Information Security &
IT-Compliance

HUGO BOSS
Leitlinie Informationssicherheit

HUGO BOSS

Änderungshistorie

Version	Gültig von	Autor	Notiz
1.0	07.03.2021	Nikolaus Kümmel	Erstellung einer Richtlinie zur Informationssicherheit
1.0	16.04.2021	Nikolaus Kümmel	Anpassung nach Feedback von Interessengruppen
1.0	19.04.2021	Stefan Baldus	Anpassung nach Feedback von Interessengruppen
1.1	10.02.2023	Steffen Schellig	Jährliche Prüfung
1.2	11.03.2024	Furuzan Hadi	Inhaltliche Anpassungen in Kapitel 3.1, 3.2 Sicherheitsziele
1.3	18.02.2025	Stefan Baldus	Aktualisierte Formulierungen und verbesserte Schreibweise
1.4	05.06.2025	Steffen Schellig	Übergang zur neuen Struktur

KURZFASSUNG

Diese Richtlinie wurde mit Unterstützung einer KI übersetzt und kann grammatikalische oder sprachliche Fehler enthalten. Im Zweifelsfall ist die Originalversion maßgeblich. Wir bitten um Ihr Verständnis.

Die HUGO BOSS Informationssicherheitsrichtlinie legt einen umfassenden Rahmen fest, um die Vertraulichkeit, Integrität und Verfügbarkeit von Daten im gesamten Unternehmen zu gewährleisten. Sie gilt für alle Mitarbeiter, Systeme und Prozesse innerhalb der HUGO BOSS AG und ihrer Tochtergesellschaften und unterstützt die Digitalisierungsstrategie des Unternehmens sowie die Einhaltung rechtlicher und regulatorischer Anforderungen.
Die wichtigsten Highlights sind:

- **Sicherheitsziele:** Fokus auf Compliance, Schutz von Geschäftsgeheimnissen, Vertraulichkeit, Integrität, Verfügbarkeit, Datenminimierung und Transparenz.
- **Führungsstruktur:** Ein zentraler Beauftragter für Informationssicherheit überwacht das Informationssicherheits-Managementsystem (ISMS) und wird von lokalen Sicherheitsbeauftragten in den wichtigsten Regionen unterstützt.
- **Vorfall-Management:** Ein solides Verfahren zur Identifizierung, Verwaltung und Behebung von Sicherheitsvorfällen mit klaren Eskalationsprotokollen.
- **Verantwortung der Mitarbeiter:** Alle Mitarbeiter sind verpflichtet, die Richtlinie zu befolgen und aktiv zur Vermeidung von Sicherheitsvorfällen beizutragen.
- **Kontinuierliche Verbesserung:** Regelmäßige Audits, Schulungsprogramme und Aktualisierungen des Leitfadens gewährleisten die Anpassung an sich entwickelnde Risiken und Standards, einschließlich ISO/IEC 27001.

Diese Richtlinie unterstreicht das Engagement von HUGO BOSS für den Schutz von Daten und die Aufrechterhaltung des Vertrauens bei Kunden, Mitarbeitern und Partnern. Sie ist ein Eckpfeiler für die operative Belastbarkeit und den langfristigen Erfolg des Unternehmens.

HUGO BOSS

INHALT

1 ZWECK

(1) HUGO BOSS ist ein globaler Mode- und Lifestyle-Konzern im Premium-Segment und gehört zu den führenden Anbietern von 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 Kommunikationstechnologie ab. Die Informationstechnologie ist eine wichtige Ressource in allen Geschäftsbereichen. Insbesondere 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, muss die Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Informationen ausreichend gewährleistet sein.

(3) Diese Richtlinie definiert die grundlegende Strategie der Informationssicherheit und ihre Organisationsstruktur für alle HUGO BOSS Unternehmens- und Organisationseinheiten, die in den Geltungsbereich dieser Richtlinie fallen.

2 GELTUNGSBEREICH

(1) Die Informationssicherheitsrichtlinie umfasst die gesamte Informations- und Kommunikationsinfrastruktur und gilt für die HUGO BOSS AG sowie alle von ihr kontrollierten Konzernunternehmen und die jeweiligen Mitarbeiter. Sie muss von den zuständigen Abteilungen aller Konzernunternehmen umgesetzt werden. Die Einhaltung muss von der Geschäftsführung jeder Konzerngesellschaft dauerhaft sichergestellt werden.

(2) Die Informationssicherheitsleitlinie bildet die Grundlage für den Informationssicherheitsrahmen und weitere notwendige Informationssicherheitsmaßnahmen (z.B. verschiedene Richtlinien, Arbeitsanweisungen, Vorlagen).

3 BEDEUTUNG DER INFORMATIONSSICHERHEIT

(1) Das Ziel der Informationssicherheit ist es, alle Arten von Unternehmensinformationen, unabhängig davon, ob sie mit oder ohne Unterstützung von Informations- und Kommunikationstechnologie verarbeitet werden, entsprechend der Risikobewertung angemessen zu schützen.

(2) Der Geschäftserfolg von HUGO BOSS hängt in hohem Maße davon ab, dass Daten und Informationen aktuell sind, nicht verändert werden und stets mit der notwendigen Vertraulichkeit behandelt werden. Die Informationssicherheit wird immer wichtiger, insbesondere in den Beziehungen zu Kunden, Lieferanten und Geschäftspartnern. Die Informationssicherheit unterstützt die Digitalisierungsstrategie von HUGO BOSS.

(3) Darüber hinaus muss die Einhaltung gesetzlicher/regulatorischer Anforderungen (insbesondere im Hinblick auf die im Rechtsregister des HUGO BOSS Konzerns als anwendbar gekennzeichneten rechtlichen Anforderungen) sichergestellt werden.

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

(5) Aus diesem Grund stellen eine effektive Informationssicherheit und der richtige Umgang mit ihr einen entscheidenden Eckpfeiler für den Unternehmenserfolg von HUGO BOSS dar.

[1] Im Folgenden aus Gründen der sprachlichen Vereinfachung als "Mitarbeiter" bezeichnet. Dieser Leitfaden bezieht sich jedoch ausdrücklich auf Personen aller Geschlechtsidentitäten.

4 SICHERHEITSZIELE

(1) Um eine angemessene Informationssicherheit innerhalb des HUGO BOSS Konzerns zu gewährleisten, hat die Unternehmensleitung die folgenden übergreifenden Sicherheitsziele definiert:

4.1 Einhaltung der gesetzlichen Vorschriften

Die Informationssicherheit muss stets die Einhaltung gesetzlicher und unternehmensinterner Anforderungen gewährleisten. So unterliegt beispielsweise der Schutz personenbezogener Daten hohen gesetzlichen Anforderungen. Es ist daher notwendig, dass HUGO BOSS in Abstimmung mit der Rechtsabteilung die geltenden Gesetze und Vorschriften berücksichtigt und einhält.

4.2 Schutz von Betriebs- und Geschäftsgeheimnissen

Die Informationssicherheit muss Unternehmensinformationen innerhalb der EU/des EWR durch geeignete Maßnahmen so sichern, dass sie gemäß den Anforderungen der EU-Richtlinie 2016/943 zum Schutz von Geschäftsgeheimnissen und den geltenden nationalen Gesetzen geschützt sind.
Für Konzernunternehmen außerhalb der EU sind die jeweiligen nationalen Vorschriften zum Schutz von Betriebs- und Geschäftsgeheimnissen zu beachten, soweit sie bestehen und von der HUGO BOSS Rechtsabteilung dokumentiert sind. Sofern anwendbar und nicht im Widerspruch zu nationalen Gesetzen, gelten die Bestimmungen der EU-Richtlinie zum Schutz von Geschäftsgeheimnissen auch für Konzernunternehmen außerhalb der EU.

4.3 Vertraulichkeit

Schutzbedürftige Daten und Informationen - unabhängig von ihrer Form - müssen angemessen vor unbefugter Offenlegung und unbefugtem Zugriff geschützt werden. Der angemessene Schutz von Informationen erfordert die Einstufung aller Daten im Hinblick auf ihre Vertraulichkeit, je nach Grad der Vertraulichkeit und gegebenenfalls der Schutzbedürftigkeit. Der Datenschutzbeauftragte des HUGO BOSS Konzerns muss in den Prozess der Auswahl und Gestaltung der Verfahren zur Verarbeitung personenbezogener Daten einbezogen werden.

4.4 Integrität

Die Genauigkeit und Zuverlässigkeit von Daten und Informationen, die geschützt werden müssen, sowie das ordnungsgemäße Funktionieren wichtiger IKT-Infrastrukturen und -Anwendungen müssen gewährleistet sein.

4.5 Verfügbarkeit

Schutzbedürftige Daten und Informationen sowie die entsprechenden IKT-Infrastrukturen und -Anwendungen müssen ein Verfügbarkeitsniveau aufweisen, das den Betrieb geschäftsrelevanter Prozesse auf der Grundlage ihrer Geschäftskritikalität gewährleistet.

(2) Aufgrund der hohen gesetzlichen Anforderungen an den Datenschutz werden für die Verarbeitung personenbezogener Daten die folgenden Ziele festgelegt:

4.6 Datenminimierung

Die Auswahl und Gestaltung von IT-Systemen und -Anwendungen muss sich an dem Ziel orientieren, dass keine personenbezogenen Daten über das zur Erreichung des Zwecks der Verarbeitung notwendige Maß hinaus erhoben und verarbeitet werden. Wo immer möglich, sollte eine Anonymisierung oder Maskierung von Daten entsprechend der Sensibilität der Daten vorgenommen werden.

4.7 Nicht-verknüpfend

Personenbezogene Daten dürfen nur für den Zweck verarbeitet und analysiert werden, für den sie erhoben wurden. Personenbezogene Daten dürfen nicht zusammengeführt werden, wenn dies nicht durch den Verarbeitungszweck gedeckt ist.

4.8 Intervenierbarkeit

Betroffene Personen haben das Recht auf Information über die Verarbeitung ihrer personenbezogenen Daten, auf Zugang, Berichtigung, Einschränkung der Verarbeitung und Löschung ihrer Daten (sogenannte Betroffenenrechte). Die IT-Systeme und -Anwendungen müssen so eingerichtet werden, dass die Rechte der betroffenen Personen stets gewährleistet sind.

4.9 Transparenz

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

5 ANGESTREBTE SICHERHEITSSTUFE / SICHERHEITSSTRATEGIE

(1) Zur Erreichung der vorgenannten Sicherheitsziele und der kontinuierlichen Verbesserung des Informationssicherheitsniveaus setzt HUGO BOSS die internationale Norm ISO/IEC 27001 (in der jeweils gültigen Fassung) um und betreibt auf dieser Grundlage ein dokumentiertes Informationssicherheitsmanagementsystem (ISMS). Das ISMS umfasst auch ein Risikomanagement, die Durchführung regelmäßiger interner Audits, eine angemessene Kontrolle der Dokumentation und der Aufzeichnungen, eine Managementbewertung und die Anwendung des Modells der kontinuierlichen Verbesserung ("PDCA"). HUGO BOSS orientiert sich auch an den Empfehlungen der ISO/IEC 27002 (in der jeweils gültigen Fassung).

(2) HUGO BOSS ist sich bewusst, dass es so etwas wie absolute Informationssicherheit nicht gibt. Der Aufwand und das Ergebnis der Sicherheitsmaßnahmen müssen in einem vernünftigen Verhältnis zueinander stehen. Das Risikoniveau und die damit verbundenen Sicherheitsziele werden durch eine Risikoanalyse der relevanten Geschäftsprozesse bestimmt und aufeinander abgestimmt. Die Maßnahmen werden dann auf der Grundlage des jeweiligen Risikoprofils von Informationen, IT-Systemen und Anwendungen nach Prioritäten geordnet.

(3) Schadensfälle mit hohen materiellen oder immateriellen Folgen für HUGO BOSS müssen verhindert werden. HUGO BOSS hat einen risikobasierten Ansatz, um die Auswirkungen zu klassifizieren.

(4) Bei der Verarbeitung personenbezogener Daten müssen die Anforderungen des Datenschutzes stets in vollem Umfang erfüllt werden.

6 VERANTWORTUNG UND ORGANISATION

(1) Die Unternehmensleitung trägt die Gesamtverantwortung für die Informationssicherheit und ist sich ihrer Bedeutung für den gesamten Konzern bewusst. Mit dieser Leitlinie definiert die Unternehmensleitung die Bedeutung der Informationssicherheit und die Sicherheitsstrategie. Die Unternehmensleitung unterstützt die in dieser Leitlinie formulierten Ziele und die daraus abgeleiteten und abzuleitenden Maßnahmen voll und ganz.

(2) Der Vorstand der HUGO BOSS AG (Deutschland) ernennt einen zentralen Informationssicherheitsbeauftragten (§ 6).

(3) HUGO BOSS Konzerngesellschaften mit eigenem IT-Personal (mindestens zehn IT-Mitarbeiter) benennen einen lokalen Verantwortlichen für Informationssicherheit (Abschnitt 7). Standorte und Tochtergesellschaften mit weniger Personal unterstehen der Leitung des zentralen Informationssicherheitsbeauftragten. Für die folgenden Konzernunternehmen müssen in jedem Fall lokale Informationssicherheitsbeauftragte benannt werden:

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

(4) Die jeweilige (Fach-) Bereichs- oder Abteilungsleitung der HUGO BOSS AG oder einer Konzerngesellschaft ist für die Einhaltung der Anforderungen dieser Richtlinie und der darauf basierenden Informationssicherheitsrichtlinien und -maßnahmen im eigenen Verantwortungsbereich verantwortlich. Die (Fach-) Bereichs- oder Abteilungsleitung ernennt Verantwortliche für alle informationstechnischen Systeme (sog. Systemverantwortliche).

7 ZENTRALER BEAUFTRAGTER FÜR INFORMATIONSSICHERHEIT

(1) Der zentrale Beauftragte für Informationssicherheit steuert den Sicherheitsprozess und ist für die Planung, Umsetzung, Pflege, Optimierung und Überwachung des Informationssicherheitsmanagementsystems (ISMS) verantwortlich. Er oder sie ist für die Koordination und Überwachung aller Aktivitäten im Bereich der Informationssicherheit zuständig.

(2) Der zentrale Beauftragte für Informationssicherheit wird frühzeitig in alle Fragen der Informationssicherheit einbezogen.

(3) Der zentrale Informationssicherheitsbeauftragte hat das Recht, sich jederzeit direkt an den Vorstand der HUGO BOSS AG und aller Konzerngesellschaften zu wenden. Er hat auch das Recht und die Pflicht, den Vorstand in wichtigen Fragen der Informationssicherheit einzubeziehen.

(4) Der zentrale Beauftragte für Informationssicherheit wird mit den notwendigen Ressourcen (Personal, Zeit, Material und Mittel) ausgestattet, um seine Aufgaben zu erfüllen.

(5) Der zentrale Beauftragte für Informationssicherheit ist der Ansprechpartner für alle Fragen zur Informationssicherheit und kann unter den folgenden Kontaktdaten erreicht werden:

HUGO BOSS AG
- Beauftragter für Informationssicherheit -
Heilige Allee 3
72555 Metzingen (Deutschland)
information-security@hugoboss.com

8 LOKALE VERANTWORTLICHE FÜR DIE INFORMATIONSSICHERHEIT

(1) Der lokale Verantwortliche für Informationssicherheit ist für die Überwachung und Einhaltung der unternehmensinternen Anforderungen an die Informationssicherheit in seinem Verantwortungsbereich zuständig. Ihm werden die notwendigen Ressourcen (Personal, Zeit, Material und Mittel) zur Verfügung gestellt, damit er diese Aufgabe erfüllen kann.

(2) Der lokale Informationssicherheitsverantwortliche bezieht den zentralen Informationssicherheitsbeauftragten frühzeitig in alle Fragen der Informationssicherheit ein.

(3) Der lokale Beauftragte für Informationssicherheit berichtet dem zentralen Beauftragten für Informationssicherheit mindestens einmal jährlich über den Stand der Informationssicherheit in seinem Zuständigkeitsbereich. Darüber hinaus kann der zentrale Beauftragte für Informationssicherheit Ad-hoc-Berichte zu bestimmten Fragen der Informationssicherheit anfordern.

(4) Wenn eine Verletzung der Informationssicherheit bekannt wird, informiert die lokal verantwortliche Person den zentralen Beauftragten für Informationssicherheit unverzüglich.

(5) Eine Liste der ernannten lokalen Informationssicherheitsverantwortlichen ist dieser Richtlinie beigefügt.

9 MANAGEMENT VON SICHERHEITSVORFÄLLEN

(1) Informationssicherheitsvorfälle können zu großen Schäden für den HUGO BOSS Konzern führen. Aus diesem Grund wurde ein geeigneter Leitfaden für den Umgang mit Informationssicherheitsvorfällen erstellt, mit dessen Hilfe Sicherheitsvorfälle schnell erkannt und effizient behandelt werden können.

(2) Im Falle von Sicherheitsvorfällen ist der zentrale Informationssicherheitsbeauftragte befugt, auch kurzfristig notwendige Sicherheitsmaßnahmen durchzuführen oder anzuordnen. Tritt ein Sicherheitsvorfall ein, der personenbezogene Daten betrifft, muss der Datenschutzbeauftragte unverzüglich informiert werden.

10 VERPFLICHTUNG DER MITARBEITER ZUR EINHALTUNG DER RICHTLINIE

(1) Jeder Mitarbeiter ist verpflichtet, die Bestimmungen dieser Richtlinie und des Informationssicherheitsrahmens (diese Richtlinie und alle anderen, die in der Informationssicherheit SharePoint veröffentlicht sind) und darauf basierende Maßnahmen für seinen Arbeitsplatz zu beachten und einzuhalten. Verstöße von Mitarbeitern gegen verbindliche Sicherheitsregeln haben disziplinarische Maßnahmen zur Folge und können auch rechtliche Konsequenzen nach sich ziehen (z.B. Abmahnung, Kündigung).

(2) Jeder Mitarbeiter sollte dazu beitragen, Sicherheitsvorfälle und Verstöße gegen die Sicherheitsziele zu verhindern. Erkannte Fehler und Vorfälle müssen sofort über ein Service Desk Ticket per E-Mail oder Anruf gemeldet werden.

11 SCHULUNGS- UND SENSIBILISIERUNGSMASSNAHMEN

(1) Die Informationssicherheit kann nur dann hinreichend wirksam sein, wenn alle Mitarbeiter sich der potenziellen Bedrohungen für die Informationssicherheit bewusst sind und in ihrem Verantwortungsbereich verantwortungsbewusst handeln.

(2) Der zentrale Informationssicherheitsbeauftragte sensibilisiert und qualifiziert die Mitarbeiter mit einem Awareness- und Schulungsprogramm in geeigneter Weise. Dies kann z.B. durch Informationen im Intranet des Unternehmens, Informationsschreiben, Online-Schulungen oder Präsenzschulungen gewährleistet werden.

12 LEISTUNGSBEURTEILUNG

(1) HUGO BOSS führt regelmäßig interne Audits durch, um ein angemessenes Niveau der Informationssicherheit zu gewährleisten und die Effektivität und Effizienz des Sicherheitsprozesses zu überprüfen. Die Ergebnisse müssen dokumentiert werden. Bei Abweichungen müssen

Korrekturmaßnahmen festgelegt und nach der Umsetzung einer erneuten Wirksamkeitsprüfung unterzogen werden.

(2) Audits werden unter Beachtung der geltenden Datenschutzbestimmungen durchgeführt. Maßnahmen zum Zwecke der Mitarbeiterüberwachung sind ohne vorherige Beteiligung des Betriebsrats und des Datenschutzbeauftragten nicht zulässig.

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

13 AKTUALISIERUNG UND ÜBERARBEITUNG

Es liegt in der Verantwortung des Teams für Informationssicherheit und IT-Compliance, diese Richtlinie mindestens alle drei Jahre zu überprüfen oder sobald sich Änderungen zum Thema ergeben. Falls erforderlich, muss die Richtlinie angepasst werden.

14 GÜLTIGKEIT UND INKRAFTTRETEN

Diese Richtlinie tritt am 01. Juni 2021 in Kraft und jeder Mitarbeiter ist verpflichtet, die Bestimmungen dieser Richtlinie und darauf basierende Maßnahmen für seinen Arbeitsplatz zu beachten und einzuhalten. Verstöße von Mitarbeitern gegen verbindliche Sicherheitsvorschriften können disziplinarische Maßnahmen nach sich ziehen und auch zu rechtlichen Konsequenzen führen (z.B. Abmahnung, Kündigung).

15 KONTAKTE

Das Team für Informationssicherheit und IT-Compliance steht Ihnen bei Fragen zu dieser Richtlinie unter information-security@hugoboss.com zur Verfügung.

Gültig für:	HUGO BOSS	Version:	1.4
Gültig ab:	18.02.2025	Status:	freigegeben, gültig
Genehmigt durch:	Vorstand der HUGO BOSS AG	Letzte Aktualisierung:	05.06.2025
Eigentümer der Richtlinie:	Informationssicherheit & IT-Compliance	Klassifizierung:	öffentlich