H U G O B O S S

Information Security Policy

Version	Date	Author	Changes
1.0	3/7/2021	Nikolaus Kümmel	Author, Information Security Policy
1.0	4/16/2021	Nikolaus Kümmel	Update after stakeholder feedback
1.0	4/19/2021	Stefan Baldus	Update after stakeholder feedback

Preamble

(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 areas. Above all, customers, but also employees [1], suppliers, business partners and shareholders trust that their data and information are secure at HUGO BOSS. In order to be able to justify this trust, HUGO BOSS must take sufficient measures to ensure the integrity, availability and confidentiality of data and information.

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

1 Scope of Application

(1) The Information Security Policy covers the entire information and communication infrastructure and applies to HUGO BOSS AG as well as all Group companies controlled by the latter and their employees. It is to be implemented by the responsible bodies of all Group companies in an appropriate manner. Compliance must be ensured on a permanent basis by the management of each Group company.

(2) The Information Security Policy forms the basis for any further information security measures required (e.g. specific Policies, work instructions, templates).

2 Importance of Information Security

(1) The objective of information security is to adequately protect company information of any kind that is worthy of protection, regardless of whether it is processed with or without the support of information and communication technology, in accordance with its need for protection.

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

(3) In addition, compliance with legal regulations (in particular regarding data protection, protection of business secrets) must be ensured.

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

(5) For this reason, a functioning information security system and the security-conscious handling of information represent a key cornerstone for the corporate success of HUGO BOSS.

[1] For the sake of simplicity, the masculine form will be used below. However, this Policy explicitly refers to individuals of all gender identities.

3 Security Objectives

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

3.1 Compliance with regulatory requirements

Information security must always ensure compliance with legal and internal corporate requirements. In particular, the protection of personal data is subject to stringent legal requirements. Data protection is an integral part of information security and cannot be realized without it.

3.2 Protection of company/trade secrets

Information security must secure information requiring protection of all Group companies within the EU/EEA by taking appropriate measures to ensure protection in accordance with the requirements of EU Directive 2016/943 on the protection of trade secrets and national laws that implement this directive into national law.
In principle, the Group companies outside the EU/EEA must also comply with the requirements set out in EU Directive 2016/943, insofar as there are no national requirements to the contrary.

3.3 Confidentiality

Data and information subject to protection must, regardless of their form, be adequately protected against unauthorized disclosure and unauthorized access. Depending on the degree of confidentiality and, if applicable, the need for protection of personal data, adequate protection of information requires classification with regard to its confidentiality. The Data Protection Officer of HUGO BOSS AG must be involved in the process of selecting and designing procedures for processing personal data in a timely manner.

3.4 Integrity

It is necessary to ensure the integrity and correctness of data and information requiring protection and thus also the correct functioning of relevant IT infrastructures and applications.

3.5 Availability

Data and information requiring protection and the relevant IT infrastructures and applications must have a degree of availability that ensures the operation of business-relevant processes.

(2) Due to the stringent legal requirements for data protection, the following additional security objectives are defined for the processing of personal data:

3.7 Data minimization

The planning, selection and design of IT systems and applications must be aligned with the goal of not collecting and processing more personal data than is necessary to achieve the processing purpose. The options of anonymization and pseudonymization must be made use of insofar as feasible for the purpose of the processing and in proportion to the need for protection.

3.8 Non-linking

Personal data may only be processed and evaluated for the purpose for which it was collected. As a matter of principle, personal data may not be merged if this is not covered by the purpose of processing.

3.9 Intervenability

Data subjects have the right to receive information about the processing of their personal data, to information, correction, restriction of processing and deletion of their data (so-called data subject rights). IT systems and applications must be set up in such a way that data subjects' rights are guaranteed at all times.

3.10 Transparency

Data subjects as well as operators of IT systems and applications and also supervisory authorities must be able to see at any time which personal data is collected and processed in a procedure for which purpose, which systems and processes are used for this purpose, where the data flows to for which purpose, and who bears legal responsibility for the data and systems in the various phases of data processing.

4 Target Security Level / Security Strategy

(1) In order to achieve the aforementioned security objectives and to continuously improve the information security level, HUGO BOSS is guided by the international ISO 27000/27001 standards and establishes a documented information security management system (ISMS) on this basis. The ISMS also includes the implementation of regular internal audits, appropriate control of documentation and records, management evaluation and the application of the continuous improvement model ("PDCA"). HUGO BOSS also follows the recommendations of ISO 27002.

(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 proportionate to each other. The defined security objectives must therefore be aligned with the protection requirements of the respective information, IT systems and applications. The need for protection is determined by a risk analysis of the relevant business processes. Measures are then prioritized on the basis of the respective risk profile of information, IT systems and applications.

(3) Damage incidents with significant material or immaterial consequences for HUGO BOSS must be prevented.

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

5 Responsibility and Organization

(1) Management bears overall responsibility for information security and is aware of its importance for the entire Group. With this Policy, management specifies the importance of information security and the security strategy. Management fully supports the objectives defined in this Policy as well as the measures derived and to be derived from them.

(2) The Managing Board of HUGO BOSS AG (Germany) must appoint a Central Information Security Officer (Section 7).

(3) HUGO BOSS Group companies with their own IT personnel (at least ten IT employees) must appoint a Local Information Security Contact (Section 8). Local Information Security Contacts must be appointed for the following Group companies in any case:

- 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 head of HUGO BOSS AG or a Group company is responsible for compliance with the requirements of these Policies as well as the Policies and information security measures based on them within its own area of responsibility. The (specialist) division or department head must appoint persons responsible for all information technology systems (so-called system managers).

6 Central Information Security Officer

(1) The central information security officer manages the security process and is responsible for planning, implementing, maintaining, optimizing and monitoring the Information Security Management System (ISMS). He is responsible for coordinating and monitoring all activities affecting information security.

(2) The Central Information Security Officer must be involved in all information security-related issues at an early stage.

(3) The Central Information Security Officer has the right to speak directly and at any time to the management of HUGO BOSS AG. He also has the right and the duty to involve management in central information security issues.

(4) The Central Information Security Officer must be provided with the necessary resources (personnel, time and material & investment resources) for the implementation of his tasks.

(5) The Central Information Security Officer is the contact person for all questions relating to information security and can be reached as follows:

HUGO BOSS AG
Information Security Officer
Dieselstraße 12
72555 Metzingen (Germany)
information-security@hugoboss.com

7 Local Information Security Contacts

(1) The Local Information Security Contact is responsible for monitoring and complying with the internal corporate information security requirements in his area of responsibility. He must be provided with the necessary resources (personnel, time and material & investment resources) to enable him to perform this task.

(2) The Local Information Security Contact must involve the Central Information Security Officer in all information security-related issues at an early stage.

(3) The Local Information Security Contact must report once a year to the Central Information Security Officer on the status of information security in his area of responsibility. In addition, the Central Information Security Contact may request ad hoc reports on specific information security issues as the need arises.

(4) If a breach of information security becomes known, the Local Information Security Contact must inform the Central Information Security Officer without delay.

8 Security Incident Management

(1) Information security incidents can cause great damage to HUGO BOSS. Therefore, a suitable procedure for handling information security incidents must be established (security incident management), by means of which security incidents can be quickly identified and efficiently handled.

(2) The Central Information Security Officer must draw up a Policy for the appropriate handling of security incidents (Security Incident Management Policy), which must be coordinated with the head of the IT division. Management must adopt this Policy. All employees must be made aware of the Security Incident Management Policy by means of internal company publication and it must be reviewed at least once a year by the Central Information Security Officer to determine whether any adjustments are required.

(3) 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, in the event of a security incident, the processing of personal data is affected, the Central Information Security Officer must immediately notify the Data Protection Officer of HUGO BOSS AG.

9 Obligation of Employees to Comply with the Policy

(1) All employees are obligated to observe and comply with the provisions of this Policy and the Policies and measures based thereon applicable to their workplace. Employees acting in breach of obligatory security rules will be subject to disciplinary action and may also be subject to legal consequences (e.g. warning, termination).

(2) All employees must do their part to avoid security incidents and violations of security objectives. Any detected errors and incidents must be immediately reported to the Central Information Security Officer.

10 Training and Awareness Measures

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

(2) The Central Information Security Officer must raise awareness and qualify employees in a suitable manner by means of an awareness and training program. This can be ensured, for example, through information on the company's Intranet, information letters, online-based training or classroom training.

11 Effectiveness Review

(1) HUGO BOSS regularly conducts internal audits to ensure an appropriate level of information security and to review the security process for effectiveness and efficiency. The results must be documented. In the event of deviations, corrective measures must be immediately defined and subjected to a renewed effectiveness review after implementation.

(2) Audits must be carried out in compliance with applicable data protection requirements. Measures for the purpose of employee monitoring are not permitted without the prior involvement of the Works Council and the Data Protection Officer of HUGO BOSS AG.

(3) The Central Information Security Officer must report to the management of HUGO BOSS AG once a year on the status of information security within the Group.

12 Updating the Information Security Policy

The Central Information Security Officer must review the Information Security Policy on a regular basis, but at the latest every 12 months, to determine whether any adjustments or additions are required. If necessary, the Policy must be adapted.

13 Contact Person

Questions regarding the regulations and the implementation of the Information Security Policy are to be directed to the Central Information Security Officer (item 6).

14 Final Provisions

The Information Security Policy enters into force on June 1, 2021. All employees must be made aware of it by the appropriate means.

Valid for:	HUGO BOSS	Version:	1.0
Valid from:	6/1/2021	Status:	Adopted
Adopted by:	Managing Board HUGO BOSS AG		