H U G O B O S S

Leitlinie Informationssicherheit

Version	Datum	Autor	Änderungen
1.0	07.03.2021	Nikolaus Kümmel	Erstellung Leitlinie Informationssicherheit
1.0	16.04.2021	Nikolaus Kümmel	Anpassung nach Stakeholder-Feedback
1.0	19.04.2021	Stefan Baldus	Anpassung nach Stakeholder-Feedback

Präambel

(1) HUGO BOSS ist ein globaler Fashion- und Lifestyle-Konzern im Premiumsegment und zählt zu den führenden Anbietern hochwertiger Damen- und Herrenbekleidung.

(2) Die zunehmend digitalisierten Geschäftsprozesse von HUGO BOSS hängen in hohem Maße von der Qualität der IT-Dienstleistungen und der Informations- und Kommunikationstechnik ab. Informationstechnik ist in allen Geschäftsbereichen eine wichtige Ressource. Vor allem Kunden, aber auch Mitarbeiter [1] , Lieferanten, Geschäftspartner und Aktionäre vertrauen darauf, dass ihre Daten und Informationen bei HUGO BOSS sicher sind. Um dieses Vertrauen zu rechtfertigen, müssen Integrität, Verfügbarkeit und Vertraulichkeit der Daten und Informationen in ausreichendem Maße sichergestellt sein.

(3) In dieser Leitlinie wird für alle vom Geltungsbereich dieser Richtlinie erfassten Unternehmens- und Organisationseinheiten von HUGO BOSS die grundlegende Strategie der Informationssicherheit sowie deren Organisationsstruktur festgelegt.

1 Geltungsbereich

(1) Die Leitlinie Informationssicherheit erstreckt sich auf die gesamte Informations- und Kommunikationsinfrastruktur und gilt für die HUGO BOSS AG sowie alle von ihr kontrollierten Konzerngesellschaften und die jeweiligen Mitarbeiter. Sie ist von den verantwortlichen Organen aller Konzerngesellschaften in geeigneter Weise umzusetzen. Die Einhaltung ist durch die Unternehmensleitung jeder Konzerngesellschaft dauerhaft sicherzustellen.

(2) Die Leitlinie Informationssicherheit bildet die Grundlage für erforderliche weitere Maßnahmen zur Informationssicherheit (bspw. spezifische Richtlinien, Arbeitsanweisungen, Vorlagen).

2 Stellenwert der Informationssicherheit

(1) Die Informationssicherheit hat zum Ziel, schützenswerte Unternehmensinformationen jeglicher Art, unabhängig davon, ob sie mit oder ohne Unterstützung von Informations- und Kommunikations-Technologie verarbeitet werden, entsprechend ihrem Schutzbedarf angemessen zu schützen.

(2) Der unternehmerische Erfolg von HUGO BOSS hängt maßgeblich davon ab, dass Daten und Informationen aktuell und unverfälscht sind und stets mit der gebotenen Vertraulichkeit behandelt werden. Vor allem in den Beziehungen zu Kunden, Lieferanten und Geschäftspartnern wird die Informationssicherheit immer wichtiger. Die Digitalisierungsstrategie von HUGO BOSS unterstreicht zusätzlich die Wichtigkeit der Informationssicherheit.

(3) Darüber hinaus muss die Einhaltung gesetzlicher Vorschriften (insb. betreffend den Datenschutz, den Schutz von Geschäftsgeheimnissen) gewährleistet werden.

(4) Eine Verletzung der Informationssicherheit kann zu erheblichen finanziellen Verlusten und Reputationsschäden führen.

(5) Aus diesem Grunde stellen eine funktionsfähige Informationssicherheit sowie der sicherheitsbewusste Umgang mit ihr einen entscheidenden Eckpfeiler für den Unternehmenserfolg von HUGO BOSS dar.

---

[1] Im Folgenden aus Gründen der sprachlichen Vereinfachung „Mitarbeiter" genannt. Diese Richtlinie bezieht sich jedoch ausdrücklich auf Personen aller Geschlechtsidentitäten.

3 Sicherheitsziele

(1) Zur Abbildung einer angemessenen Informationssicherheit im HUGO BOSS Konzern legt die Unternehmensleitung die nachstehenden Sicherheitsziele fest:

3.1 Einhaltung regulatorischer Vorgaben

Die Informationssicherheit muss stets die Einhaltung gesetzlicher und unternehmensinterner Anforderungen gewährleisten. Insbesondere der Schutz personenbezogener Daten unterliegt hohen gesetzlichen Anforderungen. Datenschutz ist integraler Bestandteil der Informationssicherheit und kann ohne sie nicht verwirklicht werden.

3.2 Betriebs- / Geschäftsgeheimnisschutz

Die Informationssicherheit muss schutzbedürftige Informationen aller Konzerngesellschaften innerhalb der EU / des EWR durch angemessene Maßnahmen dergestalt sichern, dass diese gemäß den Anforderungen der EU-Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen und nationalen Gesetzen, die diese Richtlinie in nationales Recht umsetzen, geschützt sind. Die Vorgaben der EU-Richtlinie 2016/943 sollen grundsätzlich auch durch die Konzerngesellschaften außerhalb der EU / des EWR eigenhalten werden, soweit keine nationalen Vorgaben entgegenstehen.

3.3 Vertraulichkeit

Schutzbedürftige Daten und Informationen sind – unabhängig von ihrer Form – vor unbefugter Preisgabe und unberechtigten Zugriffen angemessen zu schützen. Der angemessene Schutz von Informationen setzt, abhängig vom Grad der Vertraulichkeit und ggf. der Schutzbedürftigkeit personenbezogener Daten, deren Klassifizierung im Hinblick auf ihre Vertraulichkeit voraus. Im Prozess der Auswahl und Gestaltung von Verfahren zur Verarbeitung personenbezogener Daten ist der Datenschutzbeauftragte der HUGO BOSS AG rechtzeitig einzubinden.

3.4 Integrität

Die Unversehrtheit und Korrektheit von schutzbedürftigen Daten und Informationen und damit auch die korrekte Funktionsweise von relevanten IT-Infrastrukturen und Anwendungen sind sicherzustellen.

3.5 Verfügbarkeit

Schutzbedürftige Daten und Informationen sowie die relevanten IT-Infrastrukturen und Anwendungen müssen einen Grad der Verfügbarkeit aufweisen, dass der Betrieb geschäftsrelevanter Prozesse sichergestellt ist.

(2) Für die Verarbeitung personenbezogener Daten werden aufgrund der hohen gesetzlichen Anforderungen an den Datenschutz zusätzlich folgende Sicherheitsziele festgelegt:

3.7 Datenminimierung

Die Planung, Auswahl und Ausgestaltung von IT-Systemen und Anwendungen ist an dem Ziel auszurichten, dass nicht mehr personenbezogene Daten erhoben und verarbeitet werden, als für das Erreichen des Verarbeitungszwecks erforderlich ist. Von den Möglichkeiten der Anonymisierung und Pseudonymisierung ist Gebrauch zu machen, soweit dies nach dem Verarbeitungszweck möglich ist und in einem angemessenen Verhältnis zum Schutzbedarf steht.

3.8 Nichtverkettung

Personenbezogene Daten dürfen nur für denjenigen Zweck verarbeitet und ausgewertet werden, für den sie erhoben werden. Personenbezogene Daten dürfen grundsätzlich nicht zusammengeführt werden, wenn dies vom Verarbeitungszweck nicht abgedeckt ist.

3.9 Intervenierbarkeit

Betroffene haben das Recht auf Information über die Verarbeitung ihrer personenbezogenen Daten, auf Auskunft, Berichtigung, Einschränkung der Verarbeitung und Löschung ihrer Daten (sog. Betroffenenrechte). IT-Systeme und Anwendungen sind so aufzusetzen, dass die Betroffenenrechte jederzeit gewährleistet sind.

3.10 Transparenz

Betroffene sowie Betreiber von IT-Systemen und Anwendungen und auch Kontrollinstanzen müssen jederzeit erkennen können, welche personenbezogenen Daten in einem Verfahren für welchen Zweck erhoben und verarbeitet werden, welche Systeme und Prozesse dafür genutzt werden, wohin die Daten zu welchem Zweck fließen und wer die rechtliche Verantwortung für die Daten und Systeme in den verschiedenen Phasen der Datenverarbeitung trägt.

4 Angestrebtes Sicherheitsniveau / Sicherheitsstrategie

(1) Zur Erreichung der vorgenannten Sicherheitsziele und der kontinuierlichen Verbesserung des Informationssicherheitsniveaus orientiert sich HUGO BOSS an dem internationalen Standard der ISO-Normen 27000/27001 und etabliert auf dieser Basis ein dokumentiertes Informationssicherheits-Management-System (ISMS). Das ISMS umfasst auch die Durchführung von regelmäßigen internen Audits, eine geeignete Steuerung der Dokumentationen und Aufzeichnungen, eine Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung („PDCA"). HUGO BOSS orientiert sich darüber hinaus auch an den Empfehlungen der ISO 27002.

(2) HUGO BOSS ist sich darüber im Klaren, dass es eine absolute Informationssicherheit nicht gibt. Aufwand und Ergebnis der Sicherheitsmaßnahmen müssen in angemessenem Verhältnis zueinanderstehen. Die definierten Sicherheitsziele sind daher am Schutzbedarf der jeweiligen Informationen, IT-Systeme und Anwendungen auszurichten. Der Schutzbedarf wird durch eine Risikoanalyse der relevanten Geschäftsprozesse ermittelt. Die Priorisierung der Maßnahmen erfolgt dann anhand des jeweiligen Risikoprofils von Informationen, IT-Systemen und Anwendungen.

(3) Schadensfälle mit hohen materiellen oder immateriellen Auswirkungen für HUGO BOSS müssen verhindert werden.

(4) Bei der Verarbeitung personenbezogener Daten sind die Anforderungen des Datenschutzes stets uneingeschränkt zu erfüllen.

5 Verantwortung und Organisation

(1) Die Unternehmensleitung trägt die Gesamtverantwortung für die Informationssicherheit und ist sich ihrer Wichtigkeit für den gesamten Konzern bewusst. Mit dieser Leitlinie gibt die Unternehmensleitung den Stellenwert der Informationssicherheit und die Sicherheitsstrategie vor. Die Unternehmensleitung steht in vollem Umfang hinter den in dieser Leitlinie formulierten Zielen sowie den daraus abgeleiteten und abzuleitenden Maßnahmen.

(2) Der Vorstand der HUGO BOSS AG (Deutschland) benennt einen zentralen Informationssicherheitsbeauftragten (Ziff. 7).

(3) HUGO BOSS Konzerngesellschaften mit eigenem IT-Personal (ab mind. zehn IT-Mitarbeitern) benennen einen lokalen Verantwortlichen für die Informationssicherheit (Ziff. 8). Lokale Verantwortliche für die Informationssicherheit sind in jedem Fall für folgende Konzerngesellschaften zu benennen:

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

(4) Die jeweilige (Fach-) Bereichs- oder Abteilungsleitung der HUGO BOSS AG oder einer Konzerngesellschaft ist für die Einhaltung der Vorgaben dieser Leitlinie sowie darauf aufbauender Richtlinien und Maßnahmen der Informationssicherheit innerhalb des eigenen Verantwortungsbereichs verantwortlich. Die (Fach-) Bereichs- oder Abteilungsleitung benennt für alle informationstechnischen Systeme Verantwortliche (sog. Systemverantwortliche).

6 Zentraler Informationssicherheitsbeauftragter

(1) Der zentrale Informationssicherheitsbeauftragte steuert den Sicherheitsprozess und ist für die Planung, Umsetzung, Aufrechterhaltung, Optimierung und Überwachung des Informationssicherheits-Management-Systems (ISMS) verantwortlich. Er ist für die Koordination und Überwachung aller die Informationssicherheit tangierenden Aktivitäten zuständig.

(2) Der zentrale Informationssicherheitsbeauftragte ist frühzeitig in alle mit der Informationssicherheit zusammenhängenden Fragen einzubinden.

(3) Der zentrale Informationssicherheitsbeauftragte hat ein direktes und jederzeitiges Vortrags- und Vorspracherecht beim Vorstand der HUGO BOSS AG. Er hat ferner das Recht und die Pflicht, den Vorstand der HUGO BOSS AG in zentralen Fragen der Informationssicherheit einzubinden.

(4) Für die Umsetzung seiner Aufgaben ist der zentrale Informationssicherheitsbeauftragte mit den notwendigen Ressourcen (Personal, Zeit sowie Sach- und Investitionsmittel) auszustatten.

(5) Der zentrale Informationssicherheitsbeauftragte ist Ansprechpartner für alle Fragen rund um das Thema Informationssicherheit und unter folgenden Kontaktdaten zu erreichen:

HUGO BOSS AG
- Informationssicherheitsbeauftragter -
Dieselstraße 12
72555 Metzingen (Deutschland)
information-security@hugoboss.com

7 Lokale Verantwortliche für die Informationssicherheit

(1) Der lokale Verantwortliche für die Informationssicherheit ist für die Überwachung und Einhaltung der unternehmensinternen Vorgaben für die Informationssicherheit in seinem Verantwortungsbereich zuständig. Er ist mit den notwendigen Ressourcen (Personal, Zeit sowie Sach- und Investitionsmittel) auszustatten, so dass er dieser Aufgabe nachkommen kann.

(2) Der lokale Verantwortliche für die Informationssicherheit bezieht den zentralen Informationssicherheitsbeauftragten in alle mit der Informationssicherheit zusammenhängenden Fragen frühzeitig mit ein.

(3) Der lokale Verantwortliche für die Informationssicherheit berichtet einmal jährlich dem zentralen Informationssicherheitsbeauftragten über den Stand der Informationssicherheit in seinem Verantwortungsbereich. Darüber hinaus kann der zentrale Informationssicherheitsbeauftragte anlassbezogen ad-hoc-Berichte zu bestimmten Fragestellungen der Informationssicherheit anfordern.

(4) Bei Bekanntwerden einer Verletzung der Informationssicherheit informiert der lokale Verantwortliche unverzüglich den zentralen Informationssicherheitsbeauftragten.

8 Sicherheitsvorfall-Management

(1) Informationssicherheitsvorfälle können große Schäden für HUGO BOSS nach sich ziehen. Deshalb ist ein geeignetes Verfahren zur Behandlung von Informationssicherheitsvorfällen zu etablieren (Sicherheitsvorfall-Management), mittels dessen Sicherheitsvorfälle schnell erkannt und effizient behandelt werden können.

(2) Der zentrale Informationssicherheitsbeauftragte erstellt eine Richtlinie zur angemessenen Behandlung von Sicherheitsvorfällen (Richtlinie Sicherheitsvorfall-Management), die mit der Bereichsleitung IT abzustimmen ist. Die Unternehmensleitung verabschiedet diese Richtlinie. Die Richtlinie Sicherheitsvorfall-Management muss allen Mitarbeitern durch unternehmensinterne Veröffentlichung bekannt gemacht und mindestens einmal jährlich durch den zentralen Informationssicherheitsbeauftragten auf Anpassungsbedarf überprüft werden.

(3) Bei Sicherheitsvorfällen ist der zentrale Informationssicherheitsbeauftragte berechtigt, erforderliche Sicherheitsmaßnahmen auch kurzfristig umzusetzen oder anzuordnen. Ist bei einem Sicherheitsvorfall die Verarbeitung personenbezogener Daten betroffen, ist der Datenschutzbeauftragte der HUGO BOSS AG unverzüglich durch den zentralen Informationssicherheitsbeauftragten zu informieren.

9 Verpflichtung der Mitarbeiter zur Einhaltung der Leitlinie

(1) Jeder Mitarbeiter ist verpflichtet, die Vorgaben dieser Leitlinie sowie darauf aufbauender Richtlinien und Maßnahmen der Informationssicherheit für seinen Arbeitsplatz zu beachten und einzuhalten. Verstöße der Mitarbeiter gegen verpflichtende Sicherheitsregeln werden disziplinarisch geahndet und können ggf. auch zu rechtlichen Konsequenzen führen (bspw. Abmahnung, Kündigung).

(2) Jeder Mitarbeiter soll dazu beitragen, Sicherheitsvorfälle und Verletzungen der Sicherheitsziele zu vermeiden. Erkannte Fehler und Ereignisse sind umgehend dem zentralen Informationssicherheitsbeauftragten zu melden.

10 Schulungs- und Sensibilisierungsmaßnahmen

(1) Informationssicherheit kann nur dann hinreichend wirksam sein, wenn alle Mitarbeiter die möglichen Gefährdungen für die Informationssicherheit kennen und in ihren Aufgabenbereichen entsprechend verantwortlich handeln.

(2) Der zentrale Informationssicherheitsbeauftragte sensibilisiert und qualifiziert die Mitarbeiter mit einem Sensibilisierungs- und Schulungsprogramm in geeigneter Art und Weise. Dies kann bspw. durch Informationen über das firmeninterne Intranet,

Informationsschreiben, onlinebasierte Schulungen oder Präsenzschulungen sichergestellt werden.

11 Erfolgskontrolle

(1) HUGO BOSS führt regelmäßig interne Audits durch, um ein angemessenes Informationssicherheitsniveau zu gewährleisten und den Sicherheitsprozess auf Wirksamkeit und Effizienz zu prüfen. Die Ergebnisse sind zu dokumentieren. Im Fall von Abweichungen sind unmittelbar Abhilfemaßnahmen zu definieren und diese nach Umsetzung einer erneuten Wirksamkeitsprüfung zu unterziehen.

(2) Auditierungen erfolgen unter Beachtung geltender Datenschutzvorgaben. Maßnahmen zum Zwecke der Mitarbeiterüberwachung sind nicht ohne vorherige Einbeziehung des Betriebsrats und des Datenschutzbeauftragten der HUGO BOSS AG zulässig.

(3) Der zentrale Informationssicherheitsbeauftragte berichtet dem Vorstand der HUGO BOSS AG einmal jährlich über den Stand der Informationssicherheit im Konzern.

12 Aktualisierung der Leitlinie Informationssicherheit

Der zentrale Informationssicherheitsbeauftragte prüft die Leitlinie Informationssicherheit regelmäßig, spätestens aber alle zwölf Monate auf Anpassungs- und Ergänzungsbedarf. Sofern notwendig, hat eine Anpassung der Leitlinie zu erfolgen.

13 Ansprechpartner

Fragen hinsichtlich der Regelungen und der Umsetzung der Leitlinie Informationssicherheit sind an den zentralen Informationssicherheitsbeauftragten zu richten (Ziff. 6).

14 Schlussbestimmungen

Die Leitlinie Informationssicherheit tritt am 1. Juni 2021 in Kraft. Sie ist allen Mitarbeitern in geeigneter Art und Weise bekannt zu machen.

Gültig für:	HUGO BOSS	Version:	1.0
Gültig ab:	01.06.2021	Status:	Verabschiedet
Verabschiedet durch:	Vorstand HUGO BOSS AG		