

DHS GmbH
Am Hagen 5
59368 Werne



Data Protection & Security Policies

Prepared for: DHS GmbH

Prepared by: DOM

Issued: 10.03.2025

Version: V2

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



Content

0	INTRODUCTION	4
1	IT SECURITY POLICIES & ACCESS CONTROL	4
1.1.	SYSTEM AND DATA ACCESS	5
1.2.	PHYSICAL SECURITY	5
2	DATA PROTECTION & HANDLING POLICIES	5
2.1.	HANDLING PERSONAL DATA	5
2.2.	DATA RETENTION & DELETION	6
2.3.	PASSENGER & EMPLOYEE DATA RIGHTS	6
3	IT SECURITY THREATS & PREVENTION	6
3.1.	PISHING & FRAUD PREVENTION	6
3.2.	CYBER SECURITY TRAINING	6
3.3.	INCIDENT & MANAGEMNET RESPONSE	6
4	COMPLIANCE & AUDITING	6
4.1.	REGULAR SECURITY AUDITS	6
4.2.	DISCIPLINARY ACTIONS FOR NON-COMPLIANCE	7
5	KEY CONTACT & FURTHER INFORMATION	7



Record of revisions

Part	Title	Original Issue	Latest Review

Change revision summary

Part	Description of change



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



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.

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.

2 DATA PROTECTION & HANDLING POLICIES

2.1. HANDLING PERSONAL DATA

- Data minimization:

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**.

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.

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.

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.



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.

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!

