Informationssicherheits-Leitlinie

der

Securitas Holding GmbH und die mit ihr verbundenen Unternehmen (kurz: Securitas)

Autor:	Antonio Valls Ruiz
Dokumentinhaber:	ISB
Dokumentenkategorie:	strategisch
Klassifizierung:	öffentlich

Datum:
04.08.2023

Revision:
4

Autor(en):
Antonio Valls Ruiz

Prüfer:
ISMT

Freigeber:
Andreas Ritsch

Dokumenthistorie

Revision	Datum	Bearbeiter	Beschreibung	Status[1]
0.9	15.10.2018	Antonio Valls Ruiz	Finale Fassung zur Unterschrift	erledigt
1	01.01.2019	Manfred Buhl	Freigabe	freigegeben
1.1	11.12.2020	ISMT	Anpassung der Leitlinie um Schulung und Sensibilisierung	erledigt
2	15.12.2020	Herwarth Brune	Freigabe	freigegeben
2.1	13.05.2022	Antonio Valls Ruiz	Anpassung um Datenschutz und neue CI	erledigt
2.2	17.05.2022	Maximilian Merken	QM-Prüfung	erledigt
3	20.05.2022	Ralf Brümmer	Freigabe	freigegeben
3.1	19.07.2023	Antonio Valls Ruiz	Anpassung an neue RL 0001	erledigt
3.2	24.07.2023	Maximilian Merken	QM-Prüfung	Erledigt
3.3	04.08.2023	ISMT	Redaktionelle Änderungen	in Bearbeitung
4	04.08.2023	Antonio Valls Ruiz	Freigabe-Workflow	Freigegeben

Referenzdokumente

Nr.	Dokumentname	Stand[2]
1	DIN ISO 27001:2017 (deutsch)	In der aktuellen Version
2	DIN ISO 27002:2016-11 (deutsch)	In der aktuellen Version
3	DIN ISO 27701:2021	In der aktuellen Version
4	Informationssicherheitsorganisation	In der aktuellen Version
5	Group Enterprise Risk Management	In der aktuellen Version

Hinweis:

Aus Gründen der besseren Lesbarkeit wird aufgrund der Vielzahl der Geschlechter innerhalb dieser Leitlinie das geschlechtsneutral zu verstehendem generische Maskulinum als Formulierungsvariante verwendet. Sämtliche Mitarbeiter-Bezeichnungen und Regelungen gelten daher auch ohne ausdrückliche Nennung für Beschäftigte jeden Geschlechts gleichermaßen.

[1] Zu verwenden sind: in Bearbeitung, vorgelegt, freigegeben.

[2] Es gilt die jeweils letzte freigegebene Revisionen.

Securitas

Inhaltsverzeichnis

1 Einleitung

Diese Leitlinie zur Informationssicherheit enthält generelle Vorgaben für die Handhabung von Informationen / Daten. Detailliertere Vorgaben sind in weiteren strategischen und taktischen Richtlinien aufgeführt und werden fortlaufend aktualisiert. Dies ist die Hauptrichtlinie zur Informationssicherheit, die als Grundlage für die Sicherung und Bewahrung der Datenbestände der Securitas dient. Sie umfasst den Gesamtrahmen für das Informationssicherheits-Management, einschließlich der Leit- und Grundsätze des Securitas Konzerns.

1.1 Geltungsbereich

Diese Richtlinie gilt für die Securitas Holding GmbH und die mit ihr verbundenen Unternehmen in Deutschland, alle Mitarbeiter des Unternehmens sowie externe Mitarbeiter und ggf. Lieferanten sind angehalten, die nachfolgende beschriebene Richtlinie einzuhalten.

1.2 Klassifikation

Dieses Dokument ist eine „strategische“ Richtlinie.

Es ist mit der Informationsklassifizierung „öffentlich“ versehen.

1.3 Zuständigkeiten und Änderungen

Zuständig für die Erstellung und Aktualisierung des Inhaltes von Dokumenten ist der Dokumenteninhaber.

Der Dokumentinhaber ist verpflichtet mindestens jährlich oder bei signifikanten Änderungen das Dokument zu kontrollieren und zu aktualisieren.

Zu den weiteren Aufgaben des Dokumentinhaltes gehören die Erstellung, Pflege und Sicherstellung der Nachvollziehbarkeit von Änderungen, Revisionen und Archivierungen.

1.4 Freigabe / Veröffentlichung

Diese Dokumente und ihre Revisionen sind vom Dokumenteninhaber wie folgt freizugeben:

1. „strategische“ Dokumente von der **Geschäftsleitung der Securitas Holding GmbH oder dem General Counsel / Head of Legal, Risk & QM**
2. „taktische“ Dokumente vom **Department Head (Abteilungsleiter)** und
3. „operative“ Dokumente von der **Geschäftsbereichsleitung** (z. B. Department Head (Abteilungsleiter), Area Manager, Branch Manager / Supervisor / Team Leader, etc.)

Die Dokumente stehen in vorbezeichneter, hierarchischer Rangordnung zueinander, bei welcher die ranghöheren Dokumente den rangniedrigeren Dokumenten und deren Inhalt vorgehen.

„Strategische“ und „taktische“ Dokumente sind Bestandteil des jeweiligen Managementsystems der Securitas und müssen vor der Freigabe und Veröffentlichung zur Qualitätssicherung an den Qualitätsmanagementbeauftragten (QMB) der Securitas Holding GmbH gesendet werden.

Die Veröffentlichung von „strategischen“ und „taktischen“ Dokumenten erfolgt durch den QMB auf der SharePoint Seite des QMB. Der Dokumentinhaber soll nach Möglichkeit eine Veröffentlichung in seinem Bereich ebenfalls vornehmen und muss das Dokument und seine Aktualisierungen an Mitarbeiter im Geltungsbereich des Dokumentes per Mail bekanntgeben.

Die Veröffentlichung von „operativen“ Dokumenten soll durch den Dokumentinhaber nach Freigabe auf der SharePoint oder einem vergleichbar zugänglichen Medium seines Zuständigkeitsbereiches erfolgen. Er hat das Dokument schriftlich oder per Mail an alle Mitarbeiter im Geltungsbereich des Dokumentes bekanntzugeben.

Vorgängerdokumente sind mit der neuen Version ungültig.

1.5 Begriffe

Siehe Glossar

1.6 Verstöße

Als Verstöße gelten schuldhafte Handlungen, die aufgrund einer Abweichung von der „Leitlinie zur Informationssicherheit“, die

- den unberechtigten Zugriff auf Informationen, deren Preisgabe und / oder Änderung zulassen,
- die Nutzung von bei der Securitas verarbeiteten Informationen für illegale Zwecke beinhalten und
- einen Imageschaden hinsichtlich eines schlechten Informationssicherheitsniveaus bei der Securitas zur Folge haben.

1.7 Konsequenzen

Die Nichteinhaltung der Leitlinie für die Informationssicherheit oder der daraus abgeleiteten Sicherheitsrichtlinien kann zu arbeitsrechtlichen Konsequenzen und straf- / zivilrechtlichen Verfahren führen.

2 Informationssicherheitsleitlinie

Für die Securitas ist eine sichere und zuverlässige Informations- und Kommunikationstechnik von höchster Bedeutung. Sie ist darüber hinaus ein unerlässliches Qualitätsmerkmal.

Informationen, welche von der Securitas Deutschland und ihren verbundenen Unternehmen erhoben, verarbeitet, genutzt, übermittelt und gespeichert werden, sind einerseits die Grundlage vieler Geschäftsprozesse, unterliegen andererseits jedoch der Gefahr von Missbrauch, Sabotage und Verlust. Mitarbeiter und Kunden erwarten, dass ihre Informationen geschützt werden. Dieser Schutz soll in Art und Umfang dem Wert der Informationen angemessen sein. Alle technischen, infrastrukturellen, personellen und organisatorischen Maßnahmen, die dem Schutz von Informationen – also der Informationssicherheit – dienen, sind somit für das Unternehmen von strategischer Bedeutung.

Alle Anforderungen, welche in diesem und allen anderen Dokumenten des Informationssicherheits-Managementsystems (ISMS) der Securitas Deutschland formuliert werden, beziehen sich sowohl auf die Informationssicherheit im Sinne der Norm ISO/IEC 27001 als auch auf den Schutz von personenbezogenen Daten (Datenschutz) im Sinne der Norm ISO/IEC 27701, der EU-Datenschutzgrundverordnung (EU-DSVO) und des Bundesdatenschutzgesetzes (BDSG). Zur besseren Lesbarkeit wird in allen Dokumenten des ISMS, sofern es nicht explizit um datenschutzrelevante Zusammenhänge geht, nur der Begriff „Informationssicherheit“ verwendet.

2.1 Sicherheitsziele

2.1.1 Grundwerte der Informationssicherheit

Die Wahrung der Sicherheit von Informationen bezieht sich auf die folgenden Grundwerte:

- **Vertraulichkeit**: Schutz vor unberechtigtem Zugriff auf Informationen.
- **Integrität**: Schutz vor ungewollter Verfälschung von Informationen.
- **Verfügbarkeit**: Schutz vor ungewollter Beeinträchtigung des Zugriffs auf Informationen.

2.1.2 Angestrebtes Sicherheitsniveau

Für die Securitas wird ein gehobenes Maß an Informationssicherheit angestrebt. Das bedeutet insbesondere, dass bei Verstößen gegen die Grundwerte der Informationssicherheit (s. o.) das Schadensausmaß in der Regel keine signifikanten oder existenzbedrohlichen Ausmaße [3] annehmen soll.

Es ist sicherzustellen, dass dem Schutzbedarf angemessene und dem Stand der Technik entsprechende Sicherheitsmaßnahmen ergriffen werden, um den erforderlichen Schutz der Informationen / Daten sowie die notwendige Verfügbarkeit der IT-Systeme zu gewährleisten. Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systeme stehen.

Gesetzesverstöße werden nicht toleriert. Alle Mitarbeiter der Securitas und Dritte, derer sich Securitas zur Aufgabenerfüllung bedient haben alle einschlägigen Gesetze (z. B. Strafgesetzbuch, Gesetze und Regelungen zum Datenschutz) einzuhalten.

Alle Mitarbeiter sind sich ihrer Verantwortung beim Umgang mit Informationen (analog wie digital) bewusst und unterstützen die Sicherheitsstrategie nach besten Kräften.

[3] Siehe Referenzdokument #4

2.1.3 Die Sicherheitsprinzipien der Securitas

Bei der Umsetzung der Informationssicherheit in der Securitas sind die folgenden Sicherheitsprinzipien einzuhalten:

- **Prinzip des „aufgeräumten" Arbeitsplatzes**
  Bei Abwesenheit wird der Zugang und Zugriff auf vertrauliche Unterlagen (Papier, Datenträger) durch Unbefugte verhindert.
- **Prinzip des „gesperrten" Bildschirmes**
  Bei Abwesenheit wird der Zugang und Zugriff auf vertrauliche Daten und Anwendungen durch Unbefugte verhindert.
- **Prinzip des minimalen Zugriffs** (need to know)
  Jeder Nutzer erhält nur die Zugriffsrechte, die zur Erfüllung der jeweiligen Aufgabe, insbesondere unter Wahrung der datenschutzrechtlichen Bestimmungen, erforderlich sind.
- **Prinzip der Nachvollziehbarkeit und Nachweisbarkeit**
  Ziel ist es, alle sicherheitsrelevanten Aktivitäten nachvollziehbar zu gestalten, die Verantwortlichen eindeutig identifizieren zu können sowie Datenmaterial für Streitfälle / Unstimmigkeiten in einem angemessenen Maße insbesondere unter Beachtung der geltenden Datenschutzbestimmungen vorzuhalten und zu erheben. Dies umfasst die Nachvollziehbarkeit von Datenzugriffen, Transaktionen und der (geschäftlichen) Kommunikation zwischen den jeweiligen Stakeholdern[4]. Dabei ist die Integrität der Daten und Informationen stets zu gewährleisten.
- **Prinzip der kontinuierlichen Selbstkontrolle**
  Die Fehlerquellen werden identifiziert, Folgen minimiert und nachhaltig abgestellt.
- **Prinzip der ganzheitlichen Vorgehensweise**
  Alle wesentlichen Anforderungen werden von Beginn eines jeden Vorgangs an berücksichtigt.

2.1.4 Sicherheit der Informationssysteme während des Lebenszyklus

Die Sicherheit eines Informationssystems muss ab Beginn des Lebenszyklus ein fester Bestandteil bei der Planung, der Spezifikation, der Beschaffung, der Entwicklung, der Einführung, dem Betrieb, der Wartung und der geordneten Außerbetriebnahme sein. Das Informationssystem muss den geltenden Sicherheitsstandards (Sicherheitsrichtlinien) entsprechen.

2.2 Sicherheitsstrategie

Um die angestrebten Sicherheitsziele zu erreichen, wird bei der Securitas ein Informationssicherheitsmanagementsystem (kurz: ISMS) betrieben, welches sich an den Vorgaben der DIN ISO/IEC 27001/2[5] orientiert.

2.3 Organisationsstruktur

Um die Ziele im Bereich Informationssicherheit zu erreichen, wurde ein Informationssicherheits-beauftragter (ISB) ernannt und eine Informationssicherheitsorganisation[6] etabliert.

[4] Mitarbeiter, Kunden und Lieferanten

[5] Siehe Referenzdokumente #1 und #2.

[6] Siehe Referenzdokument #4.

2.4 Informationssicherheitsprozess

Der Informationssicherheitsprozess orientiert sich am PDCA-Modell (Plan-Do-Check-Act bzw. Planung-Umsetzung-Erfolgskontrolle-Optimierung) der ISO / IEC 27001.

Die einzelnen Phasen beschreiben einen Zyklus der wiederkehrenden Arbeiten, die im Rahmen des Informationssicherheitsmanagements durchzuführen sind. Dies sind im Einzelnen:

- **Plan-Phase** (Planung und Konzeption)
  Hierzu gehören die Planung des Vorgehens des Informationssicherheitsmanagementsystems (Planung ISMT, Entwicklung Leitlinie etc.) sowie die Erstellung eines Sicherheitskonzeptes.
- **Do-Phase** (Umsetzung der Planung)
  In der Do-Phase werden das ISMT etabliert und die im Rahmen des Sicherheitskonzeptes geplanten Vorgehen und Maßnahmen umgesetzt.
- **Check-Phase** (Erfolgskontrolle, Überwachung der Zielerreichung)
  Diese Phase beinhaltet die internen Prüfungen, die sicherstellen sollen, dass die angestrebten Sicherheitsziele erreicht werden.
- **Act-Phase** (Optimierung, Verbesserung)
  Zur Act-Phase gehören Tätigkeiten, die (meist basierend auf den Ergebnissen der internen Prüfungen der Check-Phase) Abweichungen behandeln, indem Prozesse oder Maßnahmen so angepasst bzw. verbessert werden, dass das anvisierte Sicherheitsniveau besser erreicht werden kann.

3 Mitgeltende Unterlagen

„nicht belegt“

4 Zeichnungsebene

erstellt:	geprüft:	freigegeben:
Antonio Valls Ruiz (Aug 4, 2023 12:38 GMT+2)	Werner Vettorel (Aug 4, 2023 13:45 GMT+2)	Andreas Ritsch (Aug 4, 2023 14:03 GMT+2)
ppa. Antonio Valls Ruiz	ppa. Werner Vettorel	ppa. Andreas Ritsch
ISB	IT Manager	Country General Counsel

Datum 04.08.2023
Securitas Holding GmbH

Informationssicherheitsleitlinie.r4

Final Audit Report 2023-08-04

Created:	2023-08-04
By:	Antonio Valls Ruiz (vallsruiz.antonio@securitas.de)
Status:	Signed
Transaction ID:	CBJCHBCAABAAKW0iJZV8yqbZ3SA6ivHAv2D7mKjuwCeh

"Informationssicherheitsleitlinie.r4" History

Document created by Antonio Valls Ruiz (vallsruiz.antonio@securitas.de)
2023-08-04 - 10:37:04 AM GMT

Document e-signed by Antonio Valls Ruiz (vallsruiz.antonio@securitas.de)
Signature Date: 2023-08-04 - 10:38:12 AM GMT - Time Source: server

Document emailed to vettorel.werner@securitas.de for signature
2023-08-04 - 10:38:13 AM GMT

Email viewed by vettorel.werner@securitas.de
2023-08-04 - 11:45:22 AM GMT

Signer vettorel.werner@securitas.de entered name at signing as Werner Vettorel
2023-08-04 - 11:45:37 AM GMT

Document e-signed by Werner Vettorel (vettorel.werner@securitas.de)
Signature Date: 2023-08-04 - 11:45:39 AM GMT - Time Source: server

Document emailed to Andreas Ritsch (ritsch.andreas@securitas.de) for signature
2023-08-04 - 11:45:40 AM GMT

Email viewed by Andreas Ritsch (ritsch.andreas@securitas.de)
2023-08-04 - 12:03:17 PM GMT

Document e-signed by Andreas Ritsch (ritsch.andreas@securitas.de)
Signature Date: 2023-08-04 - 12:03:27 PM GMT - Time Source: server

Agreement completed.
2023-08-04 - 12:03:27 PM GMT