DHS GmbH
Am Hagen 5
59368 Werne

Data Protection & Security Policies (DPISP)

Prepared for: DHS GmbH

Prepared by: DOM

Issued: 10.03.2025, last update: 26.03.2026

Version: V2 / Revision 1

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

GENEHMIGT
Von Dominika Doruch , 06:32, 31.03.2026

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

Content

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

Record of revisions

Part	Title	Original Issue	Latest Review
6.	Annex A - Operational Process Flow	26.03.2026	

Change revision summary

Part	Description of change
6.	Added high-level operational process flow for supplier compliance and data protection support.

0 INTRODUCTION

As a Ground Handling Agent, DHS has a high responsibility to protect passenger, employee, and company data. This document serves as a guideline for all employees on how to securely handle information, protect IT systems, and ensure compliance with security policies.

1 IT SECURITY POLICIES & ACCESS CONTROL

IT Security Policy

Cybersecurity is essential to DHS operations. Every employee plays a role in protecting company systems, data, and customer information. IT security is not optional—it is a core part of our daily work.

☑ IT Security Guidelines

- Use strong passwords and enable Multi-Factor Authentication (MFA) where required.
- Lock workstations and company devices when unattended.
- Never share login credentials or allow unauthorized access.
- Keep software and antivirus programs updated.
- Do not use personal USB drives or external storage devices.
- Avoid clicking on unknown links or email attachments.
- Always verify sender identities before sharing sensitive information.

☑ Incident Reporting & Compliance

- Report cybersecurity incidents immediately to IT Security.
- Do not attempt to fix security breaches on your own.
- Follow all data protection and confidentiality policies.
- Failure to comply may result in disciplinary action.

DHS is committed to maintaining the highest level of cybersecurity to protect our employees, customers, and operations. Every individual is responsible for safeguarding company systems and data. By following these policies, we ensure a secure and resilient work environment.

Ingo Schnitger
CEO

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

For detailed technical guidelines regarding IT system usage, device security, remote work, and cloud access, please refer to the DHS IT Policy.

1.1. SYSTEM AND DATA ACCESS

- All employees must use **strong passwords** and update them regularly.
- **Multi-Factor Authentication (MFA)** is required where applicable.
- **Unauthorized access** to IT systems is strictly prohibited.
- Employees must lock their **computers and mobile devices** when leaving their workstations.
- Use only **company-approved devices** for work-related tasks.

Example:

✔ **CORRECT:** Lock the check-in system immediately after use.

✘ **INCORRECT:** Share login credentials with colleagues.

Airline and airport IT systems (such as DCS, CUTE/CUPPS, BRS and similar platforms) are considered sensitive external systems.

All data retrieved from these systems must be handled with the same level of care and data protection as DHS internal systems. Personal data accessed via these platforms must not be stored, copied or transferred outside of the system unless explicitly authorized by the system owner.

1.2. PHYSICAL SECURITY

- Do not write down sensitive information on exposed notes.
- Lock check-in and gate computers after each use.
- Unauthorized individuals must not access security-sensitive areas.

For overarching document management responsibilities and integration into the Safety Management System, refer to Section 0.13 of the DHS SMS Manual.

2 DATA PROTECTION & HANDLING POLICIES

2.1. HANDLING PERSONAL DATA

- Data minimization:

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

Only necessary personal data should be collected and processed

- Passenger data should only be accessed for operational purposes.
- No unauthorized sharing or storage of personal information.

Example:

✔ CORRECT: Only retrieve passenger details when required for check-in or boarding.

✘ INCORRECT: Print passenger lists and take them outside work areas.

2.2. DATA RETENTION & DELETION

- Personal data is stored securely and deleted once it is no longer required.
- Secure deletion methods are used to prevent unauthorized recovery.

2.3. PASSENGER & EMPLOYEE DATA RIGHTS

- Passengers and employees have the right to access, correct, or request deletion of their personal data.
- All data requests must be forwarded to the **DHS Data Protection Officers**.

For procedural integration into operational safety responsibilities, refer to Section 0.13 of the DHS SMS Manual.

3 IT SECURITY THREATS & PREVENTION

3.1. PISHING & FRAUD PREVENTION

- Do **not** open suspicious emails with unknown attachments or links.
- Do **not** disclose confidential information via email or phone.
- **Report suspicious messages** immediately to IT security.

3.2. CYBER SECURITY TRAINING

- All employees must complete **mandatory IT security training**.
- Regular **phishing awareness tests** will be conducted.
- Employees must comply with security policies and report any security issues.

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

For alignment with safety-related training and promotion, see Sections 3.1 and 3.2 of the DHS SMS Manual.

The cybersecurity training requirements in this policy are aligned with those in the DHS IT Policy. Both documents must be read and followed.

3.3. INCIDENT & MANAGEMNET RESPONSE

- Any **security incident** (e.g., data breach, lost/stolen device) must be reported immediately.
- DHS has an **Incident Response Plan** to handle breaches effectively.

For system-wide incident investigation principles and categorization, refer to Section 0.8 of the DHS SMS Manual.

4 COMPLIANCE & AUDITING

4.1. REGULAR SECURITY AUDITS

- DHS conducts **internal IT security audits** to assess compliance.
- Employees must participate in security assessments as required.

For integration with station-level audit procedures, refer to Section 2.1 of the DHS SMS Manual.

4.2. DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

- Employees who violate IT security policies may face disciplinary action.
- Any misuse of company IT resources will be investigated and addressed accordingly.

For overall fair & just culture principles regarding employee conduct, see Section 0.11 of the DHS SMS Manual.

5 KEY CONTACT & FURTHER INFORMATION

- **Data Protection Officer**: [ingo.schnitger@dhs.aero]
- **Incident Reporting**: Report security issues via SafetyCulture App published in all offices

Your Responsibility as an Employee:

- **Follow IT security policies and best practices.**
- **Keep company and passenger data secure.**
- **Report suspicious activities immediately.**

Cybersecurity is a shared responsibility!

controlled document. Controlled version on AVBIS/DHS Manuals.
Printed/downloaded copies uncontrolled.

6 ANNEX A – HIGH-LEVEL OPERATIONAL PROCESS FLOW

This annex provides a high-level overview of the DHS operational process flow and approved systems used for service delivery and internal reporting.

The diagram is intended for management overview and supplier compliance purposes and does not represent technical process detail.

DHS Ground Handling — Operational Process Flow