

HUGO BOSS

HUGO BOSS INFORMATION SECURITY GUIDELINE

VERSION 2.0, FEBRUARY 24, 2026

DEPARTMENT INFORMATION SECURITY & IT COMPLIANCE

AT A GLANCE

This chapter is intended to quickly acquaint all HUGO BOSS employees with the core contents and provisions of the **HUGO BOSS Information Security Guideline**:

The Information Security Guideline describes the security objectives and how they are aligned to the company objectives. Further, this guideline shows the responsibilities of the management as well as of every employee. Also, contacts for information security topics can be found in this document to enable employees to reach the right persons with their questions.

Please note that the section AT A GLANCE is not intended to be exhaustive and is only meant to provide an overview of the most important points of the policy. All provisions and content of the policy are binding and must be adhered to by employees.

TABLE OF CONTENTS

1	PURPOSE	6
2	SCOPE	6
3	INFORMATION SECURITY GUIDELINE	6
3.1	IMPORTANCE OF INFORMATION SECURITY	6
3.2	SECURITY OBJECTIVES	6
	3.2.1 COMPLIANCE WITH REGULATORY REQUIREMENTS	6
	3.2.2 PROTECTION OF TRADE / BUSINESS SECRETS	7
	3.2.3 CONFIDENTIALITY	7
	3.2.4 INTEGRITY	7
	3.2.5 AVAILABILITY	7
	3.2.6 DATA MINIMIZATION	7
	3.2.7 NON-LINKING	7
	3.2.8 INTERVENABILITY	7
	3.2.9 TRANSPARENCY	7
3.3	TARGET SECURITY LEVEL / SECURITY STRATEGY	8
3.4	RESPONSIBILITY AND ORGANISATION	8
3.5	CENTRAL INFORMATION SECURITY OFFICER	8
3.6	LOCAL PERSONS RESPONSIBLE FOR INFORMATION SECURITY	9
3.7	INFORMATION SECURITY REQUIREMENTS FOR THIRD PARTIES AND SUPPLIERS	9
3.8	SECURITY INCIDENT MANAGEMENT	10
3.9	OBLIGATION OF EMPLOYEES TO COMPLY WITH THE GUIDELINE	10
	3.9.1 COMPLIANCE WITH RELATED INFORMATION SECURITY POLICIES	10
3.10	PERFORMANCE REVIEW	11
4	UPDATING, CONTROLS AND REVISION	11
5	VALIDITY AND ENTRY INTO FORCE	11
6	DEALING WITH VIOLATIONS	11
7	CONTACTS	12

1 PURPOSE

HUGO BOSS is a global fashion and lifestyle group in the premium segment and is one of the leading suppliers of high-quality men's and women's clothing.

The increasingly digitalized business processes of HUGO BOSS depend to a large extent on the quality of IT services and information and communication technology. Information technology is an important resource in all business units. Customers in particular, but also employees, suppliers, business partners and shareholders trust that their data and information are secure at HUGO BOSS. In order to justify this trust, the integrity, availability and confidentiality of data and information must be sufficiently ensured.

This guideline defines the basic strategy of information security and its organizational structure for all HUGO BOSS corporate and organizational units covered by the scope of this guideline.

2 SCOPE

This policy applies to employees at all companies and business areas of the HUGO BOSS Group. The Policy must be implemented appropriately by the responsible bodies in all Group companies.

Compliance with the standards set forth below is mandatory for all employees.

The information security guideline forms the basis for information security framework further necessary information security measures (e.g. different guidelines, work instructions, templates).

3 INFORMATION SECURITY GUIDELINE

3.1 IMPORTANCE OF INFORMATION SECURITY

The aim of information security is to adequately protect all types of company information, regardless of whether it is processed with or without the support of information and communication technology, in accordance with the risk assessment.

The business success of HUGO BOSS depends to a large extent on data and information being up-to-date, unaltered and always treated with the necessary confidentiality. Information security is becoming increasingly important, especially in relationships with customers, suppliers and business partners. Information security supports the digitalization strategy of HUGO BOSS.

In addition, compliance with legal/regulatory requirements (in particular with regard to the legal requirements identified as applicable in the legal register of HUGO BOSS Group) must be ensured.

A breach of information security can lead to significant financial losses and reputational damage.

For this reason, effective information security and the proper handling of it represent a decisive cornerstone for the corporate success of HUGO BOSS.

3.2 SECURITY OBJECTIVES

In order to ensure appropriate information security within the HUGO BOSS Group, the company management defines the following overarching security objectives.

3.2.1 Compliance with regulatory requirements

Information security must always ensure compliance with legal and internal company requirements. For example, the protection of personal data is subject to high legal requirements. It is therefore necessary for HUGO BOSS to take into account and comply with applicable laws and regulations in accordance with the legal department.

3.2.2 Protection of trade / business secrets

Information security must secure company information within the EU/EEA through appropriate measures in such a way that it is protected in accordance with the requirements of EU Directive 2016/943 on the protection of trade secrets and applicable national laws.

For Group companies outside the EU, the respective national requirements regarding the protection of trade and business secrets must be complied with, insofar as they exist and are documented by the HUGO BOSS legal department. If applicable and not in conflict with national laws, the provisions of the EU Directive on the Protection of Trade Secrets also apply to Group companies outside the EU.

3.2.3 Confidentiality

Data and information in need of protection - regardless of their form - must be adequately protected against unauthorized disclosure and unauthorized access. The appropriate protection of information requires the classification of all data with regard to its confidentiality, depending on the degree of confidentiality and, where applicable, the need for protection. The Data Protection Officer of HUGO BOSS Group must be involved in the process of selecting and designing procedures for processing personal data.

3.2.4 Integrity

The accuracy and reliability of data and information that need protection, as well as the proper functioning of essential ICT infrastructures and applications, must be guaranteed.

3.2.5 Availability

Data and information requiring protection and the relevant ICT infrastructures and applications must have a level of availability that ensures the operation of business-relevant processes based on their business criticality.

The following objectives are defined for the processing of personal data due to the high legal requirements for data protection:

3.2.6 Data minimization

The selection and design of IT systems and applications must be geared towards the goal of ensuring that no personal data is collected and processed beyond what is necessary to achieve the purpose of the processing. Wherever possible, anonymization or masking of data should be implemented in accordance with the sensitivity of data.

3.2.7 Non-linking

Personal data may only be processed and analysed for the purpose for which it was collected. Personal data may not be merged if this is not covered by the processing purpose.

3.2.8 Intervenability

Data subjects have the right to information about the processing of their personal data, to access, rectification, restriction of processing and erasure of their data (so-called data subject rights). IT systems and applications must be set up in such a way that the rights of data subjects are always guaranteed.

3.2.9 Transparency

Data subjects and operators of IT systems and applications, as well as supervisory authorities, must be able to recognize at any time which personal data is collected and processed in a procedure and for what purpose, which systems and processes are used for this, where the data flows to and for what

purpose, and who bears legal responsibility for the data and systems in the various phases of data processing.

3.3 TARGET SECURITY LEVEL / SECURITY STRATEGY

To achieve the aforementioned security objectives and the continuous improvement of the information security level, HUGO BOSS implements the international standard ISO/IEC 27001 (in the currently valid version) and operates a documented information security management system (ISMS) on this basis. The ISMS also includes risk management, the performance of regular internal audits, appropriate control of documentation and records, a management review and the application of the continuous improvement model ("PDCA"). HUGO BOSS is also guided by the recommendations of ISO/IEC 27002 (in the currently valid version).

HUGO BOSS is aware that there is no such thing as absolute information security. The effort and result of the security measures must be in reasonable proportion to each other. The risk level and the associated security objectives are determined and aligned through a risk analysis of the relevant business processes. The measures are then prioritized based on the respective risk profile of information, IT systems and applications.

Cases of damage with high material or immaterial consequences for HUGO BOSS must be prevented. HUGO BOSS has a risk-based approach to classify the impact that can be viewed in the IT Risk Management Policy.

When processing personal data, the requirements of data protection must always be met in full.

3.4 RESPONSIBILITY AND ORGANISATION

The company management bears overall responsibility for information security and is aware of its importance for the entire Group. With this guideline, the company management defines the importance of information security and the security strategy. The company management fully supports the objectives formulated in this guideline and the measures derived and to be derived from it.

The Managing Board of HUGO BOSS AG (Germany) shall appoint a central information security officer (Section 6).

HUGO BOSS Group companies with their own IT staff (at least ten IT employees) shall appoint a local person responsible for information security (Section 7). Locations and subsidiaries with fewer personnel are subject to the management of the central information security officer. Local information security officers must be appointed for the following Group companies in all cases:

- HUGO BOSS Fashions Inc., USA
- HUGO BOSS Hong Kong Ltd, CHINA
- HUGO BOSS Ticino S.A., SWITZERLAND
- HUGO BOSS Textile Industry Ltd, TURKEY

The respective (specialist) division or department management of HUGO BOSS AG or a Group company is responsible for compliance with the requirements of this guideline and the information security guidelines and measures based on it within its own area of responsibility. The (specialist) division or department management appoints persons responsible for all information technology systems (so-called system managers).

3.5 CENTRAL INFORMATION SECURITY OFFICER

The central information security officer controls the security process and is responsible for planning, implementing, maintaining, optimizing and monitoring the Information Security Management System

(ISMS). He or she is responsible for coordinating and monitoring all activities relating to information security.

The central information security officer shall be involved at an early stage in all matters relating to information security.

The Central Information Security Officer has the right to speak directly and at any time to the Managing Board of HUGO BOSS AG and all group companies. He also has the right and duty to involve the Managing Board key information security issues.

The central information security officer shall be provided with the necessary resources (personnel, time, material and funds) to carry out his or her tasks.

The central information security officer is the contact person for all questions relating to information security and can be reached using the following contact details:

HUGO BOSS AG
- Information Security Officer -
Holy Allee 3
72555 Metzingen (Germany)
information-security@hugoboss.com

3.6 LOCAL PERSONS RESPONSIBLE FOR INFORMATION SECURITY

The local person responsible for information security is responsible for monitoring and complying with the company's internal information security requirements in his/her area of responsibility. He shall be provided with the necessary resources (personnel, time, material and funds) to enable him to fulfil this task.

The local information security responsible shall involve the central information security officer in all information security-related issues at an early stage.

The local information security responsible shall report to the central information security officer at least once a year on the status of information security in his or her area of responsibility. In addition, the central information security officer may request ad hoc reports on specific information security issues on an ad hoc basis.

If a breach of information security becomes known, the locally responsible person shall inform the central information security officer promptly.

A list of appointed local information security responsible is aside of this guideline.

3.7 INFORMATION SECURITY REQUIREMENTS FOR THIRD PARTIES AND SUPPLIERS

Third-party organizations, including suppliers, service providers, consultants and contractors, must comply with the information security requirements of HUGO BOSS to ensure the confidentiality, integrity and availability of information processed, stored or transmitted on behalf of HUGO BOSS. Information security requirements for third parties must be defined, documented and contractually agreed **before** third parties are granted access to HUGO BOSS information, systems or facilities.

These requirements include in particular:

- compliance with the HUGO BOSS Information Security Framework and all applicable policies, guidelines and standards,
- adequate technical and organizational security measures,
- clearly defined access control and identity management practices,
- secure handling of information in line with the applicable information classification,
- incident reporting obligations and cooperation in incident handling,
- rules for the involvement and control of sub-contractors,
- rights of audit and appropriate monitoring of agreed controls,

- secure termination of the relationship, including return or deletion of information and other assets. Supplier selection and onboarding must include an assessment of the provider's ability to meet the defined information security requirements. Depending on the risk, this may include security questionnaires, due-diligence checks, certifications (e.g. ISO/IEC 27001) or audits. Existing supplier relationships must be regularly monitored and reviewed to ensure continued compliance with the agreed information security requirements and to identify necessary improvements. For cloud services and other ICT services, the shared responsibility model and the security capabilities of the provider must be explicitly considered in accordance with the relevant information security, cloud and supplier governance requirements.

3.8 SECURITY INCIDENT MANAGEMENT

Information security incidents can result in major damage to the HUGO BOSS group. For this reason, a suitable guideline for handling information security incidents has been established, by means of which security incidents are quickly recognized and efficiently handled. In the event of security incidents, the central information security officer is authorized to implement or order necessary security measures, even at short notice. If a security incident involving personal data occurs, the data protection officer must be informed immediately.

3.9 OBLIGATION OF EMPLOYEES TO COMPLY WITH THE GUIDELINE

Every employee is obliged to observe and comply with the provisions of this guideline and the information security framework (this policy and all others published in the information security SharePoint) and measures based on it for their workplace. Violations of mandatory security rules by employees will result in disciplinary action and may also lead to legal consequences (e.g. warning, dismissal).

Every employee should help to prevent security incidents and breaches of security objectives. Recognized errors and incidents must be reported immediately using a service desk ticket via email or call.

3.9.1 Compliance with related Information Security Policies

In addition to this guideline, every employee is obliged to observe and comply with all further information security policies and related requirements issued as part of the HUGO BOSS Information Security Framework. The following policies are binding and must be adhered to as applicable:

- Acceptable Use Policy
- Bring Your Own Device
- Remote Working Policy
- Human Resources Security Policy
- Information Security Awareness Policy
- Clean Desk & Clear Screen Policy
- Policy on Policies
- IT Risk Management Policy
- IT Security Self Audit Policy
- Third Party Management Policy
- Data and System Classification Policy
- Data Encryption Policy
- Data Exchange and Loss Prevention Policy
- Paper and Removable Media Policy
- Retention & Destruction of Records Policy
- Anti Malware Policy

- Password Policy
- Remote Access and Maintenance Policy
- AI and Gen-AI Policy
- Software Policy
- SAP Security Policy
- Visitor Handling Policy
- Physical Security Policy
- Business Continuity Management Policy

The current version of all mentioned policies can always be found [here](#).

3.10 PERFORMANCE REVIEW

HUGO BOSS regularly conducts internal audits to ensure an appropriate level of information security and to check the effectiveness and efficiency of the security process. The results must be documented. In the event of deviations, corrective measures must be defined and, after implementation, subjected to a new effectiveness test.

Audits shall be carried out in compliance with applicable data protection regulations. Measures for the purpose of employee monitoring are not permitted without the prior involvement of the Works Council and the data protection officer.

The central information security officer shall report to the Managing Board of HUGO BOSS AG once a year on the status of information security in the Group.

4 UPDATING, CONTROLS AND REVISION

Effectiveness of the procedures will be reviewed by the Information Security & IT Compliance Department at least once a year or as required. The Information Security & IT Compliance Department reserves the right to carry out checks on fulfilment of the requirements set out in this Policy at any time and without prior notice. This Policy may be amended at any time and will be subject to a regular review by the Information Security & IT Compliance Department at least once a year to ensure it is up to date. Experiences from the past year and suggestions from internal and external stakeholders are always considered. The most recent version of the Policy will always be available on HUGO BOSS's intranet.

5 VALIDITY AND ENTRY INTO FORCE

The Policy takes effect on 01.06.2021 and applies without restrictions throughout the entire HUGO BOSS Group.

6 DEALING WITH VIOLATIONS

A violation of this Policy may lead to disciplinary measures proportionate to the seriousness of the relevant actions. Such measures may include the termination of your employment at HUGO BOSS, without prejudice to possible legal action. (Potential) Violations of this Policy as well as (potential) misconduct of any kind can be (anonymously) reported at any time to the [HUGO BOSS Speak Up Channel](#) or the [HUGO BOSS Ombudsperson](#).

7 CONTACTS

In case of any questions or suggestions, please contact the Information Security & IT Compliance Department.

Valid for:	HUGO BOSS Group	Version:	2.0
Valid from:	01.06.2021	Status:	released, valid
Approved by:	Managing Board HUGO BOSS AG	Last Update:	24.02.2026
Policy Owner:	Information Security & IT Compliance	Classification:	public

REFERENCES (IF APPLICABLE)

EN_Local_Information_Security_Contacts

This document shows the different colleagues responsible for information security in the main subsidiaries.

CHANGE HISTORY

Version	Valid from	Author	Note
1.0	07.03.2021	Nikolaus Kümmel	Creation
1.1	10.02.2023	Steffen Schellig	Annual Audit – No Changes
1.2	11.03.2024	Furuzan Hadi	Content adjustments in chapter 3.1, 3.2 Security objectives
1.3	18.02.2025	Stefan Baldus	Updated wordings and improved writing
2.0	24.02.2026	Steffen Schellig	Transition to new structure