DHS GmbH
Am Hagen 5
59368 Werne

IT Policy

Prepared for: DHS GmbH

Prepared by: DOM

Issued: 30.07.2025, 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 , 06:33, 31.03.2026

Content

Record of revisions

Part	Title	Original Issue	Latest Review
13.	Annex A – High-Level IT Infrastructure Overview	26.03.2026	

Change revision summary

Part	Description of change
13.	Added Annex A – high-level IT infrastructure overview including approved cloud services and external operational systems for supplier assurance and policy support

0 PURPOSE AND SCOPE

This policy applies to all employees, contractors, and partners who have access to the IT systems, networks, or devices of DHS. It defines the rules for the secure, lawful, and responsible use of the company's IT resources.

1 CORE PRINCIPLES

IT systems and data are the property of the company. All users must use the systems in a way that ensures security, data protection, and the company's interests at all times.

2 ACCESS RIGHTS AND SECURITY

- Systems may only be used with a personal user ID and a secure password.
- Multi-factor authentication (MFA) must be used where available.
- Passwords and login credentials must never be shared.
- All devices must be locked or secured when left unattended.

This policy applies not only to DHS internal IT systems, but also to any external systems provided by third parties, such as Avbis, Safety Culture, or systems operated by airlines (e.g., Departure Control Systems (DCS), airline document libraries) and airports (e.g., CUTE/CUPPS, BRS, and other operational platforms).

Access to these systems is strictly limited to operational purposes and must comply with all security standards and conditions defined by the respective system owner. Any misuse of these systems constitutes a violation of the DHS IT Policy.

3 EMAIL AND COMMUNICATION

Email systems are primarily intended for business purposes. Occasional private use is permitted, provided that it does not interfere with work. Offensive, discriminatory, or inappropriate content is strictly prohibited. Suspicious links or attachments must not be opened.

4 INTERNET AND CLOUD USAGE

Internet access is primarily for business purposes. Private use is allowed during breaks, as long as it is legal and safe. For storage and data transfer, only DHS-approved cloud solutions may be used. Personal cloud services must not be used for company data.

5 DATA PROTECTION & COMPLIANCE

All processing of personal data must comply with the General Data Protection Regulation (GDPR) and applicable laws. Personal data may only be stored and processed on company systems. Confidential paper documents must be securely destroyed after use.

For detailed rules and procedures on handling personal and passenger data, please refer to the DHS Data Protection & Information Security Policies (DPISP).

6 USE OF DEVICES

Laptops, tablets, and mobile phones are the property of the company. Employees are responsible for the careful handling of these devices and must report any loss or damage immediately.

Bring Your Own Device (BYOD):

The use of private mobile devices for business purposes is permitted only when explicitly required (e.g., for AVBIS). Such devices must be secured with a password or biometric lock, and company data may only be accessed through approved, secure applications. If a privately used device is lost or stolen, this must be reported immediately so that access can be blocked.

7 REMOTE WORK / HOME OFFICE

Work performed outside the company must meet the same security standards as work performed on site. Secure, password-protected Wi-Fi is mandatory. If internal systems are accessed externally, this must be done through DHS-approved secure methods (e.g., secure web applications or specific access procedures). A VPN connection is not mandatory.

8 IT SECURITY & AWARENESS

- Suspicious emails, links, or IT incidents must be reported immediately.
- No software or apps may be installed without IT approval.
- Participation in mandatory cybersecurity training is required.

This policy works in conjunction with the *DHS Data Protection & Information Security Policies (DPISP)*. All employees are required to be familiar with both documents.

9 SOCIAL MEDIA AND PUBLIC COMMUNICATION

Employees may only speak or post on behalf of the company with explicit authorization. Confidential information, processes, security details, or incidents must not be published on social media.

10 MONITORING AND LOGGING

To ensure IT security and meet legal requirements, system access and internet usage are logged. These logs are used exclusively to investigate security-related incidents, conduct audits, or meet legal requirements. Employees should be aware that their use of company systems may be traceable in such cases.

11 ENFORCEMENT

Violations of this policy may result in disciplinary action up to and including termination. This policy will be reviewed annually and updated as necessary.

12 ROLES AND RESPONSIBILITIES

Managers: Ensure that their teams are familiar with the IT Policy and Data Protection & Security Policies, monitor compliance, and immediately report violations or incidents.

Employees: Read and follow this policy, participate in cybersecurity training, protect devices and login credentials, and promptly report suspicious emails or incidents.

13 ANNEX A – HIGH-LEVEL IT INFRASTRUCTURE OVERVIEW

This annex provides a high-level overview of the DHS IT infrastructure and approved external systems used for operational and administrative purposes.

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