



Informationssicherheitsleitlinie

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

Datum:
31.03.2026

Revision:
7

Autor: Antonio Valls Ruiz

Dokumentinhaber: ISB

Dokumentenategorie: strategisch

Klassifizierung: öffentlich

Autor(en):
Antonio Valls Ruiz

Prüfer:
IDMT

Freigeber:
Andreas Ritsch



Dokumenthistorie

Revision	Datum	Bearbeiter	Beschreibung	Status ¹
0.9	15.10.2018	Antonio Valls Ruiz	Finale Fassung zur Unterschrift	vorgelegt
1	01.01.2019	Manfred Buhl	Freigabe	freigegeben
1.1	11.12.2020	ISMT	Anpassung der Leitlinie um Schulung und Sensibilisierung	vorgelegt
2	15.12.2020	Herwarth Brune	Freigabe	freigegeben
2.1	13.05.2022	Antonio Valls Ruiz	Anpassung um Datenschutz und neue CI	vorgelegt
2.2	17.05.2022	Maximilian Merken	QM-Prüfung	vorgelegt
3	20.05.2022	Ralf Brümmer	Freigabe	freigegeben
3.1	19.07.2023	Antonio Valls Ruiz	Anpassung an neue RL 0001	vorgelegt
3.2	24.07.2023	Maximilian Merken	QM-Prüfung	vorgelegt
3.3	04.08.2023	ISMT	Redaktionelle Änderungen	vorgelegt
3.4	04.08.2023	Maximilian Merken	QM-Prüfung	vorgelegt
4	04.08.2023	Antonio Valls Ruiz	Freigabe-Workflow	freigegeben
4.1	09.08.2023	ISMT	Keine Änderungen	vorgelegt
4.2	09.04.2024	Maximilian Merken	QM-Prüfung	vorgelegt
5	09.04.2024	Antonio Valls Ruiz	Freigabe-Workflow	freigegeben
5.1	06.03.2025	Antonio Valls Ruiz	Anpassungen an die neue Vorlage	vorgelegt
5.2	17.03.2025	Maximilian Merken	QM-Prüfung	vorgelegt
6	24.03.2025	Antonio Valls Ruiz	Freigabe-Workflow	freigegeben
6.1	13.03.2026	IDMT	Keine Änderungen	vorgelegt
6.2	31.03.2026	Maximilian Merken	QM-Prüfung	vorgelegt
7	31.03.2026	Antonio Valls Ruiz	Freigabe-Workflow	freigegeben

Referenzdokumente

Nr.	Dokumentname	Stand ²
1	DIN ISO 27001	In der aktuellen Version
2	DIN ISO 27002	In der aktuellen Version
3	DIN ISO 27701	In der aktuellen Version
4	Informationssicherheits- und Datenschutzorganisation	In der aktuellen Revision
5	Group Enterprise Risk Management	In der aktuellen Revision

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.



Inhaltsverzeichnis

1	Zusammenfassung der Änderungen	3
1.1	Begriffe	3
2	Informationssicherheitsleitlinie	4
2.1	Sicherheitsziele.....	4
2.1.1	Grundwerte der Informationssicherheit.....	4
2.1.2	Angestrebtes Sicherheitsniveau.....	4
2.1.3	Die Sicherheitsprinzipien der Securitas	5
2.1.4	Sicherheit der Informationssysteme während des Lebenszyklus	5
2.2	Sicherheitsstrategie.....	5
2.3	Organisationsstruktur	5
2.4	Informationssicherheitsprozess	6
2.5	Verstöße.....	6
2.6	Konsequenzen	6
3	Mitgeltende Unterlagen.....	7
4	Zeichnungsebene	7



1 Zusammenfassung der Änderungen

Änderungen seit der letzten Revision sind lediglich redaktionell.

1.1 Begriffe

Nicht belegt

Öffentlich



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, Kunden, Lieferanten und Behörden 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-DSGVO) 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 Ausmaße³ 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“ Bildschirms**
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 Stakeholdern⁴. 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 (Projektierung), 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 27001/2⁵ orientiert.

2.3 Organisationsstruktur

Um die Ziele im Bereich Informationssicherheit zu erreichen, wurde ein Informationssicherheitsbeauftragter (ISB) ernannt und eine Informationssicherheits- und Datenschutzorganisation⁶ etabliert.

⁴ Mitarbeiter, Behörden, 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 IDMT, Entwicklung Leitlinie etc.) sowie die Erstellung eines Sicherheitskonzeptes.
- **Do-Phase** (Umsetzung der Planung)
In der Do-Phase werden das IDMT etabliert und die im Rahmen des Sicherheitskonzeptes geplanten Vorgehen und Maßnahmen umgesetzt.
- **Check-Phase** (Erfolgskontrolle, Überwachung der Zielerreichung)
Diese Phase beinhaltet die internen sowie externen 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 sowie externen Prüfungen der Check-Phase) Abweichungen behandeln, indem Prozesse oder Maßnahmen so angepasst bzw. verbessert werden, dass das anvisierte Sicherheitsniveau besser erreicht werden kann.

2.5 Verstöße

Als Verstöße gelten schuldhaftes Handeln, 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.

2.6 Konsequenzen

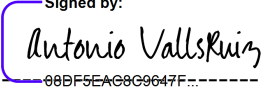
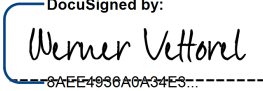
Die Nichteinhaltung der Leitlinie für die Informationssicherheit oder der daraus abgeleiteten Sicherheitsrichtlinien kann zu arbeitsrechtlichen Konsequenzen und straf- / zivilrechtlichen Verfahren führen.



3 Mitgeltende Unterlagen

„nicht belegt“

4 Zeichnungsebene

erstellt:	geprüft:	freigegeben:
<div><div>Signed by:</div><div></div><div>08DF5EAC8C9647F...</div></div> <p>ppa. Antonio Valls Ruiz ISB</p>	<div><div>DocuSigned by:</div><div></div><div>8AEE4936A0A34E3...</div></div> <p>ppa. Werner Vettorel IS / IT Cluster Director Europe Central</p>	<div><div>DocuSigned by:</div><div></div><div>9680857E0BED4AB...</div></div> <p>ppa. Andreas Ritsch Country General Counsel</p>
<p>Datum 31.03.2026 Securitas Holding GmbH</p>		