Information Security &
IT Compliance

HUGO BOSS
Guideline Information Security

HUGO BOSS

Change History

Version	Valid from	Author	Note
1.0	07.03.2021	Nikolaus Kümmel	Creation of an information security guideline
1.0	16.04.2021	Nikolaus Kümmel	Adjustment after stakeholder feedback
1.0	19.04.2021	Stefan Baldus	Adjustment after stakeholder feedback
1.1	10.02.2023	Steffen Schellig	Annual audit
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
1.4	05.06.2025	Steffen Schellig	Transition to new Structure

EXECUTIVE SUMMARY

The HUGO BOSS Information Security Guideline establishes a comprehensive framework to ensure the confidentiality, integrity, and availability of data across the organization. It applies to all employees, systems, and processes within HUGO BOSS AG and its subsidiaries, supporting the company's digitalization strategy and compliance with legal and regulatory requirements.
Key highlights include:

- **Security Objectives:** Focus on compliance, protection of trade secrets, confidentiality, integrity, availability, data minimization, and transparency.
- **Governance Structure:** A central Information Security Officer oversees the Information Security Management System (ISMS), supported by local security officers in key regions.
- **Incident Management:** A robust process for identifying, managing, and mitigating security incidents, with clear escalation protocols.
- **Employee Responsibility:** All employees are required to comply with the guideline and actively contribute to preventing security incidents.
- **Continuous Improvement:** Regular audits, training programs, and updates to the guideline ensure alignment with evolving risks and standards, including ISO/IEC 27001.

This guideline underscores HUGO BOSS's commitment to safeguarding data and maintaining trust with customers, employees, and partners. It is a cornerstone of the company's operational resilience and long-term success.

CONTENT

HUGO BOSS

1 PURPOSE

(1) 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.

(2) 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[1], 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.

(3) 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

(1) The Information Security Guideline covers the entire information and communication infrastructure and applies to HUGO BOSS AG as well as all Group companies controlled by it and the respective employees. It must be implemented by the responsible departments of all Group companies. Compliance must be ensured by the management of each Group company on a permanent basis.

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

3 IMPORTANCE OF INFORMATION SECURITY

(1) 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.

(2) 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.

(3) 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.

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

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

4 SECURITY OBJECTIVES

(1) In order to ensure appropriate information security within the HUGO BOSS Group, the company management defines the following overarching security objectives:

4.1 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.

[1] Hereinafter referred to as "employees" for reasons of linguistic simplification. However, this guideline expressly refers to persons of all gender identities.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

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

4.6 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.

4.7 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.

4.8 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.

4.9 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.

5 TARGET SECURITY LEVEL / SECURITY STRATEGY

(1) 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).

(2) 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.

(3) 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.

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

6 RESPONSIBILITY AND ORGANISATION

(1) 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.

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

(3) 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 personal 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

(4) 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).

7 CENTRAL INFORMATION SECURITY OFFICER

(1) 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.

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

(3) 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.

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

(5) 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

8 LOCAL PERSONS RESPONSIBLE FOR INFORMATION SECURITY

(1) 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.

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

(3) 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.

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

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

9 SECURITY INCIDENT MANAGEMENT

(1) 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.

(2) 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.

10 OBLIGATION OF EMPLOYEES TO COMPLAY WITH THE GUIDELINE

(1) 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).

(2) 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.

11 TRAINING AND AWARENESS MEASURES

(1) Information security can only be sufficiently effective if all employees are aware of the potential threats to information security and act responsibly in their areas of responsibility.

(2) The central information security officer shall sensitize and qualify employees with an awareness and training program in an appropriate manner. This can be ensured, for example, through information on the company intranet, information letters, online-based training or classroom training.

12 PERFORMANCE REVIEW

(1) 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.

(2) 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.

(3) 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.

13 UPDATING AND REVISION

It is the responsibility of the Information Security and IT Compliance team to review this guideline at least every three years or as soon as changes to the subject are done. If necessary, the guideline must be amended.

14 VALIDITY AND ENTRY INTO FORCE

This policy enters into force on 01. June 2021 and every employee is obliged to observe and comply with the provisions of this policy and measures based on it for their workplace. Violations of mandatory security rules by employees may result in disciplinary actions and may also lead to legal consequences (e.g. warning, dismissal).

15 CONTACTS

The Information Security and IT Compliance team is available to answer questions regarding this guideline via information-security@hugoboss.com.

Valid for:	HUGO BOSS	Version:	1.4
Valid from:	18.02.2025	Status:	released, valid
Approved by:	Managing Board HUGO BOSS AG	Last Update:	05.06.2025
Policy Owner:	Information Security & IT Compliance	Classification:	public