DHS GmbH
Am Hagen 5
59368 Werne

Aviation Security Manual

Prepared for: Station Management and all Employees

Prepared by: DOM

Issued: 02.02.2023, last update 30.03.2026

Version: V2/Revision 3

This version supersedes all previous versions released prior to the date of issue.

GENEHMIGT
Von Dominika Doruch , 06:31, 31.03.2026

Record of revisions

Part	Title	Original Issue	Latest Review
1.1.	Security Statement	12.2018	13.03.2024
7.	Information Security	12.2018	24.03.2025
4.	Insider Threat Management	30.03.2026	
8.4	Policy on Security Information Sharing	30.03.2026	
2.9	Risk Assessment	12.2028	30.03.2026
2.10	Risk Control	12.2018	30.03.2026
0	General	12.2018	30.03.2026

Change revision summary

Part	Description of change
1.1.	Security Policy Statement revised
7.2	Added cross-reference to the DHS Data Protection & Information Security Policy (DPISP_V2_2025) for detailed IT security and data protection guidelines.
4.	New chapter added: Insider Threat Management. Covers definition and scope, risk indicators, radicalization awareness (EU 2015/1998), prevention measures, reporting and response procedures, and management responsibility. Chapters previously numbered 4–15 renumbered to 5–16 accordingly.
8.4	New section added: Policy on Security Information Sharing. Defines need-to-know principles, authorised recipients, conditions for internal and external sharing, and internal communication of security updates. Cross-reference to DPISP and Section 14.2.
2.9	Risk Assessment section updated. Cross-reference added to DHS SMS Manual Section 1.2 as Single Source of Truth for risk assessment methodology, tools, and review requirements. Standardised 5x5 Risk Matrix applies to all security risk assessments.
2.10	Risk Control section revised. Previous risk matrix (Monitor/Review/Unacceptable + ERIC-TD model) superseded. Section now references DHS SMS Manual Section 1.2.4–1.2.5 as Single Source of Truth for risk assessment methodology, matrix, and tolerability zones. Security risk assessments apply the same standardised 5x5 methodology.
0.2	Section expanded. New subsection added: Communication of Security Updates. Defines responsibility of SSTM for timely communication of amendments, communication channels (AvBIS, operational briefings, email), Station Manager responsibilities, and record-keeping requirements.

Contents

0 GENERAL

0.1. INTRODUCTION

This Security Manual contains key information in relation to DHS Security Policy and how that Policy should be implemented at operational level. As such, it is an important document that must be maintained according to the following procedures:

Line Managers should ensure that the Security Manual is:

- Legible.
- Accessible to those Managers who should be aware of its contents.

Line Managers should pay particular attention to any amendments to the Security Manual, which may require changes to local procedures.

The current version will always be available on AvBIS.

0.2. AMENDMENT RECORD INSTRUCTION

Line Managers should pay particular attention to any amendments that may require changes to local policies and procedures.

The current version will always be available on AvBIS, any printed versions of this document shall be classed as uncontrolled.

Communication of Security Updates

When amendments to this manual or related security procedures are issued, the Safety, Security & Training Manager is responsible for ensuring timely communication to all relevant staff. Communication shall be carried out through one or more of the following channels:

- Publication of the updated document on AvBIS with notification to Station Managers
- Operational briefings at station level, conducted by the Station Manager or delegated supervisor
- Direct communication via email to relevant operational staff where immediate awareness is required

Station Managers are responsible for ensuring that all relevant personnel within their station are made aware of security updates in a timely manner and that local procedures are adjusted accordingly. Where an update requires changes to operational practice, this must be confirmed to the Safety, Security & Training Manager.

Records of communication and briefings shall be retained at station level for audit purposes.

1 COMMITMENT OF SECURITY

1.1. SECURITY STATEMENT

Security Policy

Safety and security are a must and a non-negotiable requirement in our business. They are not optional extras. Employees are expected to act with integrity, honesty, and always in the best interest of DHS and our customers.

All levels of management are accountable to ensure that the security measures are implemented and adhered to by all employees. These will comprise (but not be restricted to) the following security guidelines:

- Always adhere to work instructions, policies, procedures, and training.
- Refrain from stealing or taking anything that is not yours, and report any lost property right away.
- Never engage in any form of fraud.
- Permits and ID cards should always be worn and displayed correctly. Lost permits and ID cards should be reported right away.
- Respect the Clear Desk Policy to the letter and take extra precautions to protect sensitive data.
- Never convene unapproved meetings on company property, in company-designated workspaces, or during company business hours.
- Ensure that uniforms, personal protective equipment (PPE), and any other materials or equipment issued by our company are properly maintained and returned to the company upon termination of employment.
- Always keep in mind that suspicions about something are frequently correct. Always report your suspicions!

When it comes to actions that might be considered gross misconduct, DHS has a Zero Tolerance policy.

Ingo Schnitger
CEO

V2R0_2024

1.2. HEAD OF SECURITY

Security is a fundamental operational priority and forms an integral part of the safety of civil air carrier operations worldwide. The primary objective of

International Civil Aviation Security is to assure the protection and safeguarding of passengers, crew, ground personnel and the general public. Each country regulates security through a National Aviation Security Programme (NaSP). Airports and carriers will have their own security programs to ensure the integrity of security systems. DHS is committed in doing its part in the support of aviation security and the security of the DHS business activities across our German network.

To support this commitment, this manual contains the generic (framework) policies and procedures that must be applied across all operations. It must also be noted that local, national (State) and carrier specific requirements may mean that additional security measures and procedures must be enacted in addition to the company's own security procedures. Where such measures contradict or conflict with DHS policy and procedures, advice should be sought from head office.

It is vital that all employees fully understand that they have an important role to play in the protection of aviation security, our customers, the company's employees and assets. Although this manual is sensitive (restricted), contents must be made available to those who have a need to know specific elements in order to carry out their role and responsibilities. Key elements must also be integrated into local procedures and training.

2 STRUCTURE AND RESPONSIBILITIES

This section sets out the main security responsibilities for the organisation.

2.1. LEGAL REQUIREMENTS

The International Civil Aviation Organisation (ICAO) was established by the Convention on International Civil Aviation, signed at Chicago, on 7 December 1944 (Chicago Convention). Its Contracting States have agreed on certain principles and arrangements in order that international civil aviation may be developed in a safe and orderly manner. ICAO provisions for international aviation security are disseminated as Annex 17 to the Chicago Convention.

The European Civil Aviation Conference (ECAC) was founded in 1955 as an Inter-governmental organisation. Its objective is to promote the continued development of a safe, efficient and sustainable European air transport system. ECAC AvSec standards and guidance are published in 'Doc 30'.

The European Union (EU) was established by the Treaty on European Union at Maastricht on 7 February 1992, and is founded on the European Communities, supplemented by the policies and forms of cooperation established by this Treaty. The European Community was created by the Treaty Establishing the European Community at Rome on 25 March 1957. EU AvSec regulations are published in 'EC 300/2008'.

On September 11, 2001, nearly 3,000 people were killed in a series of coordinated terrorist attacks in New York, Pennsylvania and Virginia. The attacks resulted in the creation of the Transportation Security Administration (TSA) in the United States of America (USA); designed to prevent similar attacks in the future. The

Aviation and Transportation Security Act, passed by the 107th Congress and signed on November 19, 2001, established the TSA.

Pursuant to the provisions of Article 37 of the Chicago Convention, International Standards and Recommended Practices on Security were adopted by the ICAO Council on 22 March 1974, and designated as Annex 17 to the convention with the title 'Standards and Recommended Practices – Security: 'Safeguarding International Civil Aviation against Acts of Unlawful Interference'.

ICAO Annex 17 must be applied in conjunction with regional and country specific laws and regulations.

The primary objective of International Civil Aviation Security is to assure the protection and safeguarding of passengers, crew, ground personnel and the general public against **acts of unlawful interference**.

It is the responsibility of all personnel to be able to instinctively respond to criminal acts and to acknowledge the necessity for security controls and standards.

2.2. SECURITY MANAGEMNET SYSTEMS

The Security Management System (SeMS) is a key element of our management's responsibility as set out above. The SeMS provide the security framework, security scope of work, security policies and management's commitment to integrate security into every element of our business. The philosophy of SeMS is a top-to-bottom culture that leads to the efficient provision of a secure operation.

As with any business plan, goals are set, levels of authority are established and as such the SeMS provides a formalised, risk-driven framework for integrating security into the daily operations and culture of our business. The SeMS enables management to identify and address security risks, threats, gaps and weaknesses in a consistent and proactive way to meet quality control measures.

2.3. SECURITY FRAMEWORK

The framework provides a focus for the development of the security management systems, following a top down approach: from the commitment of the CEO and Line Managers, through a framework which provides for all the business units in the group, inspired by the commitment to ensure legal compliance by all elements within the SeMS, with due regard for all principles applied and based upon our core security values.

2.4. SEMS COMPONENTS

The SeMS includes the following key components:

- Management commitment
- Structure and responsibilities

- Risk and threat management
- Policies and procedures
- Training, education and awareness
- Quality management
- Incident response and investigation
- Security toolbox

The effective implementation of the SeMS will ensure DHS has the ability to prepare for and react to events that may otherwise present a threat and ensure the most efficient use of resources at optimum cost.

2.5. HEAD OF SECURITY

The Head of Security is responsible for the implementation, supervision and control of the company security programme and policies. He/she will also ensure that the policies and security standards are applied consistently across all DHS operations. These standards will comply with or may exceed the standards demanded by our customers and/or the states in which DHS operates.

The Head of Security has direct access to the CEO, the station managers and departmental managers on matters of security and is authorised to use methods and techniques, as may be appropriate, to ensure that the security integrity of DHS is maintained and protected at all times.

The Head of Security is responsible for:

- The formulation of company security policy;
- The development of security standards and practices;
- Ensuring compliance with national and international requirements and regulations;
- Liaison with regulatory authorities, law enforcement agencies and government departments on security matters;
- Providing an effective risk analysis and threat assessment and response capability;
- Advising Directors and Managers on implementing security procedures;
- Advising on physical security issues pertaining to the operation of the company;
- The conduct of investigations into all matters that could impact on the operational security of the company;
- Investigation of any threat or acts of unlawful interference, or the failure of implementation of any security control;
- The development, implementation and maintenance of the DHS Security Programme and oversight of the implementation of security controls in the Local Security Programmes (LSP) at each station;
- To advise on all matters of training in aviation security;
- To supervise all systems and audits used for the monitoring of compliance and quality of security systems;
- Formulation and initiation of additional measures to be applied during periods of increased threat and operations of increased risk.

2.6. STATION AND DEPARTMENT MANAGERS

General, Station and Departmental Managers and supervisory personnel are responsible for ensuring that the security measures set out within the DHS Aviation Security Manual are applied consistently to the Operation within their departments by implementing a Local Security Procedure (LSP) in accordance with the Security Programme of customer airlines, airport authorities and the Civil Aviation Security Programme of States where operations are conducted. Also establish and maintain close liaison with regulatory authorities, law enforcement agencies and government departments on security matters.

They are responsible for monitoring the application and relevancy of security procedures. Where departments use contractors, it is the responsibility of those managers to ensure that contractors comply fully with the DHS Security Manual and any relevant National (State) regulatory requirements that may be applicable.

Third party suppliers are to be held responsible for ensuring the DHS Security Management Systems are adhered to. Local management must make provision for this in any contract or agreement. Contracting third parties shall also incorporate measurable performance indicators in areas of security compliance.

Third party contractors and suppliers will be subject to regular audits and checks to ensure they are complying with the above.

All managers will have direct access to the Head of Security via the direct reporting structure, on matters of security, should the need arise and as may be appropriate.

For procedural requirements related to subcontractor safety, training and documentation, refer to Chapter 5 of the DHS SMS Manual.

2.7. MANAGERS RESPONSIBILITY FOR SECURITY

Each station will nominate or appoint a Principal Manager who is accountable for matters relating to Security at the station. Security accountabilities must be clearly defined in the appointed person's job description and be identified on the Station Management Organisational chart or diagram. The accountable Manager is responsible for overseeing and implementing the Security Programme and implementing all elements of the Security Management System at a local level and ensuring that the applicable regulatory and airport security regulations are adhered to. They will be responsible for driving initiatives aiming to achieve at least a 10% reduction in Security related incidents at the station year on year and will act as the representative of DHS at any airport committee, steering group or forum where Security is an agenda item.

For safety-related accountabilities and the role of Health & Safety Officers, refer to Sections 0.5 and 0.7 of the DHS SMS Manual.

2.8. SECURITY MANAGEMENT (PROACTIVE)

Security management involves identifying areas of vulnerability and implementing measures to eliminate or mitigate exposure. Security measures should

be appropriate to the risk level; the risk is determined by continuous assessments of the threat measures against the likelihood that we are exposed to a vulnerability (i.e. Risk = Threat x Vulnerability). Ensure that the level of security matches the value of the assets and the severity of the threat.

Risk = Threat x Vulnerability

2.9. RISK ASSESSMENT

Risk assessments must be performed by a competent, trained person. Risk assessments must be done if there is a significant change in operations; when an incident occurs where there was an event outcome or potential outcome; and,or when a vulnerability is identified.

As a minimum, a planned security risk assessment must be done once a year per station. All risk assessments must be completed using the DHS Risk Assessment Template.

Security risks are not limited to specific tasks or processes and risk assessment of DHS property, offices and operational areas must also be included in the risk assessment portfolio.

Risk assessments should be reviewed:

- When new facilities, work practices or security equipment are introduced;
- Following a security incident where there was an event outcome or potential outcome;
- Periodically to ensure they are still fit for purpose.

Risk assessments shall be conducted using the standardised 5x5 Risk Matrix (Severity A-E x Probability 1-5) and Tolerability Zones as defined in the **DHS SMS Manual, Section 1.2.** The SMS Manual Section 1.2 serves as the Single Source of Truth for risk assessment methodology, tools, and review requirements across all DHS operations.

2.10. RISK CONTROL

Once the risk assessment is complete, the risk level is determined by combining the Probability and Severity of the identified hazard using the DHS standardised Safety Risk Matrix. The resulting Safety Risk Index (SRI) determines the Tolerability Zone and required response.

The risk matrix, Tolerability Zones (Intolerable / Tolerable ALARP / Acceptable), severity and probability scales, response timelines, and risk acceptance authority are defined in full in the **DHS SMS Manual, Section 1.2.4–1.2.5**, which serves as the Single Source of Truth for risk assessment methodology across all DHS operations. Security risk assessments shall apply the same methodology.

2.11. RISK MANAGEMENT

The risk assessment is used to address risks; protect employees, assets and reputation; assist in prioritising resource allocation; and to act as an early warning system. Station Management must provide a corrective action plan to indicate how the risk will be mitigated, who the responsible person(s) will be and a date by when the action will be completed. It is management's responsibility to drive the process until all corrective action requests have been completed satisfactorily. Mitigating measures must be robust yet practicable (feasible), balanced against the risk and cost effective.

For a comprehensive overview of the organizational risk management process, including hazard identification and mitigation strategies, refer to Section 1.2 of the DHS Safety Management System Manual (SMS).

2.12. SECURITY MANAGEMENT (REACTIVE)

Realistically security may never be 100% due to the changing nature of threats. It is important that security procedures and systems remain robust and effective. On occasion, management will have to react to an incident. Procedures must be in place to handle security incidents and avoid operational disruptions in as far as possible. Security incidents must be reported, investigated and corrective actions managed.

2.13. INCIDENT REPORTING

Local operational and/or security Management must report and investigate all Security related incidents and/or breaches using the Safety Culture System, following the DHS Category Classifications. For serious CAT A or D security incidents, management shall immediately notify the CEO and SSTM.
See DHS – Investigation Basic Principles document for investigation guidance.

Reporting procedures must further be in accordance with the requirements of customer airline(s) and the civil aviation security programme of states. Reportable incidents include but are not limited to: crime, regulatory breaches or infringements, threats & acts of unlawful interference.

2.14. WHISTLE BLOWING

Where employees have concerns about security they should be encouraged to report concerns, either to management, or in using the Safety Culture barcode posted in every office. The tool provides an independent, confidential reporting service that any DHS employee can use to report non-compliance with company policy and ethical requirements.

We always encourage those of you who may have a concern to first speak with your manager. If, however, you believe an issue about dishonesty or malpractice within DHS needs investigating but feel uncomfortable using the usual channels, then you should use the Safety Culture tool.

This whistle-blower tool aims to address serious concerns related but not limited to:

• Criminal activity of any kind
• Failure to comply with a legal obligation.
• Miscarriage of Justice.
• Danger to Health and Safety or the Environment.
• Financial malpractice or fraud.
• Improper conduct or unethical behaviour.
• Attempts to conceal any of the above.

2.15. DISCIPLINARY PROCESS

Employees are expected to act with honesty, integrity and in the best interest of DHS at all times. The disciplinary process must be managed and management should create a climate whereby employees are aware of and willingly adhere to the rules and norms of the company. Unacceptable behaviour must be corrected by applying a process of discipline.
The disciplinary process must be fair, impartial and reasonable. Emphasis must be placed on strict compliance to the Company procedures and whether just cause is established to institute disciplinary action.

When conducting an enquiry for misconduct, consideration should be given to:

• Whether a rule, regulation or a standard was contravened?
• If a rule, regulation or standard was contravened, it should be determined whether it was valid and/or reasonable.
• Was the person aware, or could reasonably be expected to have been aware of the rule, regulation or standard?
• Was the rule, regulation or standard consistently applied?

Care and concern should be taken to ensure that our people are treated with respect and that we are fair and consistent in our approach in dealing with employees.

For further information on accident investigation, reporting culture, and internal reporting obligations, see Sections 0.8 to 0.11 of the DHS SMS Manual.

2.16. SECURITY CULTURE

Security is not the sole responsibility of top level management, or the appointed security persons' task. Security involves everyone and a positive security culture is essential in promoting and maintaining a secure work environment. To promote good security practice, line management need to visibly promote security at all times in complying with the law, as well as the security policies and procedures of the company, clients, airports and local authorities.

Senior Management	Line Managers	Employees
• Fully comitted to security policy and procedures. Encourage employees to be loyal and comitted by setting a postive example.	• Taking responsibility for maintaining and implementing procedures. Set a positive example. Often first to notice unusual behaviour take action: • Intervene to prevent problems becoming serious. • Provide support and report it.	• Must be made fully aware of security responsibilities. • Receive security induction and refresher training • Continously made aware of threats and the role they have in keeping their workplace secure. • Encourage to report openly (just and fair).

It is the Policy of DHS to engage positively and support the aims of regulatory powers and local control authorities in matters of security. DHS actively encourages its management to establish relationships with other businesses and security organisations to promote intelligence sharing to promote a collaborative, coordinated approach to security.

For leadership commitment and integration of safety culture within DHS operations, refer to Section 0.6 of the DHS SMS Manual.

3 RECRUITMENT AND TRAINING

3.1. RECRUITMENT

The development of a security culture begins at the hiring process.
ICAO Annex 17, Standard 4.2.4 and German law §7 LuftSiG requires that background checks must be performed and any inactive periods should be clarified by the candidate. As such, all personnel must undergo security clearance checks to ensure that their honesty and integrity is appropriate to allow them access to security restricted areas and airport critical parts.
A background check should not be limited to only verifying a candidate's criminal past. Vetting and background checks must fully comply with any guidelines or requirements specified by the Airport of Operation. This procedure must be fully adhered to when employing full time, part time, temporary or agency staff.
The screening of applicants must be carried out before they are offered any form of contract or employment and the applicant must sign on the form that they have no objection to the pre-employment screening process.
If an applicant refuses to participate in the screening process they will NOT be offered employment with DHS. Records of pre-employment checks must be maintained against each employee's personal record (i.e. file). As per current regulation a background checks should be repeated every five years.

3.2. JOB DESCRIPTION

All job descriptions must outline that safety and security is everyone's responsibility and a signed copy must be held on the personnel file.

For job descriptions refer to SQM 1.2.

3.3. TRAINING

The security training programme must be in accordance with the Security Programme of customer airlines, requirements of the civil aviation security authority of states, and requirements of the airport authority at stations where ground operations are conducted. The training program must include initial and recurrent training, and have a balanced curriculum of theoretical and practical training to ensure:

• The proper implementation of security controls and that personnel have the competence to perform their duties;

• Through security awareness training, ground handling personnel are acquainted with preventative measures and techniques in relation to passengers, baggage, cargo, mail, equipment, stores and supplies intended for transport on aircraft, as applicable, so they may contribute to the prevention of acts of sabotage and other forms of unauthorised interference.

Refer to the DHS Training Policy Manual for further guidance.

3.4. STAFF ENGAGED IN OPERATIONAL DUTIES

All DHS staff will receive the required security training necessary for the role they are to perform before taking up their duties, which also applies to ALL part- time, temporary or agency staff.

ICAO Annex 17 Standard 3.6.1 requires each contracting state to implement a security training programme to enable staff to effectively operate the national security programme.

Staff performing security related duties must meet the National Aviation Security Programme (NaSP) requirements of each Country of Operation. Refresher training must fully comply with any guidelines or requirements specified by Luftfahrtbundesamt (LBA).

3.5. BASIC SECURITY AWARENESS TRAINING

DHS – Basic Security Awareness Training (BSAT)

The training applies to the protection of assets from internal and external interference and the necessity of ensuring all ground handling personnel have a positive attitude to security. All operational personnel will undergo the DHS Basic Security Awareness Training (BSAT) as part of their induction training, adapted to comprehensively cover local security process and procedures. This

training must fully comply with relevant legislation or guidelines set in the Country or Airport of operation. The principal aim of such training is to promote awareness of security issues and threats and to understand security responses and increase vigilance. Subject to local regulatory requirements, refresher training will be conducted at intervals of no longer than 36 months.

LBA 11.2.6. Aviation Security Training (Luftsicherheitstraining)
This training applies to all operational personnel who require unescorted access to security restricted areas to perform their duties.
Subject to local requirements, refresher training will be conducted at intervals of no longer than 60 months.
When using external training companies, only companies that have been accredited by LBA, must be used.

Module Safety/Security Culture

On Dec. 31, 2021, new training requirements under EU law on "safety culture" were introduced for all training under Chapter 11.2 of the Annex to Implementing Regulation (EU) 2015/1998. According to this knowledge of "elements that contribute to building a robust and resilient safety culture in the workplace and aviation sector, which include insider threats and radicalization, among others" is demonstrated. The Safety Culture module is integrated into the 11.2.6 Aviation Security Training from 1.1.2021.

Copies of the institute's certification should be retained for audit purposes.

3.6. TRAINING RECORDS

Records of all initial and refresher training; stipulating the subjects covered and the date of the training; must be maintained by the training department for inspection. Records of initial and refresher training must be kept on the training personnel file. Be aware that sub-contractors, must comply with the standards as set by DHS, customer airlines and state of operations.

"For SMS-related training components, documentation requirements and refresher procedures, refer to Section 3.1 of the DHS SMS Manual."

3.7. AUDITING OF EMPLOYEES PERSONNEL AND TRAINING FILES

To ensure regulatory compliance, employee files must be audited on a regular basis (at least once per annum) to ensure continuous compliance. The auditor must ensure that regulatory requirements are met in terms of the employment processes, which should include:

- Background checks,
- Right to work checks,
- National Identification verification,
- Training records,
- Signed and up to date Job description,
- Signed and dated employment contract, and

• Where required, a valid driver's licence.

It is a requirement that DHS Human Resources must perform an annual audit of 10% on the total of employee files and a record of such an audit must be made available to the auditor. All personnel files must be kept in a secure location, with access restricted to authorised personnel only. Any issues of either a regulatory or criminal nature must be escalated to the CEO and Head of Security immediately.

4 INSIDER THREAT MANAGEMENT

4.1. DEFINTION & SCOPE

An insider threat arises when a current or former employee, contractor or trusted individual uses their authorised access to DHS facilities, systems, personnel or information in a manner that could harm the organisation, its customers, or the safety and security of aviation operations. Insider threats may be intentional (malicious) or unintentional (negligent or coerced).

DHS recognises that insider threats represent one of the most significant vulnerabilities in aviation security, consistent with the requirements of ICAO Annex 17, EU Regulation (EC) 300/2008, and Chapter 11.2 of the Annex to Implementing Regulation (EU) 2015/1998.

4.2. RISK INDICATORS

Managers and employees must remain alert to behavioural and situational indicators that may suggest an insider threat. These include, but are not limited to:

- Unexplained access to restricted areas outside of assigned duties
- Unusual interest in security systems, procedures or colleague access credentials
- Sharing of sensitive operational information with unauthorised persons
- Signs of financial distress, coercion or unusual lifestyle changes
- Expression of views supporting unlawful interference, violence, or extremist narratives, or sudden concerning behavioural changes
- Repeated or deliberate violation of security procedures
- Removing or copying sensitive documents without authorisation

The presence of one indicator does not constitute evidence of insider threat activity. Patterns of behaviour should be considered in context and reported to the Safety, Security & Training Manager.

4.3. RADICALIZATION AWARENESS

In accordance with EU Regulation 2015/1998, Chapter 11.2, DHS requires all operational personnel to be aware of the risks of

radicalization in the workplace. Radicalization is a process by which an individual comes to adopt views that could lead to acts of unlawful interference or terrorism.

DHS managers must:

- Be trained to recognise early indicators of radicalization
- Create an environment in which employees feel safe to raise concerns confidentially
- Respond to concerns through established reporting channels without prejudice to the individual concerned until facts are established

Radicalization awareness is integrated into the DHS Basic Security Awareness Training (BSAT) and the LBA 11.2.6 Aviation Security Training (Safety/Security Culture module).

4.4. REVENTION MEASURES

DHS applies a layered approach to insider threat prevention:

- Pre-employment background screening in accordance with Section 3.1, including five-yearly renewal
- Role-based access control limiting airside and system access to operational necessity
- Regular audit of personnel and training files per Section 3.7
- Enforcement of the Clear Desk Policy (Section 7.1) and IT security controls (Section 7.2)
- Periodic review of airside ID card holders to confirm ongoing operational need (Section 4.3)

4.5. REPORTING AND RESPONSE

Any employee who identifies behaviour consistent with an insider threat must report it immediately using one of the following channels:

- Direct report to their line manager
- Report to the Safety, Security & Training Manager
- Confidential report via the Safety Culture reporting tool (refer to Section 2.14 — Whistle Blowing)

Reports will be treated in strict confidence. Retaliation against any employee making a good-faith report is a disciplinary offence.

Upon receipt of a credible insider threat report, the Safety, Security & Training Manager will assess the situation, implement proportionate access control measures, and where appropriate inform senior management, relevant airport authority, or law enforcement in accordance with Section 14.

4.6. MANAGEMENT RESPONSIBILITY

Station Managers are responsible for ensuring insider threat awareness is embedded in local induction, refresher training, and daily supervision. Security accountabilities relating to insider threat are to be reflected in relevant job descriptions in accordance with Section 3.2.

5 ACCESS AND EGRESS CONTROL

Most of our premises are provided by the airport or are situated in Custom bonded areas, or we rent private property. It is imperative that the Station Manager ensures the minimum security requirements are adhered to and any concerns, irregularities should be reported to the landlord and/or their security representative.

All property occupied by DHS, must have suitable measures to restrict access to authorised persons only. Entry points should be controlled by the use of an electronic entry system where applicable. Where no electrical system is available and key system is used, the station manager must ensure a control mechanism is impin place.

5.1. KEY CONTROL PROCEDURES

A copy of all keys must be stored in a secure lockable safe or cupboard to which only the most senior manager, or a designated person appointed to the responsibility, have access. Safe keys may not remain in locks when not in use and neither may the safe be left open when not in use or returned to the Airports Office. All offices in the public area shall be locked when not in use. All offices in the restricted area should be locked when not in use during working hours. After working hours, all offices in the restricted area shall be locked. Lost keys must be reported to the manager immediately and appropriate measures must be put in place to secure the area and where required to replace the lock.

5.2. PHYSICAL SECURITY OF DOORS AND GATES

In the event of a key or locking mechanism being compromised, arrangements must be made to replace, or update the locking mechanism.
Security doors are only effective when shut and secured; therefore DHS operates a closed door policy. When doors are not in use they must be closed. When doors are left open for operational or maintenance purposes, they must be attended at all times.

5.3. AIRPORT ID AIRSIDE CARDS/BADGES

Where it is necessary for airside ID cards to be issued, DHS will comply with the procedures of the issuing authority. Holders of airside ID cards will be reviewed and

where there is no longer an operational need for a person to hold an airside ID card, that ID card will be withdrawn.

In the event of an identity card being lost, the person to whom it is issued must report it to their line manager who will notify the authorised signatory or security manager who will arrange for the ID card to be withdrawn. Where crime or a security breach is suspected, the matter will be reported immediately to the Police or relevant authority and the airside identity card must be parked.

In the event of the loss of an airside identity card, the person to whom it was issued will report it immediately to the issuing authority, their line manager and if required to the Police. The airside identity card must be returned to the Airports office (Ausweisstelle) when an employee terminates employment.

All persons issued with an airside identity card will at all times conform to the conditions of its issue as stated by the issuing authority. Airside identity cards may only be used for work related activities and not to bypass security for personal use. Also, when employees are on duty travel they may not use their airport ID cards to bypass security screening of themselves or their baggage (checked or cabin baggage) before they embark an aircraft. They must proceed through the normal passenger security screening channels.

Should an employee be found in contravention of these laws, they will be disciplined and may face prosecution by the local authorities.

5.4. VISITORS

Where visitors are visiting a DHS property within a controlled area of an Airport, the procedures for that airport will be strictly adhered to.
All visitors to DHS occupied properties will be required register upon entering and leaving the property. They will be identified by a member of DHS staff who will take responsibility for them for the duration they are on site.
Visitors will be under the supervision of a member of DHS staff at all times whilst on the property. Access to areas sensitive to the safety and security of any DHS operation, will be kept to a minimum and restricted to those persons who have a need to be there.
If airside areas have to be visited (e.g. airline auditor), an airport visitor's pass is applied for at the respective airport by the station manager.

6 DUTY OF CARE AND PERSONNEL SECURITY

6.1. OFFENSIVE WEAPONS

In order to make the workplace a safe and secure environment for all DHS staff there is a prohibition on bringing firearms, or any other offensive weapon, into the workplace (includes break rooms).

6.2. VIOLENCE IN THE WORKPLACE

Violence in the workplace is not limited to physical attacks, but also includes verbal abuse and insults. DHS adopts a policy of zero tolerance when such acts are committed against its employees.

At DHS, we strive to provide a polite and courteous service whilst helping to address any concerns that customers may have. Verbal or physical abuse will not be tolerated, and must be reported to management.

6.3. EMERGENCY EVACUATION

Emergency Evacuation Procedures in identified stations must be put in place by the Station Manager taking into account local requirements. All employees must be trained on fire safety and emergency exits at the appropiate airport.

7 FINANCIAL PROTECTION

7.1. CASH AND CREDIT CARD HANDLING

The main purpose of a cash and credit card procedure is to prevent theft and fraudulent transactions which can also have a negative impact on the good reputation of the Company (where the term cash is used, it will also refer to petty cash and cash equivalent items). This policy must be applied across all operations where cash or credit card transactions take place within DHS operations (e.g. Ticketing Offices, Check-in Counters, Boarding Gates, Lost Property Offices, ad hoc charters etc.).

It must be noted that, where applicable, carrier specific requirements and other local procedures relevant to cash and credit card handling, must be implemented.
Airline procedures must be followed, but where there are no procedures in place, a local procedure must be developed. The security responsible person must do a proper risk assessment on each area in order to provide local management with guidance on measures and procedures that will mitigate identified risks.
It is vital that all employees fully understand they have an important role to play in the protection of our customers' interest and in protecting the Company's assets. Local procedures and training must be developed and provided to those employees to enable them to carry out their responsibilities.
All transactions must be recorded correctly and accounted for at all times. All financial documentation must be kept in a secure place and must be accessible for audit purposes. It is part of the DHS Managers "duty of care" to the company, passengers and customers to comply with this policy and to adequately protect and apply appropriate measures to facilitate this process when handling cash and credit cards for the various services provided.

7.2. THEFT OR ACCOUNTING DISCREPANCIES

In the event of any monies being stolen or the accounting system being subject to suspected fraud the Ceo and Security Manager will be informed immediately and a thorough investigation conducted. In accordance with the DHS zero tolerance policy relating to theft and fraud, internal disciplinary procedures will be applied and where appropriate, the Police will be informed and DHS will assist in the investigation.

8 INFORMATION SECURITY

By its very nature, security documentation must be controlled. The rules for handling and disseminating this material are written in each individual Country's National Aviation Security Programmes (NaSP).
Internal security documents will be held in a secure shared drive. Where required by law, paper formats must also be held and must be controlled by the responsible manager and audited by the regional security manager.
Paper copies will only be issued where it is necessary for the efficient running of the operation. Paper copies will not be amended. When a paper copy of any documentation is no longer required it shall be destroyed by means of shredding or secure waste disposal.
Whilst the DHS security manual is of a sensitive nature, it must be remembered that this is an operational document and it must be available to persons having an operational need to be aware of its content. Electronic copies of documentation will have distribution limited to those who require access to it.

8.1. CLEAR DESK POLICY AND HOUSEKEEPING

All operational security, commercial and financial documentation and valuables (e.g. mobile phones, cash boxes, laptops, barcode readers, radios, etc.) should be stored in locked facilities when not in use. This is the basis of the 'clear desk' policy. No sensitive documentation will be left out on unattended desks. Supervisors and managers are required to frequently check office desk space and remove confidential, restricted and/or sensitive documents.

Housekeeping is the general care, cleanliness, orderliness, and maintenance of our operational work areas. Good housekeeping is an important consideration to prevent fire hazards, criminal activity and injuries.

8.2. INFORMATION TECHNOLOGY SECURITY

Information Technology systems must be secured to reduce cyber risks and preventative measures must be in place to reduce unauthorised disclosure or loss of information.
Access to the network must be limited to those persons who have a requirement to access it to carry out their duties. Persons with access to the network must use secure passwords and everyone must be made aware that passwords may not be shared. All e-mails coming into the system should be screened to

prevent 'Spam' mails (unsolicited e-mails which could also contain malicious programmes).

Network users must be briefed as to the importance of keeping the network secure. All employees must be made fully aware of their legal responsibilities with respect to their use of computer based information systems and data. When operators leave workstations unattended, they must log off from the network. Passwords that has been compromised, or a possibility exists that the network has been penetrated, it must be reported immediately to the Security Manager.

For detailed guidance on data protection, IT access control, phishing prevention and GDPR compliance, refer to the DHS Data Protection & Information Security Policy (DPISP).

For company-wide document control processes and distribution responsibilities, refer to Section 0.13 of the DHS SMS Manual."

8.3. SOCIAL MEDIA

Employees should be aware that they must not use their personal social media accounts to make comments or publish articles which risk damaging the reputation of DHS, the Airline Customer, the Airport or other third parties. This includes but is not limited to political statements in forums where professional status is highly visible, such as LinkedIn. Statements regarding customers, airports, and their operations or practices and any statements which imply the employee is speaking on behalf of DHS. Employees must be authorised by the senior leadership team before making any such postings on any Social Media plattform.

8.4. POLICY ON SECURITY INFORMATION SHARING

Security information must be shared on a strict need-to-know basis. The dissemination of security-related information is governed by the sensitivity of its content, the operational role of the recipient, and applicable legal requirements.

Authorised recipients

Security information may be shared with the following parties, subject to the conditions set out below:

- DHS management and operational staff, to the extent required to carry out their duties
- Customer airlines, where sharing is required under the terms of the ground handling agreement or carrier-specific security programme
- Airport authorities and regulatory bodies, where required by law or formal request
- Law enforcement agencies, in accordance with national legal requirements
- Third-party contractors and suppliers, limited to information necessary for the performance of contracted security-related duties

Conditions for sharing

- Security documents classified as sensitive or restricted may not be shared without prior authorisation from the Safety, Security & Training Manager
- No security information may be communicated to media or public channels without explicit approval from senior management
- Sharing of security information with external parties must be documented where practicable
- Where security information contains personal data, sharing must additionally comply with the DHS Data Protection & Information Security Policies (DPISP)

Internal communication of security updates

Updates to security procedures, threat levels, or regulatory requirements must be communicated to relevant staff in a timely manner by the Safety, Security & Training Manager or delegated Station Manager. Communication channels include operational briefings, AvBIS document updates, and the SafetyCulture reporting platform.

For confidentiality obligations in the event of a security incident, refer to Section 14.2.

9 LOST AND FOUND PROPERTY

When dealing with items of property found in areas where DHS staff are working, consideration must always be given to the fact that the item may not be what it seems.
If an item appears out of place, has signs of tampering or appears unusual in any way, it must be treated as a 'suspicious item'. Do not touch or move it, call for the duty manager and invoke local procedures for dealing with such an incident. If a suspect item is found on board an aircraft or in a facility not owned and managed by DHS, the duty manager for the airline or facility must be contacted and take responsibility for dealing with the incident.
A system to register property and other items, including the means of disposal must be maintained with formal sign-off controls.
If the item is found on DHS premises, then it becomes the responsibility of DHS to deal with in accordance with local procedures.

9.1. PROPERTY FOUND ON AIRCRAFT

Any item found on an aircraft by DHS staff will be left where it is found and a representative of the airline contacted and requested to take charge of it. The operator of the aircraft has the responsibility to deal with such incidents and is usually better placed to trace the owner. DHS staff must be aware of any local procedures in force and comply with them.
Carrier specific lost and found procedures must be followed. A gap-analysis must be done with the airline's procedures and any gaps identified must be raised in writing with the customer airline. Should they not agree to implement more robust measures, it must be placed on record in the airline file. Where

no procedure is available, the DHS Lost & Found Property Procedure must be followed.

9.2. SUSPICIOUS ITEM

Confirm

- Check the apearance of the item and the surrounding area to confirm that the item does not belong to any persons in the near vicinity
- Confirm the items exact location, its appearance and mark its position
- Do not touch or attempt to move the item
- If in doubt always treat the item as suspicious

Clear

- Asses the surroundings and clear all persons from the danger of the suspicious item

Cordon

- Establish a cordon or physical barrier to prevent anyone gaining access to the cleared area of danger
- A cordon should have one entry point. Anyone seeking access to the cordoned area must be directed to the single point of entry
- The police may a further outer Cordon on access routes

Control

- Inform your airport security, local police, supervisor, line manager to take control of the situation
- Remain available to threat assesors, Police or other agencies to assist with any enquiries
- Follow local procedures for responding to suspicious item incidents

For any suspicious mail items, these additional checks must be done:

• Check if the sender's name and address are given, try to contact them to confirm the dispatch of the letter or package and to validate its contents.
• Check for the following indicators:

- Any unusual smell
- Delivered by hand or an unknown source
- Excessive wrapping, tape or staples
- Too many stamps for ist weight
- Came from unexpected source
- Envelope or package heavy for its size
- Weight distribution uneven
- Visible wire or tin foil
- Poor handwriting, spelling or typing
- Wrongly addressed
- Grease marks on the envelope or wrapping

Suspicious items must be evaluated and a common sense approach should be adopted which should give you a good idea of the likely threat and the precautions needed to be taken.
Suspicious items may be explosive or incendiary (the two most likely kinds), or chemical, biological or radiological. A letter / parcel bomb will probably have received fairly rough handling in the post and so is unlikely to detonate through being moved, but any attempt at opening it, however slight, may set it off.

Additional actions for chemical or biological suspect packages:
• Close windows and doors to room;
• If possible switch off air conditioning;
• Isolate person who opened the package, and those in room at the time
Although any suspect item should be taken seriously, remember most will be false alarms, and a few may be hoaxes. Try to ensure that your local procedures are not needlessly disruptive.

Take the following into account in your planning:
• Ensure everyone has access to emergency contact numbers (internal and external).
Ensure that everyone with a desk phone has access to the Bomb Threat Check Sheet – either in print or on their PC:

DHS

Bomb Threat Check Sheet (for completion by recipient of call)

Date:	**Time:**		**Person receiving call:**			
Your Tel no:			**Location where call received:**			
Exact message:						
Where is the Bomb?	Terminal	Cargo Area	Aircraft	Flight No.	Offices	Other
Was the caller familiar with the location given?			YES	NO		
When will the device explode? Enter given time:				Enter given date		
What does it look like?						
(Circle and write information above)		Briefcase	Parcel	Suitcase	Box/Bag	Other
Who are you? enter reply						
Why are you doing this? enter reply						
Where are you now? enter reply						
Caller's identity – circle as appropriate		Male	Female	Age (approx.)		
Voice characteristics – circle as appropriat		Loud	Soft	Deep	Rasping	Pleasant
		High pitch	Intoxicated	Other		
Accent – circle as appropriate			Local	Regional	Foreign	Other
Command of language – circle as appropriate			Excellent	Good	Fair	Poor
List any slang or colloquialisms used						
Speech – circle as appropriate		Fast	Slow	Distinct	Stutter	Nasal
		Distorted	Slurred	Other – list		
Manner – circle as appropriate		Calm	Angry	Rational	Irrational	Coherent
		Incoherent	Obscene	Deliberate	Emotional	Righteous
		Laughing	Proper	Other- list		
Background noise – circle as appropriate		Chaos	Quiet	Trains	Aircraft	Music
		Animals	Street traffic	Office	Party	Voices
		Other - list				
Could you obtain the number?			YES	NO		

DOM_V1.Rev0

10 AIRCRAFT PROTECTION

ICAO requires air carriers to produce Air Carrier Security Programmes. These detail the procedures that must be carried out to protect their operation and personnel (including passengers). Air Carriers will issue either a copy of the complete programme or relevant sections of the programme to DHS to enable staff to comply with the programme.
Although the security of the aircraft remains the responsibility of the Air Carrier, as their Ground Service Provider some security functions will fall to DHS as part of the standard ground handling agreement (SGHA).

DHS must comply with the Air Carrier's requirements as well as with the local regulatory requirements were security functions are subcontracted to the ground handler. Station Managers must ensure they have a full understanding of the clients' requirements on security issues. Remember that security will be regulated by the clients' own state and failure to comply will not only expose the operation to unnecessary risk, but may also lead to sanctions against the client or DHS.

10.1. SECURING OF UNATTENDED AIRCRAFT

In the absence of client procedure for an aircraft not in service and unattended, hold and cabin doors must be closed; steps and other equipment removed and where applicable, the jet way (Air Bridge) must be withdrawn to prevent unauthorised access to the cabin and holds.
The last authorised person leaving an aircraft must have either secured the aircraft in accordance with carriers' requirements or have applied tamper evident seals as required. In addition, where tamper evident seals have been used, the seal numbers will be recorded along with its location on the aircraft.
When access to the aircraft is required, the authorised person shall check the seals for tampering and will confirm the numbers correspond to those in the register.
Where seals are found to have been tampered with or the serial numbers do not reconcile, or if there is reason to believe unauthorised access to the aircraft was gained, the airline must be contacted immediately. There may be a further requirement to report the security breach to the regulatory authority of the country concerned.
A search of the aircraft will be undertaken by air crew and/or trained approved ground staff sufficient to reasonably ensure no prohibited articles, or any other article of concern, is on board the aircraft.

This search shall include:

• A thorough visual and physical inspection of the interior of the aircraft and its fittings.
• An inspection of accessible hatches and service panels, undercarriage wells, and areas under control surfaces.
• An inspection of all life jacket pouches.

10.2. CONTROL OF ACCESS TO AIRCRAFT

Access to an operational aircraft must be restricted to the following persons:
• The operating crew members of the aircraft.
• Persons acting in the course of a statutory duty such as Police, Customs and Immigration Officials, Department of Transport, Civil or Federal Aviation Authorities.
• Authorised staff of the carrier who have an essential operational need to be on the aircraft.
• Essential service providers, such as catering suppliers, specifically appointed for the task by the carrier.
• Passengers, on production of a boarding card for that flight provided they have been screened in accordance with local requirements

All persons other than passengers must be in possession of a valid airside identity card, or an official airline identity card. Note: Law enforcement and control authorities may use their official identity documents, DHS staff should be familiar with the appearance of such documents and where validity is in question, and advice should be sought from management or airport security.
DHS staff employed in duties on board or around the aircraft should stop and challenge persons attempting gain access and request to see their identification card.

Any unauthorised persons must be reported to airport security. DHS staff employed on gate duties must ensure when boarding passengers, the boarding card is correct for that particular flight and when cross checked with a passport or travel document, the passenger is in fact the person to whom the boarding pass was issued – if there is any doubt the passenger should be placed to one side while further checks are completed.

11 PASSENGERS

11.1. CHECK-IN

Terrorists or other perpetrators may target the check-in areas using explosive devices or armed attacks. All staff should visually check their area to ensure no unaccounted items are in the area that should not be there. Staff should remain alert during the check-in procedure and report suspicious behaviour and items left unattended (refer to Section 14).

11.2. TRAVEL DOCUMENTS AND VARIFICATION

Reasonable checks are to be taken to confirm the identity of every passenger intending to board an aircraft and passengers must produce an acceptable form of government issued identification. Where there is any doubt about the validity of any documents produced, the acceptance of that passenger should be suspended until the matter has been resolved.
Travel documents must be checked as follows for the flight(s) concerned (including onward travel):

• Validity of the ticket with regards to itinerary, flight, date, carrier, reservation status, class, and restrictions.

• Confirm the final destination with the passenger.
• Verify the passenger's identity against the travel document presented, including review of date of birth, expiry status of document (most countries require passports to be valid for no less than six months upon arrival), a visual comparison of the photo to the passenger, and ensure the name on the travel document matches the booked name.
• Verify the travel document is valid and good for all persons traveling, as not all States allow family members to be registered in a single passport.
• Report any document that shows signs of tampering (i.e. possible fraudulent documents which can be detected with the naked eye).
• Locate the passenger in the Departure Control Systems (DCS) and review any special remarks (e.g. this will include Timmatic or airline specific travel advice guidance).
• Check travel documents for destination and/or transit requirements.
• Review Visa or entry conditions or limitations such as but not limited to: check the visa is valid for destination and transit points; ensure the visa has not expired; check the visa dates matches with the dates of travel.
• Collect Advanced Passenger Information (API) if required. The data is collected by the authorities of each country and used for law enforcement purposes.
• When you identify an issue with a document, notify your supervisor who will contact the appropriate authority for assistance.
• Confirm each passenger's boarding acceptance in the DCS before allowing them to board.

DHS shall not be liable for immigration fines issued for falsified travel documents (i.e. fraudulent travel documents that cannot be detected by the naked eye) or other events which are outside of their control (e.g. passenger switching passports or destroying their passport, traveller being denied entry due to criminal record, or not having enough funds, etc.).

11.3. PASSENGER BOARDING

When preparing the boarding gate, staff must ensure that the boarding facilities and gate monitors are displaying the correct flight information. The area must be cordoned off with tensa barriers to prevent unauthorised access to the aircraft and airside areas. The Dangerous Goods and Prohibited Articles notices must be displayed at the boarding gate and ensure that airline stock is out of reach from unauthorised persons and not left unattended.

Once boarding commences, each passenger's identity must be verified and confirm boarding acceptance in the DCS before allowing them to board. For manual or non-automated boarding, check the flight number and date on the boarding card. Secure the flight by matching the checked–in passengers to the boarded passengers. Ensure the final checked-in count matches the boarded passenger count prior to door closure.

When there are passenger discrepancies (minus or plus), they must be resolved prior to closing the aircraft door. Apply airline procedures and government regulations with respect to the removal of checked baggage of passengers who have checked-in but

fail to board the aircraft. The same applies to baggage of passengers who were offloaded from the flight.

Flight documents (electronic or paper files) must be retained as per airline procedures and for a period of no less than three months unless otherwise specified.

11.4. SECURITY OF DOCUMENTS

All materials used for passenger and hold baggage processing (e.g. boarding passes, baggage tags, FIMs, vouchers, stamps, etc.) must be protected or be under surveillance at all times in order to prevent unauthorised access and use.

Departure Control Systems (check-in systems) must be controlled to prevent unauthorised access. Before leaving the counter, sign-out, log-off and lock the system. Sign-ins and passwords are user specific and may not be shared. Remove boarding passes and baggage tags from the respective printers or lock them. Printed material such as boarding passes, baggage tags, passenger lists, and handling forms must be disposed of according to data protection rules, as they contain passenger data. When not in use, the check-in area must be cleared and arrangements made locally for the secure storage of such stationery. Supervisors should only allow enough supplies to be issued which are required to complete the operation. On completion of check-in operations remaining stock must be returned to the secure storage area.

11.5. PASSENGER PROTECTION

Screened passengers and their cabin baggage must not have contact with unscreened passengers. In cases where screened passengers mixed with unscreened passengers, those passengers and their cabin baggage will have to be rescreened before boarding the aircraft. During the boarding process passengers must be supervised and processed through passages in a way that ensures all passengers boarded at the gate will enter the aircraft cabin without breaching security protocols. All gates and departure areas must be secured by keeping doors closed when not in use, using appropriate barricades and where required staff must be positioned when directing passengers.

11.6. SPECIAL CATEGORY PASSENGERS

Potentially disruptive passengers could pose a safety hazard to other passengers, crew members or the overall safety of a flight. Such passengers typically include:

• Persons that display indications of being intoxicated or demonstrate abnormally abusive or aggressive behaviour (physical or verbal);
• Persons required to travel because they have been the subject of judicial or administrative proceedings (e.g. Deportees, Illegal Immigrants), as well as Inadmissible passengers).

Procedures must be put in place in accordance with requirements of the customer airline for the notification to the pilot-in-command, prior to flight

departure, of passengers on board that are persons required to travel because they have been the subject of judicial or administrative proceedings.

Report any unruly passenger behaviour you observe at check-in or at the boarding gate to the supervisor and put baggage of such passengers on standby. If the passenger is denied carriage, offload the passenger and baggage. The incident must be reported according to airline procedures.

12 BAGGAGE

12.1. SECURITY QUESTIONS

Passengers checking in are to be questioned about their hold baggage and any bags or other items they intend carrying onto the aircraft. This requirement is not affected by the existence of 100% hold bag screening or any other security measure and must be carried out for every passenger. The purpose of the questions are to help identify circumstances in which passengers may be inadvertently carrying a prohibited article onto an aircraft. All passengers should be asked whether the checked and carry-on baggage belongs to them and whether they are travelling with any prohibited items (i.e. sharp objects, dangerous goods). Subject to local law and airline requirements, the method of questioning or referring to security posters may differ.
Further security questions will either be explained by security posters at the check-in area, or it will be required of the check-in agent to ask the following additional questions:

- Did you pack your own bag(s)?
- Are you carrying any item(s) in your baggage on behalf of someone else?
- Are you sure no one has put anything into your bag(s) since you packed it?

12.2. CABIN BAGGAGE

Assess the size, weight and intended number of pieces of carry-on baggage to meet the airline's requirements. If the carry-on baggage exceeds the free allowance size and/or weight, it must be hold-checked, and charged if applicable. Check with the passenger that the baggage contents are in compliance with the Dangerous Goods Regulations and request the passenger to remove any items prohibited in hold baggage.

12.3. CHECKED BAGGAGE

Passengers are entitled to a pre-determined checked baggage allowance which can vary based on the fare paid, passenger category, routing, group status or class. There are two standard checked baggage allowance concepts:

• Piece Concept: Passengers are permitted to check two bags with a per-bag weight of up to 23kg for Economy Class, and up to 32kg for Business or First Class. Certain airlines operating under the Piece Concept may add

additional checked baggage allowance for their elite level fliers. Weight restrictions are per bag, and excess baggage will be charged for any additional bags.

• Weight Concept: Passenger are permitted to check a total bag weight in irrespective of the number of bags. Unlike the Piece Concept, in which weight restrictions are per bag, the Weight Concept allows passengers to combine their bag weight into fewer bags.

The maximum weight for any single item of baggage is 32kg to help reduce the manual handling injuries among airport staff. Luggage weighing more than 32 kg will not be accepted at check-in. Baggage weighing more than 32kg and must be split between two bags. Excess baggage charges will be dependent on whether the airline charges per piece or weight concept.

Local and client conditions may dictate the weight and size of individual pieces of hand luggage. Where a stipulation is made, it is vital that for both security and safety reasons the limitation is adhered to. Where gauges are issued for hand luggage, the item must fit comfortably into the gauge. Check-in staff should remain vigilant at all times and any luggage that does not ‘make sense’ i.e. a bag that appears excessively heavy for its size, must be questioned and consideration given to treating it as suspect.

It is important that check-in staff are briefed on the safety and security consequences of entering the incorrect weigh into the system, i.e. they are endangering the lives of passengers, crew and the public and their actions are criminal in that they are committing fraud, as well as contravening civil aviation laws.

12.4. EXCESS BAGGAGE

Excess baggage fees by weight or piece are generally applied at the time of checked baggage acceptance. Fees may not be waived without authorisation and all excess baggage counter-receipts must be accounted for.

12.5. HOLD BAGGAGE

Only accept checked baggage that is appropriately packaged and correctly labelled with passenger identification. Review weight and pieces information for recording in the DCS and for applying the appropriate fees. Always ask the passenger the security related questions and ensure that the IATA or carrier dangerous goods signage is on display.
Remove any old tags and apply the appropriate destination tag and handling tags.
Where required, use limited release tags as per the airline procedures.
Crew baggage may be presented at check-in, or airside and should be clearly identified with a crew label as well as flight details.

12.6. BAGGAGE RECONCILIATION

To comply with ICAO Annex 17, Chapter 4, Section 4.3, Standard 4.3.1, which reads:
“4.3.1 Each Contracting State shall establish measures to ensure that operators, when providing services from that State, do not transport the baggage of

passengers who are not on board the aircraft, unless the baggage separated from passengers is subject to other security control measures."

Each piece of hold baggage must be identified as accompanied by a passenger or accepted for transport as unaccompanied baggage. Unaccompanied baggage may only be accepted if appropriate security controls have been applied. Electronic system or manual (bingo sheet) procedures must be in place to ensure passenger bags are removed from a flight should a passenger fail to board or is denied boarding.

Baggage must be retained in the make-up area, moving it to the aircraft no earlier than necessary. Prior to the loading of hold baggage, loading agents must visually inspect all of the aircraft holds to ensure prohibited items and stowaways are not present. Any stowage compartments should be secure and any suspect item, stowaway or signs of tampering must be reported immediately in accordance with local instruction. Records concerning loading and unloading of aircraft must be kept for a period of at least three months.
For security requirements to be met, it is important to ensure accurately and reliably, that:
• All hold baggage loaded is accounted for, i.e. formally recorded on a manifest;
• All hold baggage loaded is appropriately identified as accompanied or unaccompanied;
• All unaccompanied hold baggage is subjected to extra security controls;
• All hold baggage is authorised for carriage;
• A person who boards the aircraft, and who is recorded as having placed baggage in the custody of the operator for that flight, is the same person who placed that baggage in the custody of the operator; and

The signature of an Appointed Person on the hold baggage manifest principally confirms that they have taken all reasonable steps to satisfy themselves that:
• All hold baggage loaded has been recorded (accounted for) on the hold baggage manifest;
• All hold baggage loaded has been appropriately identified as accompanied or unaccompanied and identified as such on the hold baggage manifest;
• All checked-in passengers have boarded the aircraft (or, where they have not, the associated hold baggage has been removed from the aircraft); and
• All unaccompanied hold baggage has been subjected to the appropriate security controls and specific confirmation of this is recorded on the hold baggage manifest.

All relevant documentation/information must be provided to the Appointed Person prior to aircraft push back allowing them to check and decide whether, based on that information, the conditions of carriage have been met. There should be only one Appointed Person per flight and they must be fully trained in the baggage reconciliation processes at the airport concerned. Relevant staff involved in the baggage reconciliation process should be aware of who the Appointed Person is for each flight. The hold baggage manifest must be retained intact at the airport of departure for a period of not less than seven (7) days after the flight.

Each stage of the process must be completed reliably and accurately in order for the final judgement to be made. The staff involved at each stage must

therefore fully understand what their responsibilities are and ensure that the correct standards are met. This should provide the necessary assurance for the Appointed Person to sign the hold baggage manifest and give authority for the aircraft to depart. DHS should maintain a record of those they have approved as appointed persons.

12.7. HOLD BAGGAGE TAKEN AT BOARDING GATE

All items of baggage taken at the boarding gate from passengers must be recorded. This may be done on the main baggage manifest, a separate Gate Manifest or in the DCS of the carrier. Where a separate manifest is used, it must display the flight number and date and be clearly marked to show that it relates to Gate Baggage. Where the main manifest is used, each entry will be marked ‘Gate’.
The details recorded will include the Bag Tag number and will be linked to the passenger. If a separate manifest is used it will indicate whether the details have been entered against the passenger’s DCS record to assist the cross check.

12.8. PASSENGERS WHO FAIL TO TRAVEL

Subject to State or Air Carrier requirements where a check-in passenger fails to board the aircraft (assigned flight) and it is established that the passenger(s) baggage has been checked, in it will be identified and offloaded or prevented from loading. The aircraft must not be despatched until this has been confirmed.

If baggage has been 'pooled', the aircraft operator must ensure that each item of hold baggage that has been placed in the custody of the operator by the person, who fails to travel, is identified and removed from the aircraft. Where it cannot be accurately established from airline records which actual bag within the 'pool' belongs to the passenger who has failed to travel, then those members of the 'pool' who are still travelling should physically identify their baggage and the remaining bag(s) in the 'pool' removed.

Where a person who fails to travel is part of an immediate family group (Mother, Father, Son, Daughter, Husband, Wife, etc.) and baggage has been 'pooled' with elements of each passenger's contents spread throughout the baggage (as opposed to each member of the party clearly having a specific bag, in which case the specific bag of the person not travelling should be offloaded), then at baseline threat level baggage can remain on board the aircraft provided that the Appointed Person and the Captain are fully satisfied as to the circumstances. The Appointed Person will record full details on the hold baggage manifest. Where, in similar circumstances, the group is not regarded as a family, the ground staff should remove all the baggage within the 'pool' and ensure that it is searched before it is placed back on board the aircraft. The details of the action taken must be recorded on the hold baggage manifest by the Appointed Person.

Where bags are removed from the aircraft in accordance with the above procedures, details of those bags should be deleted from the hold baggage manifest. Deletions should be made following specific confirmation that the relevant baggage has been positively identified and offloaded.

12.9. ACCOUNTING FOR UNACCOMPANIED HOLD BAGGAGE

Each item of unaccompanied hold baggage must be recorded on the hold baggage manifest using a separate bingo card clearly marked ‘Unaccompanied’. Each entry must specifically identify the bag as being unaccompanied and show the bag's identifier, e.g. its baggage tag number. Where a 'bingo card' (or similar) is used to record the details of each unaccompanied bag, the card must be headed with the relevant flight details and date.
Where there is no unaccompanied hold baggage, this fact must be positively recorded on the hold baggage manifest (the use of the annotation 'Nil' being more robust than a simple dash). The reason for this is that the baggage reconciliation process is primarily concerned with the identification of unaccompanied hold baggage and for ensuring that such bags are subjected to enhanced controls.

12.10. MISHANDLED BAGGAGE

Enter mishandled or unclaimed found baggage details into the tracing system. All such baggage must be held in a secure area where access is controlled.

13 HANDLING OF WEAPONS AND PROHIBITED ITEMS

Accepting and handling of firearms and ammunition is regulated by local legislation. Operator handling and acceptance procedures must be followed in line with airport and country specific security regulations in terms of acceptance and handling. Where required, a local procedure should be developed. Weapons must be handled, stored and transported in the prescribed manner.

13.1. PASSENGER AUTHORISED TO CARRY WEAPONS ON BOARD

It is possible that an airline might be carrying armed law enforcement officers or persons authorised to carry firearms. Should this be applicable to local operations a procedure must be put in place in accordance with the requirements of applicable laws and the customer airline for the check-in, handling and boarding of persons authorised to carry weapons on board the aircraft in the performance of their duties.

Procedures must include guidance to ensure the pilot-in-command is notified prior to flight departure, and if permitted by applicable laws involved, such notification shall include the number and seat locations of the authorised armed persons on board the aircraft.

13.2. WEAPONS IN HOLD BAGGAGE

The transportation of firearms and munitions of war on board civil aircraft needs to follow strict guidelines to ensure the safety of all passengers and staff members, both on the aircraft during the flight and on the ground at the departing and arriving airport. If such a service is authorised by the airline carrier, procedures in line with the carrier's procedure and local legislation must be put in place to ensure that the weapon is declared by the passenger and a form should be filled out by the passenger declaring the weapon to be unloaded and packed correctly. Passengers are responsible to have the necessary documentation, failure to do so may result in a denial of carriage. Baggage containing weapons and ammunition must be checked in against an individual passenger and not pooled with baggage belonging to other passengers. The correct label must be applied and the necessary clearance should be obtained from the appropriate authorities prior to acceptance. Details must be entered in the DCS system and a load message must be forwarded to the destination.

At the airport of arrival, weapons and ammunition must be delivered to the authorised and appointed entity of the carrier and delivered to the passenger in a secure manner in line with local laws and procedure. Weapons and ammunition must be secured at all times and not left attended for any reason.

In the event a weapon or any item suspected to be a weapon is discovered, it must be reported and handled following airline and / or local security procedures.

Where we handle weapons that are transported on the aircraft with, but are not in the possession of passengers, procedures must be put in place to meet the legal and customer requirements for the check-in, handling (departure and arrival) and boarding of such weapons. Take note that ammunition is typically treated as a weapon and the same procedures will apply.

On arrival flights, firearms and ammunition carried as baggage or otherwise surrendered for carriage on board an aircraft must be collected immediately from the aircraft side by an "authorised representative" (i.e. the entity authorised to handle firearms on behalf of the air carrier subject to local regulatory requirements). The "authorised representative" must deliver the weapon(s) and/or ammunition to the relevant authority in accordance with local legislative requirements.

Note: It is a criminal offence to mishandle weapons. When compiling local procedures it is imperative that it complies with legislation and only focus on the responsibility we have as a company and not take on responsibilities outside our scope.

14 LOAD CONTROL

Load control is a function which ensures the production of all applicable documentation to comply with airline and regulatory requirements. Relevant documents shall be manually or electronically signed, retained and disposed of as per airline and regulatory requirements.

The aircraft shall be loaded in accordance with the Loading Instructions/Report (LIR) and must be signed by the responsible appointed person to confirm that the containers, pallets and bulk load have been loaded and secured in accordance with airline instructions and complies with regulatory requirements.

Note: Under no circumstances may documents be signed before completion of the task.

14.1. NOTIFICATION TO THE CAPTAIN

The flight crew must be provide with a notification concerning dangerous goods and any other special load on board the aircraft.

15 CONTINGENCY PLANNING AND EMERGENCY RESPONSE

15.1. EMERGENCY RESPONSE TO SECURITY INCIDENTS

The primary objective of a contingency plan is the protection of life and property, and the resumption of normal operations. Each plan should be a coordinated programme between DHS and the surrounding community. The plan should set out the coordinated response and participation of all existing agencies and should designate specific duties.

15.2. CONFIDENTIALITY

In the event of an incident all information must be regarded as confidential and may only be released with the approval of the Security Manager. Staff must be advised that discussions or statements made to non-DHS staff, must not include anything that may be interpreted as an admission that the incident has been caused, or contributed to in any way, by some fault on the part of the company or its employees or agents.

15.3. SERIOUS SECURITY INCIDENT OR BREACH

Should a security incident occur over which doubt exists, the Security Manager must be contacted for guidance.

15.4. SECURITY THREATS

Threat to DHS property, or aircraft/facility/other property under the control of DHS.

The making of a bomb threat or any other security threat is a criminal offence. It is DHS policy to liaise with the Police with a view to achieving prosecution in appropriate cases.

It is the responsibility of the owner of a facility or aircraft which is subject to a bomb or other security threat to assess the threat as soon as possible and DHS must inform the customer airline immediately if they are not aware. If the customer airline cannot be contacted the Local Police and Airport Authority should be informed.

If the threat involves any DHS vehicle, building, property or personnel then the DHS Duty Manager will contact the Security Manager immediately on receipt of the details of the warning.

The action taken in respect of a bomb or security threat will depend on the assessment of the threat.

On receipt of a threat, DHS and agency staff must record all relevant details and report them immediately to the DHS manager on duty by the fastest possible means. Staff working in areas most likely to receive a threat, must be instructed on the appropriate actions to be taken.
The sole responsibility for assessing the validity of bomb or any other security threats to any facility rests with the owner or operator of the facility.

For general emergency response coordination and business continuity principles, refer to Chapter 4 of the DHS SMS Manual.

15.5. DISCOVERY OF PROHIBITED ARTICLES

In the event of a prohibited article being discovered on a person or in their hand baggage, consideration should be given to calling the Police.

Ground handlers, including DHS, and airport authorities are responsible for preparing the plans required under this heading. Contingency planning is to cover the action to be taken on the discovery of a dangerous or suspicious item in the following circumstances:

• On the person of a crew member, passenger or ground staff employee or agent intending to board an aircraft;
• In hand-carried items being taken on board an aircraft by crew members, passengers, ground staff or agents' employees;
• In hold baggage;
• In company mail;
• In catering and aircraft stores;
• During searches or checks of aircraft.

The action most appropriate to deal with the discovery of a dangerous or suspicious item will depend on a number of circumstances. These include:

• Whether the presence of the item threatens life;
• Whether the circumstances of the discovery indicate that a crime has been or may be about to be committed;
• Whether the item is inherently dangerous (e.g. an explosive);
• Whether the item is dangerous only in certain circumstances (e.g. a knife taken into the passenger cabin);
• Whether the regulations on the carriage of firearms apply;
• Whether the dangerous goods regulations apply.

The discovery of a dangerous or suspicious article will call for one or more of the following courses of action to be taken:

• Reporting of the incident to the Duty Station Manager;
• Reporting of the incident to the Police and the airport authorities;
• The placing of the article in the aircraft hold where it will be inaccessible to the passenger during the flight;
• Inviting the passenger to have a friend or relative remove the offending article from the airport;
• Retention of the article against a receipt for return to the owner at a later date (e.g. on his return to the airport);
• Destruction of the article. This course is dependent on the passenger signing a certificate to the effect that he has no objection to the proposed destruction.

16 SECURITY QUALITY MANAGEMENT

Managers are required to monitor the quality of the security programme and ensure it fully complies with local conditions, regulatory requirements. A programme of regular structured and demonstrable audits (Quality Assurance) and inspections (Quality Control) must be implemented for critical security operations, including any 3rd party sub contracted suppliers. Contractors should be audited prior to commencement of the contract and training records should be checked and copies retained.

It is likely that carriers and regulators will wish to carry out their own audits and inspections of DHS stations and facilities, DHS will cooperate fully when such requests are made. Where findings are made in any audit it is vital that corrective action is taken to rectify any deficiency.

16.1. QUALITY ASSURANCE

The security quality programme will provide for the auditing and evaluation of the management system (SeMS) and operational security functions at planned intervals to ensure DHS comply with the security programme and achieving its objectives.

16.2. QUALITY CONTROL

Periodic or event-driven security surveys, tests and inspections must be done to identify needs and weaknesses in the security programme, infrastructure and related procedures.

Further guidance on Quality Management can be found in the DHS Quality Manual (SQM).

For details on station self-assessments and real-time safety monitoring, refer to Section 2.1 of the DHS SMS Manual.