.

The known supplier shall designate a person responsible for the implementation and supervision of security regulations in the company. The company management shall be responsible for ensuring that the person to be designated has sufficient means and qualifications for the duty and can be considered as reliable.

When employing personnel, special attention shall be paid to reliability. The company shall ensure that catering and other supplies intended to be loaded onto an aircraft are only handled by such persons who have received appropriate security training.

The company shall be responsible for access control to its stores and premises. Access to and movement in premises used for production, processing, collection and storage shall be controlled so that only those persons duly authorised by the company are allowed to enter. When the premises are not in constant use or under continuous surveillance, all doors leading to them shall be kept locked.

The company shall establish a procedure to ensure that any prohibited articles used in its operations are not sent outside the company premises, e.g. with deliveries to aircraft.

For transporting items from company premises to aircraft, the catering company shall use vehicles in which the cargo compartment is locked or, where necessary, sealed.

If sealing is used in catering trolleys to ensure the integrity of the consignments, the seals shall be numbered and registered.

The supplies delivered shall be subjected to random security screening either before or after delivery to aircraft. They can be screened by x-ray equipment or searched by hand.



## **2.12.6 Security Screening**

In-flight supplies to be loaded on a Finnair aircraft shall be screened unless:

- 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 those controls were applied until the delivery at the aircraft, or, where applicable, to Finnair or another regulated supplier; or
- 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 those controls were applied until delivery to Finnair or regulated supplier.

Any in-flight supply received from a regulated supplier or a known supplier that shows signs of being tampered with, or where there is reason to believe that it has not been protected from unauthorised interference from the time that controls were applied, shall be screened.

Following screening methods are accepted:

- Hand search;
- Visual check;
- X-ray equipment;
- Explosive detection systems (EDS) equipment;
- Explosive detection dogs; and
- Explosive trace detection (ETD) equipment.

After delivery, stores and supplies shall be screened on a random basis. This screening is done visually and shall be made by Finnair crew when checking the delivery.

Stores and supplies from a company which has not been subject to measures listed above shall not be taken on board an aircraft.

Prior to loading, the stores that will be loaded on board an aircraft, shall be stored and handled only in areas and premises where only authorised persons have access.

In-flight stores shall be checked, made up and kept under constant control by authorised personnel, who are properly recruited and trained, until loaded on board an aircraft.

Staff preparing the above-mentioned items should receive appropriate supervision.

Once security controls have been implemented sterility of catering stores and supplies shall be maintained until such time as it is placed onboard aircraft and maintained until departure of the aircraft. In-flight supplies located in the critical part of the security restricted area of an airport are considered to be adequately protected and no additional measures are necessary.

## **2.12.7 Stebs and Lags**

In-flight supplies of STEBs shall be delivered in tamper-evident packaging to an airside area or to a security restricted area. After first reception on airside or in a security restricted area and until their final sale on the aircraft, LAGs and STEBs shall be protected from unauthorised interference. The LAGs and STEBs shall be visually checked for marks of tampering. This check shall take place at the first point of reception at the airside or security restricted area. STEBs shall be kept under control regardless if located in the critical parts of the airport security restricted area.

## **2.12.8 Subcontractors**

All companies subcontracted by Finnair to deliver in-flight supplies (e.g. catering, cleaning) shall comply with this section and the local legislation.

The companies delivering in-flight supplies for Finnair in Finland must be approved by the Finnish CAA.



---

## **2.13 TRANSPORTATION OF WEAPONS**

### **2.13.1 Aim**

The aim of this section is to state the Finnair requirements for controlling transportation of weapons carried on board Finnair aircraft.

### **2.13.2 Objective**

The objective is to ensure that weapons carried on board aircraft are handled securely.

---

### **2.13.3 Transportation of Weapons in the Cabin or Cockpit**

Finnair will not transport weapons or persons carrying weapons in the cabin or cockpit with the exceptions of

- a security guard who travels as a guard of the President of the Republic of Finland, his spouse, the Prime Minister and the Minister for Foreign Affairs or as a guard of the Head of a Foreign State, his spouse, the Prime Minister and the Minister for Foreign Affairs;
- a person authorised to board the aircraft armed, holding special permission granted by the Head of Security or his deputy.

Crew members are prohibited from accepting weapons for transport in the cabin or cockpit.

#### **2.13.3.1 Denial of Carriage**

The Commander has the right to deny carriage of weapons in the cabin for special security reasons.

If the Commander denies the carriage of a weapon in the cabin, the weapon can be transported in the aircraft hold according to paragraph 2.15.4 (Transportation of sporting and hunting weapons in aircraft holds).

#### **2.13.3.2 Notification by Authorities**

Competent authorities must always notify Finnair of the arrival of an armed security guard to a Finnair flight no later than 24 hours prior to departure.

#### **2.13.3.3 Informing the Commander**

The Commander shall always be informed in advance according to the prior notification, if armed persons are to be on board. This shall be done by Crew Service Desk. The Finnair representative at the departure station shall see that the Commander has received the information.

The Commander shall be informed by the Finnair representative of the seating of a security guard or other armed persons and of possible special arrangements in the cabin prior to commencing boarding of the aircraft.

#### **2.13.3.4 Onboard Handling Procedures**

In the above situations, only a handgun with cartridges is allowed in the cabin. The weapon must be kept on board the aircraft in a briefcase or in a bag or non-visibly on person (e.g. shoulder holster) and must be unloaded. The cartridges must be kept separately from where the weapon is kept.

It is prohibited to transport weapons in the cockpit.

#### **2.13.3.5 Disabling Devices**

Disabling devices such as mace, pepper spray etc., containing an irritant or incapacitating substances are prohibited.



---

## **2.13.4 Transportation of Sporting and Hunting Weapons in Aircraft Holds**

Sporting and hunting weapons are carried under the following conditions:

- prior to acceptance the check-in personnel must be assured that the weapon is not loaded. This is done by questioning the customer and gaining a positive answer. Documentation and licenses regarding the carriage of weapon shall be controlled as specified in the State's National Civil Aviation Security Programme.
- the weapon must be suitably packed to prevent possible damage during the flight,
- ammunition must be securely boxed and carried separately to the weapon
- the weapon shall be kept under constant control when in the custody of Finnair
- weapons and ammunition must be stowed in an area that is inaccessible to any person during the flight and shall not be carried in the cockpit or retained by any member of the crew,
- transit and transfer stations must be advised and shall ensure the integrity of such items, and

at the final destination security procedures must be implemented to return the weapons and/or the ammunition to the passenger.

---

## **2.14 IN-FLIGHT SECURITY**

### **2.14.1 Normal Procedures**

#### **2.14.1.1 Authority of Commander**

The Commander has the highest authority on board an aircraft and all crew members are obliged to follow his orders.

The Commander has authority over passengers only in matters of safety and security.

#### **2.14.1.2 Responsibilities On Board**

It is within the Commander's responsibility to decide on necessary actions in situations beyond the normal routine procedures.

It is the responsibility of the crew to take care of passengers and goods on board.

#### **2.14.1.3 Observation of Passengers**

The cabin crew shall observe the behaviour and mental and physical condition of the passengers during the flight to prevent possible conflict situations. Accordingly, the consumption and service of alcohol shall be carefully evaluated (especially on long-haul flights) if any doubt exists. Observance of smoking rules shall be controlled as well.

#### **2.14.1.4 Violation of Rules and Orders**

If any violation against aviation rules or crew orders occurs in the cabin, the CC must be informed and it is his/her responsibility to evaluate the situation and take necessary action towards the unruly passenger. The Commander must be informed if the actions taken towards the passenger are beyond normal routine procedures.

---

## **2.14.2 Unruly Passengers On Board**

### **2.14.2.1 Prevention**

It is the duty of the ground personnel and cabin crew to prevent unruly passengers from boarding the aircraft. The Commander has the right to deny boarding of any disruptive passenger.

If, however, a situation with a disturbing passenger occurs during a flight, it is primarily the responsibility of the cabin crew to resolve and calm down the situation.



#### **2.14.2.2 Handling Procedures**

See OM-A 23, Handling of Unruly Passengers.

---

#### **2.14.3 Crime On Board**

If a crime of any kind takes place on board a Finnair flight it is the responsibility of the Commander to inform OCC and if needed the local (point of arrival if in mid-air) Finnair representatives of this. It is within the responsibility of the local Finnair representatives to inform the local authorities. The Head of Security shall be contacted if necessary.

Crew members should give necessary assistance to the authorities to solve the crime, e.g. by giving witness statements, etc.

A person who is suspected of having committed a crime on board should not be allowed to disembark from the aircraft until the local authorities have arrived.

A crime on board shall be reported to the Head of Security by the Commander and by the Finnair representative at the station.

---

### **2.15 CREW SECURITY**

---

#### **2.15.1 Crew Screening**

Crew members are subject to screening according to local legislation.

Crew members on positioning flights shall comply with the same security procedures and follow the same check-in and boarding procedures as the passengers. Crew members on DH- positioning on the Company flight shall comply with the security procedures for either passengers or crew members.

---

#### **2.15.2 Supernumeraries**

Supernumeraries shall be screened as a minimum as crew members.

---

#### **2.15.3 Carriage of Unknown Articles**

Crew members shall never accept anything for carriage, including letters or envelopes, given by strangers, fellow employees or acquaintances. This is with the exception of

- travel documents mentioned in 2.4.7.7,
- items authorised by the Head of Security and accepted by the Commander.

Crew members travelling on duty, but with no obligations on the flight (e.g. dead head crew), shall comply with the same security procedures and follow the same check-in and boarding procedures as the passengers.

---

#### **2.15.4 Crew Baggage**

Finnair crew members are responsible for their personal baggage. After packing the baggage before the flight the baggage shall be under control of the crewmember. The baggage must never be left unattended and measures to prevent unauthorised access must be taken.

Crew baggage shall be security screened.

---

#### **2.15.5 Crew Layovers**

The Head of Security is responsible for evaluating the security of crew layovers (e.g. local security situation, hotel safety and security, ground transportation) and the security approval of the hotel. In urgent circumstances the OCC Duty Manager may act on behalf of the Head of Security.



---

The assessment of crew hotels shall be made in co-operation with the department responsible for crew hotel agreements. The assessment can be made by on-site visits or by other means as deemed appropriate by Head of Security considering the threat level.

---

## **2.15.6 Reporting**

Crew members shall always report all security incidents to the Head of Security. This should be made through normal reporting channels. In urgent cases, reporting should be done directly.

---

## **2.15.7 Security Awareness**

Finnair crew members shall be aware of and observe the following security related items

- exceptional behaviour of passengers and personnel,
- irregular occurrences during the flight or on board a Finnair aircraft,
- unusual conditions and/or ineffective security measures at the airports.

---

## **2.16 CODESHARE PROCEDURES**

Before starting codeshare operations with a new carrier, a mutual agreement concerning security related issues shall be completed.

This agreement shall contain the following items:

- passenger and carry-on baggage security,
- hold baggage security,
- passenger and baggage reconciliation,
- cargo security,
- transportation of weapons on board and information procedure,
- procedures concerning inadmissible persons, deportees and persons in lawful custody,
- notification procedures for threats affecting the operations of Finnair or codeshare partners,
- security contact information.

Finnair negotiators are responsible for ensuring that this agreement is completed as a part of the whole codeshare agreement.

The Head of Security shall be involved when planning and completing this agreement.

---

## **2.17 SECURITY OF OPERATIONS ABROAD**

---

### **2.17.1 Definition**

The Head of Security is responsible for security of operations abroad. This consists of continuous evaluation, assessment of current threat and risk situation and implementation of necessary measures in those areas and locations where Finnair operates.

Following areas are included:

- Terrorism
- Civil unrest
- Acts of war
- Environmental disasters



## **2.17.2 Aim**

Finnair protects its operations abroad in a manner acceptable both to the local authorities and in keeping with the Company's own policy. This is achieved by treating the national laws as minimum criteria. Furthermore, the risks that Finnair operations may face abroad shall be taken into consideration and security measures adjusted accordingly.

## **2.18 SECURITY QUALITY CONTROLS**

The implementation and effectiveness of security measures shall be regularly subjected to verification of compliance with the Finnair Security Manual, IOSA standard, ICAO Annex 17 and applicable national regulations. The verification is done by security audits, inspections and self assessments.

The security functions are audited in accordance with Finnair Safety and Compliance Management Manual and applicable checklists to ensure compliance with regulations and SEM.

The auditors performing security inspections and audits shall be accepted by the Head of Security. The auditor shall also meet the requirements set in Finnair Safety and Compliance Management Manual, Appendix 3 (Safety and Compliance Advisor). In addition, the auditor shall have appropriate training in security quality control.

The inspections and audits are performed according to the audit plan approved by Head of Security and maintained by Safety and Compliance Management.

Monitoring of Security Audit and Inspection plan progress takes place in Audit and Inspection Review meeting, which is held at least 2 times per year. Security auditors participate in the meeting and minutes are recorded. Secondary objective of the meeting is to continuously monitor and improve Security related competence and training needs of auditors. As minimum auditors are given refresh training, which includes Generic Security status and threat update.

The Self Assessment process is described in Finnair Operational Security Quality Control Programme.

### **2.18.1 Security Audit**

A security audit is a comprehensive evaluation of airport and airline security needs including the identification of vulnerabilities which could be exploited to carry out an act of unlawful interference or endanger the security of company personnel and assets, and the recommendation of corrective actions.

A security audit shall be conducted

- before starting operations to a new destination based on risk assessment completed by Security Management, or
- when deemed necessary by the Head of Security. However, as a minimum at least six security audits shall be carried out in a calendar year.

An audit shall as a minimum cover the following key areas:

- airport security;
- passenger and carry-on baggage security;
- hold baggage security;
- cargo security;
- aircraft security;
- security of in-flight supplies
- airport security contingency and response procedures, including exercises;
- security of company premises and assets (e.g. airport and sales offices, valuables)
- crew hotel security (including crew transportation), and
- handling of threats

A specific security audit checklist shall be used when performing an audit. Cargo security shall be audited according to the Cargo Security Audit Checklist (see Annex 4, Attachment 1).

The Head Security of is responsible for ensuring that the security audits are carried out.



## **2.18.2 Security Inspections**

A security inspection is an examination of the existing implementation of relevant requirements set by this Manual. The main focus is on Finnair operations.

The Head of Security shall ensure that security inspections are performed to ensure that the acceptable level of security on Finnair operations is achieved.

An inspection shall be performed in conjunction with each regular station audit performed by Safety and Compliance Management Department or when determined necessary by the Head of Security due to specific security reasons or increased threat. However, as a minimum six inspections shall be carried out in a calendar year.

An inspection shall cover the following key areas:

- airport security programme;
- passenger and carry-on baggage security;
- hold baggage security;
- passenger and hold baggage reconciliation;
- cargo security, if applicable
- aircraft security;
- security of in-flight supplies
- threat handling.

A specific security inspection checklist shall be used when performing an inspection. Cargo security is inspected as part of cargo inspections/audits performed by Finnair Cargo.

## **2.18.3 Audit and Inspection Reports**

A report shall be completed after each security audit and inspection. This shall not be made later than two weeks after the audit and inspection. The Q-Pulse system shall be used as the reporting tool.

The Head of Security is responsible for maintaining a file of the audit and inspection reports. The Q-Pulse system shall be used.

The Head of Security or the auditor shall distribute the audit and inspection reports to the relevant nominated persons and Safety and Compliance Management. This shall be done by the Q-pulse system.

## **2.18.4 Observations and Findings**

The respective post holders shall be informed by the Head of Security or the auditor about observations and findings made during the audit and inspections. The Q-Pulse system shall be used. Post holders shall ensure that corrective actions are initiated and performed within the timeline given in the report. Nominated persons shall inform the Head of Security of the corrective action plan and the completed corrective action through the Q-Pulse system.

## **2.19 SECURITY OF SUBCONTRACTORS**

The security status and the working practice of subcontractors contracted by Finnair shall be carefully evaluated.

The background of the subcontractor's personnel working for Finnair or in Finnair facilities shall be checked (e.g. criminal background check, employment history) in an appropriate way, to ensure the trustworthiness of these personnel.

Applicable personnel or subcontractors and service providers shall have appropriate security training as required by the State or Finnair. Such personnel that manage or operate security screening systems shall be certified with requirements of the applicable aviation security authority and shall complete initial and recurrent training, which shall include training in the identification of explosives, weapons or other dangerous items or devices.

The responsibility of ensuring the security of subcontractors and their personnel belongs to the person who signs the contract on behalf of Finnair.



All Finnair subcontractors and service providers shall comply with the security regulations applicable at the location and with the Finnair Security Manual Subcontractor version and related directives.

Each nominated person is responsible for ensuring that the Finnair Security Manual Subcontractor version is distributed to relevant subcontractors and external service providers and that personnel belonging to those entities have received applicable security training. The Head of Security is responsible for distributing the Finnair Security Manual Subcontractor version to the nominated persons.

---

## **2.20 SECURITY EQUIPMENT AND PRODUCTS**

Equipment and other security products used to implement security controls shall be approved or certified by the state of operations if applicable. If no local standards exist reference shall be made to International Civil Aviation Organisation (ICAO) standards and recommendations.

---

## **2.21 AD HOC FLIGHTS**

Standard security measures described in SEM can be deviated for ad hoc flights if equivalent level of security can be ensured and deviation is approved by Head of Security. If applicable Traficom shall be informed. However, following minimum requirements shall always be complied with:

- Screening of passengers and hand luggage: According to chapter 2.3.6.
- Screening of hold baggage: According to chapter 2.6.7.
- Cargo: 100% screening, or reliable and well known customer who is a regulated agent or known consignor. Cargo shall be handled in a secure environment by appropriately trained staff and transport is secured to prevent unauthorised access.
- Aircraft protection: According to chapter 2.9.5.

## **3. INTENTIONALLY LEFT BLANK**

Intentionally Left Blank

## **4. HANDLING OF THREATS**

---

### **4.1 GENERAL**

Since all Finnair staff may become the recipients of or intermediaries in a sabotage or hijacking threat, it is important that staff members know precisely what action to take in such circumstances.

In case a threat is received, a list of offices, names and private telephone numbers of appropriate supervisory personnel who need to be informed shall be available at all switchboards, in all airport and other offices.

In the same way, the local airport and security authorities shall be informed of the appropriate persons within the local Finnair organization that must be contacted if threats involving Finnair's operations and property are received.

---

### **4.2 DESCRIPTION OF THREATS**

A sabotage threat is information stating, e.g. that an explosive device has been or will be placed on board an aircraft, in a building or other installation.

A hijack threat is information stating that one or more persons will try to assume control of an aircraft by force, threat or other form of intimidation.

---

### **4.3 CLASSIFICATION OF THREATS**

Threats are classified into two categories on the basis of the content and specificity of the threat.



#### **4.3.1 Non-Specific Threats**

A non-specific threat is in question if

- the airline is not identified;
- the flight or building is not specified;
- neither date nor time is mentioned;
- neither point of origin nor destination is given.

#### **4.3.2 Specific Threat**

A specific threat is in question if

- the originator of the threat identifies himself;
- the airline is identified;
- a specific flight or building is mentioned;
- the exact date and/or time is stated;
- the origin and/or destination of the flight is given; or
- the names of Finnair staff on duty or passengers on board the aircraft are mentioned.

### **4.4 RECEIVING THREATS**

Threats can be received by Finnair staff normally over the telephone, by mail or by social media /chat. Threats are mostly made by anonymous persons or persons who give the name of a private person or an organization. It is also possible that a person in contact with Finnair staff will make a threat.

A threat can be received by Finnair staff when in contact with the public and passengers. It is important to try to memorize the person who has expressed a verbal threat and the content of the threat. The person should be kept under surveillance. All the practical information needed to later find and identify the person must be entered in the threat report form.

The recipient of a threat shall immediately inform his supervisor, Finnair Operations Control Center (OCC) and, if applicable, the local police for further action and send a completed threat report form to the Head of Security as soon as possible. OCC shall inform the Head of Security and police about the threat. Finnair Security Management shall inform relevant aviation security authorities of the threat.

Finnair staff may also receive threat messages as official warnings from local authorities concerning directly or indirectly Finnair operations or property. When the warning is given over the telephone by an unknown official, the receiver should confirm the authenticity of the message with a return call. The contact person shall be informed immediately.

#### **4.4.1 Tracing a Threat Call**

If it is technically feasible to trace telephone calls, arrangements should be made with local law enforcement authorities to obtain a standing authorisation permitting the immediate tracing of threat calls by the telephone company.

#### **4.4.2 Recording a Threat Call / A Second Person Listening to the Call**

Threat calls should be recorded if it is possible and permitted by local law. Alternatively, the calls should be listened to by a second person. During a threat call it is important to try

- to write down the telephone number if possible;
- to keep the caller talking and get useful information by asking questions;
- to get the caller to repeat his message, wholly or in part, to ensure that nothing has been missed or misrecorded;
- to observe variations in language or expressions which later may be of use when assessing the threat;
- to listen carefully to accent, pronunciation and expressions and to attempt to judge the type of voice, e.g. youthful, slurred; etc.



- to be alert for any background noises such as music, conversation, traffic, public announcements, machinery or jet engines; and
- to get the caller's name, address and telephone number by informing the caller that Finnair can not accept anonymous calls; and
- to try to trace the call by holding the line open after the call and by informing the telephone company.

#### **4.4.3 Recording a Threat Call**

All information on the threat should be entered immediately in the threat report form or if not available in free format. The threat report form, which can also be found from Finnair intranet, should be placed near every switchboard operator and near the public service desks and telephones.

#### **4.4.4 Informing about a Threat**

The station supervisor shall inform the local law enforcement and aviation security authorities about the threat in all details when applicable. OCC shall inform the law enforcement agency. Security management shall inform Traficom.

When the threat concerns a specific target, flight, station, airport, building etc., it is important to inform the person who is responsible for the targeted operations or property of the threat. In all cases, the Head of Security shall be informed.

### **4.5 REPORTS**

All threat incidents shall be reported by the local Finnair officer in charge to the Head of Security as soon as possible. Incidents concerning air traffic shall always be reported via Finnair OCC, who will contact the Head of Security.

The first report of an incident shall contain the following information if available:

- the target of the threat (flight number, building, office etc.);
- the content of the threat;
- the receiver of the threat;
- the evaluated risk category;
- the number of passengers and crew on board;
- actions which are or will be taken;
- other useful information (expected delay etc.).

A chronological log of actions as they are taken shall be kept.

If the incident in question is RED, the Head of Security shall monitor the progress of action. The Head of Security shall be immediately informed about the progress of action in other cases.

At the conclusion of the incident, a full report shall be sent immediately to the Head of Security. A specification of all costs incurred by Finnair due to the threat and the subsequent action shall be included in the report.

#### **4.6 Methods of Communicating the Change in Threat Level**

The Head of Security shall communicate the change in threat level to the crew, operational personnel, management and stations.

The methods used for communicating may include, but are not limited to following:

- telephone, fax
- SITA-message
- ACARS
- e-mail
- in person



- Finnair Crew Information System
- Finnair Intranet.

The Head of Security shall initiate the communication through relevant channels. When using the Crew Information System the Head of Security shall ensure that the information is inserted to the system to be available for crew members and also deleted when not applicable any more.

## **5. FINNAIR AVIATION SECURITY TRAINING PROGRAMME**

### **5.1 INTRODUCTION**

Finnair Aviation Security Training Programme is based on the National Civil Aviation Security Training Programme, EU regulation 2015/1998, EASA-OPS and applicable ICAO standards and the general interests of Finnair.

To ensure that everyone with aviation security related duties is aware of their responsibilities concerning aviation security issues relevant to their duties. Training must have been received and completed so that an appropriate level of awareness is gained. The depth of training required for each function is dependent on the responsibilities and varies from a general appreciation to in-depth knowledge. Training shall include, as appropriate, theoretical and practical training to ensure:

- Personnel, employed by or under the control of the Finnair who implement security controls, have the competence to perform their duties;
- Flight and cabin crew members, as well as frontline aircraft ground handling and cargo handling personnel, are able to act in the most appropriate manner to minimize the consequences of acts of unlawful interference and disruptive passenger behaviour.

In general the security training shall include following elements:

- Security systems and access control
- Ground and in-flight security
- Pre-board screening
- Baggage and cargo security
- Aircraft security and searches
- Weapons and prohibited articles
- Overview of terrorism, and
- Other areas and measures relating to security that are considered appropriate to enhance security awareness.

See also Operations Manual – Part D and GOM (chapter 3.5.).

In ICAO Signatory States outside EU aviation security training programmes approved by the national appropriate authority are considered acceptable.

Aviation security training consists of three categories: initial, differences and recurrent training. Additional and/or in-depth training for various departments and functions shall be initiated if deemed necessary by Head of Security.

### **NOTE:**

Personnel with aviation security related duties are such whose duties and/or decision making has or may have effect on the security of Company operations.

### **5.2 RESPONSIBILITIES**

#### **5.2.1 Head of Security**

The Head of Security is responsible for reviewing and updating company security programmes for continuous improvement and to reflect regulatory and operational changes.



To ensure the continuous improvement of security training and the incorporation of regulatory amendments of operational changes the Head of Security shall follow

- Feedback from staff
- Quality and security audit reports
- Changes in regulations and authority requirements
- Changes in threat
- Changes and developments in operational environment, and

inform the relevant postholders of needs for revising the security training accordingly.

The Head of Security is also responsible for approving company security training programmes.

## **5.2.2 Nominated Persons**

The respective nominated persons are responsible for ensuring that the applicable personnel receive initial aviation security training, and that they obtain the required renewals in due time.

## **5.2.3 Department Management**

In such areas that are not covered under the responsibilities of nominated persons the management of the respective departments are responsible that the applicable personnel receive initial aviation security training, and that they obtain the required renewals in due time.

## **5.2.4 SECURITY INSTRUCTORS**

Security Instructors shall have appropriate training and comprehensive experience in the field of the training subject. Security Instructors shall be approved by Traficom or applicable local authority.

## **5.2.5 SECURITY MANAGERS**

Security managers shall have completed security training as defined in Commission Implementing Regulation (EU) 2015/1998 section 11.2.5 resulting in following competencies:

- knowledge of relevant legal requirements and how they should be met;
- knowledge of internal, national, Union and international quality control;
- ability to motivate others;
- knowledge of the capabilities and limitations of security equipment or screening methods used.

## **5.3 INITIAL (AWARENESS) TRAINING**

Initial training is required for all Company personnel with aviation security related duties as specified in table in chapter 5.6.

All Company personnel must receive initial aviation security training before assuming duties that involve security responsibilities.

At such stations where there are no Finnair employees responsible for the operations the in-house station manager or equivalent person responsible for Finnair operations at a specific station, shall receive Finnair security training. This training can be conducted by an e-learning training programme.

## **5.4 DIFFERENCES TRAINING**

Differences training is normally included in the recurrent training. Depending on the need, differences training can also be given during separate training sessions or as on-the-job training.



## 5.5 RECURRENT TRAINING

Recurrent training shall be successfully completed within a 3 year period after obtaining initial training and every 3 years thereafter. Flight and cabin crew shall receive yearly recurrent security training specific to their duties.

## 5.6 TRAINING SYLLABUS FOR SECURITY

### Training Syllabus for initial and recurrent training

Crew members shall have initial and recurrent security training. Crew members shall have initial training prior to assuming duties that involve security responsibilities.

Cabin crew member shall have received a training in general security aspects in aviation, including awareness of the provisions laid down in Regulation (EC) No 300/2008 and hold a valid cabin crew attestation issued in accordance with Annex V (Part-CC) to Regulation (EU) No 1178/2011 before participating in operator conversion security training.

Detailed syllabi of the initial and recurrent trainings are specified in Appendices A-1 and B-1 and C-1.

Initial and recurrent trainings cover the following areas.

	Flight Crew		Cabin Crew	
	Initial training	Recurrent training	Initial training	Recurrent training
Terrorism (e)	X	X	X	X
Regulations and organizations	X	X	X	X
Finnair security program and organization	X		X	
Aircraft protection and sealing	X	X	X	X
Access control	X	X	X	X
Aircraft security search (b) (h)	X	X	X	X
Passenger and hand baggage security	X		X	
Hold baggage security	X		X	
Cargo and mail security	X			
Security of company mail and materials	X			
Carriage of weapons	X		X	
Prohibited items and explosives (h) (i)	X	X	X	X
Unruly passengers (a) (b) (c) (d) (f) (g)	X	X	X	X
Special and risk category passengers	X	X	X	X
Handling of threats (a) (b) (e) (f) (h) (i)	X	X	X	X
Hijack situations (b) (e) (f) (g)	X	X	X	X
Protection of the flight deck (a) (b) (e) (g)	X	X	X	X
Airport emergency and contingency situations	X		X	
Reporting	X		X	
New and evolving threats to aviation	X	X	X	
Layover safety and security	X	X	X	X
Information security	X		X	

Notes:

- Flight Crew and Cabin Crew trainings are referenced to EU Reg 2015/1998 11.2.3.6., 11.2.3.7, 11.2.6., and 11.2.7.
- Initial and recurrent trainings can include classroom/hands-on training and e-learning.
- Marked recurrent training subjects are covered within intervals not exceeding 36 months.
- Subjects including the following elements are marked with the letters (a) - (i)
  - (a) Determination of the seriousness of the occurrence



- (b) Crew communication and coordination
- (c) Appropriate self-defence responses
- (d) Use of non-lethal protective devices assigned to crew members
- (e) Understanding of behaviour of terrorists so as to facilitate the ability of crew members to cope with hijacker behaviour and passenger responses
- (f) Live situational exercises regarding various threat conditions
- (g) Flight Crew compartment procedures to protect the aircraft
- (h) Aircraft search procedures in accordance with reg 300/2008, incl. Identification of prohibited articles
- (i) Guidance on the Least Risk Bomb Locations
- Flight Crew Cyber Threat training is given at intervals deemed appropriate by the Head of Security.

### **Security Training (Operational Ground Staff)**

Operational Ground Staff members shall have initial and recurrent security training. Staff members shall have initial training prior to assuming duties that involve security responsibilities.

Detailed syllabus of the initial and recurrent trainings is specified in Appendix C-1.

Initial and recurrent trainings cover the following areas.

	Initial training	Recurrent training
Terrorism	X	X
Regulations and organizations	X	X
Finnair security program and organization	X	X
Aircraft protection	X	X
Access control	X	X
Passenger and baggage reconciliation	X	X
Passenger and hand baggage security	X	X
Hold baggage security	X	X
Cargo and mail security	X	X
Security of company mail and materials	X	X
Carriage of weapons	X	X
Unruly passengers	X	X
Special and risk category passengers	X	X
Handling of threats	X	X
In-flight security	X	X
Airport emergency and contingency situations	X	X
Reporting	X	X
New and evolving threats to aviation	X	X
Information security	X	X

Notes:

- Operational Ground Staff trainings are referenced to EU Reg 2015/1998 11.2.3.6., 11.2.3.7, 11.2.3.8., 11.2.6., and 11.2.7.
- Initial and recurrent trainings can include classroom/hands-on training and e-learning.
- Marked recurrent training subjects are covered within intervals not exceeding 36 months.

---

## **5.7 APPROVALS**

Finnair aviation security training programs are reviewed and approved by the Head of Security and the Finnish CAA.



---

## 5.8 RECORDS OF TRAINING

A record of training must be maintained in the organization receiving the training. This must include:

- Individuals name
- Date of completion
- Reference to training course/ requirement
- The name and address of the organization providing the training

The training record must be made available upon request to the appropriate Authority.

---

## 5.9 ASSESSMENT OF COMPETENCES

The assessment of competencies for operational personnel shall ensure that the objectives of the training have been met. For Flight and Cabin crew assessment is done via testing after the security awareness training.

Operative Ground and Cargo staff perform security awareness training and the following test as part of Airport ID card applying or renewal process. This training and test is defined by CAA Finland.

External Security Partner (ISS) providing security services for Finnair is responsible for arranging awareness training and the assessment of competences for it's personnel. This training is mandated by CAA Finland. Monitoring of this process takes place annually as part Security Audit Programme.



## **Appendices A1, B1 and C1 to SEM 5**

A	Security training course for Flight Crew	App A-1
B	Security training course for Cabin Crew	App B-1
C	Security training course for Operational Ground Staff	App C-1

### **Appendices A-1, B-1 and C-1**

#### **Appendix A-1: Flight Crew - Initial Security Training**

Security arrangements and regulations

- International agreements and regulations
- National AVSEC program and legislation
- Finnair security program and organisation

Terrorism

- History and current threats
- Motives
- Understanding the behaviour of terrorist
- Modus operandi
- Current threat situation

Aircraft protection and sealing

- Means to protect aircraft
- Sealing procedures

Access control

- Security restricted areas of the airport
- Security screening, passengers, vehicles and staff
- Airport ID, background checks
- Role of the crew members

Aircraft security search

- Legal requirements
- Responsibilities
- Areas to be searched
- Correct actions if suspicious items found

Airport security measures

- Passenger and hand baggage security
- Hold baggage security
- Cargo and mail security
- Security of catering and supplies

Carriage of weapons

- Authorized persons
- Finnair policy and procedures

Explosives and prohibited items

- Recognition of explosives
- List of prohibited items



Unruly passengers

- Motives, background
- Prevention principles
- Crew procedures and practices
- Appropriate self-defence responses
- Use of protective devices
- Legal aspects

Special and risk category passengers

- Finnair policy and procedures
- Persons exempted from screening
- DEPO, INAD, PIC
- Finnair security measures

Handling of threats

- Reception of threat
- Response of the organisation, threat assessment
- Crew actions and decision-making
- Bomb search and handling
- Least risk bomb location

Hijack situations

- Types of hijackers, motives
- What to expect?
- Crew communication and coordination
- Crew priorities and good practices

Protection of the flight deck compartment

- Enhanced cockpit door
- Regulations
- Importance of the correct door procedures
- Two-person rule

Airport emergency and contingency situations

- Roles of different emergency personnel
- Remote parking areas for aircraft under threats

Reporting of security incidents

- Importance of reporting
- Reporting channels

New and evolving threats to aviation

- MANPADS
- Laser attacks
- Drones
- Attacks to airports
- Risk and conflict zones
- Insider threat
- Human trafficking

Layover safety and security

- Preparedness, staying safe



**SEM**  
**FINNAIR SECURITY MANUAL**

---

Effective date  
21.09.2023, Rev 19

Page  
58

---

- Good practices
- Contingency and emergency procedures

Information security

- Handling of sensitive information, responsibilities



## **Appendix B-1: Cabin Crew - Initial Security Training**

### Security arrangements and regulations

- International agreements and regulations
- National AVSEC program and legislation
- Finnair security program and organisation

### Terrorism

- History and current threats
- Motives
- Understanding the behaviour of terrorist
- Modus operandi
- Current threat situation

### Aircraft protection and sealing

- Means to protect aircraft
- Sealing procedures

### Access control

- Security restricted areas of the airport
- Security screening, passengers, vehicles and staff
- Airport ID, background checks
- Role of the crew members

### Aircraft security search

- Legal requirements
- Responsibilities
- Areas to be searched
- Correct actions if suspicious items found

### Airport security measures

- Passenger and hand baggage security
- Hold baggage security

### Carriage of weapons

- Authorized persons
- Finnair policy and procedures

### Explosives and prohibited items

- Recognition of explosives
- List of prohibited items

### Unruly passengers

- Motives, background
- Prevention principles
- Crew procedures and practices
- Appropriate self-defence responses
- Use of protective devices
- Legal aspects

### Special and risk category passengers

- Finnair policy and procedures
- Persons exempted from screening



# SEM

## FINNAIR SECURITY MANUAL

---

Effective date  
21.09.2023, Rev 19

Page  
60

---

- DEPO, INAD, PIC
- Finnair security measures

### Handling of threats

- Reception of threat
- Response of the organisation, threat assessment
- Crew actions and decision-making
- Bomb search and handling
- Least risk bomb location

### Hijack situations

- Types of hijackers, motives
- What to expect?
- Crew communication and coordination
- Crew priorities and good practices

### Protection of the flight deck compartment

- Enhanced cockpit door
- Regulations
- Importance of the correct door procedures
- Two-person rule

### Airport emergency and contingency situations

- Roles of different emergency personnel
- Remote parking areas for aircraft under threats

### Reporting of security incidents

- Importance of reporting
- Reporting channels

### New and evolving threats to aviation

- MANPADS
- Laser attacks
- Drones
- Attacks to airports
- Risk and conflict zones
- Insider threat
- Human trafficking

### Layover safety and security

- Preparedness, staying safe
- Good practices
- Contingency and emergency procedures

### Information security

- Handling of sensitive information, responsibilities



## **Appendix C-1: Operational Ground Staff - Initial Security Training**

Security arrangements and regulations

- International agreements and regulations
- National AVSEC program and legislation
- Finnair security program and organisation

Terrorism

- History and current threats
- Motives
- Understanding the behaviour of terrorist
- Modus operandi
- Current threat situation

Aircraft protection

- Means to protect aircraft
- Responsibilities
- Aircraft security Search
- Sealing procedures

Access control

- Security restricted areas of the airport
- Security screening, passengers, vehicles and staff
- Airport ID, background checks
- Role of the operational staff

Airport security measures

- Passenger and hand baggage security
- Hold baggage security
- Passenger and Baggage reconciliation
- Cargo and mail security
- Security of catering and supplies
- Prohibited items

Carriage of weapons

- Authorized persons
- Finnair policy and procedures

Unruly passengers

- Motives, background
- Prevention principles, profiling
- Staff procedures and practices
- Legal aspects, refusal of carriage

Special and risk category passengers

- Finnair policy and procedures
- Persons exempted from screening
- DEPO, INAD, PIC
- Finnair security measures

Handling of threats

- Reception of threat, staff procedures



- Notification and reporting
- Response of the organisation
- Detection of prohibited items
- Response to prohibited items

#### In-flight security

- Protection of the flight deck compartment
- Unruly passengers prevention and handling
- New and evolving threats

#### Airport emergency and contingency situations

- Roles of different emergency personnel
- Remote parking areas for aircraft under threats

#### Reporting of security incidents

- Importance of reporting
- Reporting channels

#### New and evolving threats to aviation

- MANPADS
- Laser attacks
- Drones
- Attacks to airports
- Risk and conflict zones
- Insider threat
- Human trafficking

#### Information security

- Handling of sensitive information, responsibilities

## 6. CYBER SECURITY

Critical information and communications technology systems are listed on a separate document called Critical Aviation Safety and Aviation Security Systems. This document defines the protection, detection, and recovery measures related to Critical Aviation Security systems.

Risk assessments related to these systems are done according to principles described in Finnair ISMS manual Chapter3.

Critical systems have been selected based on their Flight Safety impact. Criticality classification has been defined as follows.

Orange: There is potential direct major negative impact on flight safety

Yellow: There is potential direct minor negative impact on flight safety or Indirect negative impact on safety

Green: Flight Safety impact is negligible



## APPENDICES

### Annex 1

#### 1. 1 PROHIBITED ARTICLES

1. Passengers are not permitted to carry the following articles into the security restricted area and the cabin of an aircraft:
  - (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, excluding telescopic sights,
    - compressed air and CO<sub>2</sub> 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 — 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 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 — 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 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.

## 2. Articles prohibited from hold baggage

The following articles shall not be placed in 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.



**SEM**  
**FINNAIR SECURITY MANUAL**

Effective date  
21.09.2023, Rev 19

Page  
65

## Annex 2

### 2.1 SECURITY ASSURANCE AND DECLARATION OF A KNOWN CONSIGNOR DELIVERING AIR CARGO



**SECURITY ASSURANCE AND DECLARATION OF A KNOWN CONSIGNOR  
DELIVERING AIR CARGO**

Company: _____	
Address: _____	
Telephone: _____	Fax: _____

	YES	NO	Comments
1. Finnair Condition of Carriage for Cargo and the instructions concerning a known consignor have been read and understood	<input type="checkbox"/>	<input type="checkbox"/>	_____
2. Secure handling and storage of air cargo consignments so that:	<ul style="list-style-type: none"><li>- Area of handling and storage protected from unauthorised interference <input type="checkbox"/> <input type="checkbox"/> _____</li><li>- Reliable personnel used for these tasks <input type="checkbox"/> <input type="checkbox"/> _____</li><li>- Instructions given to personnel <input type="checkbox"/> <input type="checkbox"/> _____</li><li>- Personnel duly trained <input type="checkbox"/> <input type="checkbox"/> _____</li><li>- The consignment consist only of goods mentioned in the AWB <input type="checkbox"/> <input type="checkbox"/> _____</li></ul>		
3. Transportation is arranged so that air cargo consignments are protected from unauthorised interference	<input type="checkbox"/>	<input type="checkbox"/>	_____
4. Documents of the consignment are kept for later examination	<input type="checkbox"/>	<input type="checkbox"/>	_____
5. Finnair has the possibility to check the functions and instructions of secure handling when required	<input type="checkbox"/>	<input type="checkbox"/>	_____

I assure that the above mentioned information is correct and that air cargo delivered by this company is handled and transported accordingly.

Place and date: \_\_\_\_\_ Signature (official) \_\_\_\_\_  
Name clarification \_\_\_\_\_

For Finnair use only:

ACCEPTED   
UNACCEPTED

Signature and code \_\_\_\_\_



## Annex 3

### 3.1 NON-HEADCOUNT EVALUATION AND ACCEPTANCE PROCEDURE

#### 1. Evaluation of non-headcount station

Before accepting a station to become a non-headcount station an evaluation must be completed. This evaluation is based on following questions:

1. Does your National Aviation Security Programme demand the passenger headcount to be done in the cabin?
2. Are the procedures at your station such that the number of boarded passenger are 100% reconciled with the number of checked-in passenger?
3. Are the facilities at your station such that it can, on reasonable basis, be ensured that all the passenger who have passed through the boarding point enter the aircraft?

This questionnaire shall be completed by the area or station manager (or equivalent).

The evaluation is done by the Head of Security.

**Station:** \_\_\_\_\_

**Date:** \_\_\_\_\_

**Completed by:** \_\_\_\_\_

#### 2. Acceptance of non-headcount station

The evaluation is done by the Head of Security.

After the evaluation procedure is completed the Head of will make the decision of accepting a station to operate as a non-headcount station.



**SEM**  
**FINNAIR SECURITY MANUAL**

---

Effective date  
21.09.2023, Rev 19

Page  
67

---

#### **Annex 4, Finnair ACC3 Programme**

Finnair ACC3 Programme is a separate document and can be requested from Head of Security.



## **Annex 5**

### **SECURITY KEY PERSONNEL**

#### **CEO**

Mr Topi Manner

#### **Accountable Manager, Chief Operating Officer**

Mr Jaakko Schildt

#### **Head of Security**

Mr Kaarlo Karvonen

#### **Manager, Operational Security**

Mr Christian Rangdell

#### **Manager, SeMS**

Mr Harri Koskinen

#### **Security Manager, Finnair Cargo**

Mr Markku Luostari

#### **Security Manager, Finnair Kitchen**

Mr Markku Luostari



## Annex 6

### SECURITY POLICY

#### 1. VERSION CONTROL AND DOCUMENT HISTORY

Version	Changes / notes	Policy owner	Approved by	Approval and effective date	Data classification
Initial	New Policy	Chief Operating Officer (COO)	Executive Board	29.01.2020	Internal

#### 2. PURPOSE

Finnair operates in a global and fast-changing environment with a volatile threat landscape where a robust and resilient security system is a basic competitive requirement.

The purpose of security activities is to protect Finnair's business, operations, activities, customers, personnel and assets against acts of unlawful interference or other deliberate or unwanted acts. This is achieved by complying with applicable international and national laws and security regulations, and by developing Company own precautions against such acts. Security consists of Company-wide processes, methodologies and measures based on risk and threat management.

This Security Policy ("Policy") states Finnair's approach and view to security.

Finnair Air Operator Security Programme as required and approved by aviation authorities is in the form of Finnair Security Manual.

#### 3. SCOPE

The scope of this Policy is Finnair. The Policy shall be appropriately communicated to staff members and appropriate external individuals and entities.

Security in Finnair consists of following security domains: aviation security, corporate security, information security and cyber security.

**Aviation Security** is defined as combination of measures and human and material resources intended to safeguard civil aviation against acts of unlawful interference.

**Corporate Security** is defined as safeguarding of assets, personnel, customers and Finnair brand against criminal activities and damage as well as against fire, fraud and other unwanted or illegal happenings.

**Cyber Security** is defined as the organization's ability to secure its assets, personnel, customers, information, systems and reputation in cyberspace, cyberspace being the always-on, technologically interconnected world; it consists of people, organizations, information and technology.

**Information Security** is defined as the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information, data or knowledge from unauthorized access, use, misuse, disclosure, destruction, modification, or disruption in order to provide confidentiality, integrity, and availability of information.

#### 4. STATEMENT

Security is a fundamental priority for Finnair. We are committed to

- ensure the safety and security of our customers and staff as applicable,
- prevent human trafficking and illegal travel, and
- protect our assets whether physical, digital or intangible.

Furthermore, Finnair and its organization are committed to

- the provision of resources necessary for the successful implementation of this Policy,
- compliance with applicable regulations and Finnair security standards,
- promotion of security awareness and the establishment of a security culture,



- the establishment of security objectives and security performance standards,
- continual improvement of the Security Management System(s), and
- periodic review of this Policy to ensure continuing relevance to the organization.

In addition, in order to maintain the competitive edge, cash-flow, profitability, legal and contractual compliance, Finnair brand as well as operational excellence, Finnair is committed to preserve the highest standards of security throughout the Company.

Finnair does not accept dishonesty or non-compliance conducted by its personnel or representatives. Such conduct may lead to administrative and other sanctions as described in Code of Conduct.

Finnair Management demonstrates its commitment to security through the approval of this Policy by the Executive Board.

## **5. POLICY OBJECTIVES**

This Policy is established to ensure adequate level of security throughout Finnair to prevent unlawful or other criminal or unwanted acts. The aim of this policy is to develop a strong security culture and a common and robust approach to security throughout the Company. Furthermore, the Policy aims to ensure that we meet internal and external expectations regarding security. Key objective is to protect Finnair's brand, personnel, customers, assets and reputation.

This policy shall be communicated throughout Finnair by Security Management.

## **6. ROLES AND RESPONSIBILITIES**

Finnair has a dedicated person (Head of Security) who is responsible for security within the Company. Head of Security leads the Security Management unit with the responsibility for assessing security risks and threats, promoting and developing good practices in security, monitoring implementation of such practices and ensuring regulatory compliance of security throughout the Company.

Cyber and Information Security forms a part of the Finnair's overall security domain and is lead and managed by Digital Services.

Finnair and its service providers employees have a key role to ensure successful outcome of security. Every employee, supplier and partner is responsible for observing and working according to the given security policy, manuals, standards and instructions.

The roles and responsibilities associated with implementation and compliance with this policy are detailed below.

### **6.1 THE EXECUTIVE BOARD AND THE CEO**

The Executive Board holds the ultimate responsibility and ownership of the Security Management System(s) in Finnair and is responsible for approving this Security Policy. COO is the owner of the Security Policy.

The CEO and Executive Board of Finnair hold the responsibility to oversee the implementation of the Security Policy in their respective units and for reviewing security priorities.

### **6.2 BUSINESS UNITS, FUNCTIONS AND SUBSIDIARIES**

Business units and subsidiaries of Finnair are responsible for implementing the Security Policy into their management systems and aligning their security objectives and procedures accordingly.

It is the responsibility of Heads of Business Units to determine security critical processes, services and resources within their business units. This determination is needed for ensuring that the security procedures and measures are focused correctly.

Heads of Units, Functions and Subsidiaries shall

- Ensure their Unit is compliant with Company's Security Policy and applicable standards and instructions.
- Ensure that their Unit, where applicable, participates in the Security Management System.
- Ensure that security is included in their management of change process.
- Ensure, where applicable, that appropriate security requirements are included in third party contracts.
- Nominate, if requested, a security liaison officer to act as the focal point of contact with Security Management.



### **6.3 HEAD OF SECURITY**

Head of Security is accountable for

- leading and managing security, including aviation cyber security,
- Finnair Security Programme and the Security Management System(s),
- security threat and risk assessments,
- promotion of security culture, policies and practices, and
- monitoring and ensuring security compliance

Head of Security is also the nominated person for security as required by EU Aviation Security Regulation and the National Civil Aviation Security Programme of Finland.

### **6.4 DIGITAL SERVICES / HEAD OF CYBER SECURITY**

Head of Cyber Security is responsible for

- leading and managing cyber security, and
- implementation of aviation cyber security.

### **6.5 UNIT SECURITY LIAISON OFFICER**

Security Liaison Officer is responsible for

- acting as the Business Unit's focal point of contact regarding security issues,
- promote security practices and culture within his/her respective unit
- contributing to the change management process, and
- participating and contributing, where applicable, to the Security Management System.

### **6.6 RESOURCES**

Each Unit shall determine and arrange the resources needed for the establishment, implementation, maintenance and continual improvement of security. If requested, the Units shall have a predefined role (security liaison person) with the responsibility to act as focal point in security related matters in their respective units as well as promote security within the unit.

### **6.7 THIRD PARTIES**

Third parties are required to comply with implementation of this policy as applicable.

## **7. MANAGEMENT SYSTEMS**

### **7.1 SECURITY MANAGEMENT SYSTEM (SeMS)**

Finnair Security Management System (SeMS) provides a formalized, systematic risk-driven framework for managing and integrating security into the overall management system of Finnair. SeMS enables identification of security threats, changes and weaknesses in a consistent way and mitigating them proactively. All key security areas, such as Aviation Security, Corporate Security, Information and Cyber Security, Facilitation and Fraud Management are included in SeMS. Key components of SeMS are: management commitment, governance model, security organization and responsibilities, threat and risk management, security assurance, resource management and security promotion. Finnair SeMS is documented in the SeMS Manual which is published in Company Hub.

### **7.2 INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)**

Information Security Management System (ISMS) is focused on cyber and information security. It includes the same key components as SeMS and is a sub-system of, and integrated as applicable to, SeMS. Digital Services is responsible for managing and facilitating the ISMS. Finnair ISMS has been approved by Safety Review Board 28.4.2022.



**SEM**  
**FINNAIR SECURITY MANUAL**

---

Effective date  
21.09.2023, Rev 19

Page  
72

---