

Informationssicherheitsleitlinie

Version	3.2
Gültig ab	24.09.2025
Gültig für	Mitarbeitende der SoCura Gesellschaften, Geschäftspartner (zur Kenntnis)
Autor / verantwortlich	Igor Wink
Freigabe Geschäftsführung	24.09.2025
Nächste Revision	31.07.2026
Vertraulichkeitsstufe	Öffentlich
Änderungshistorie	
3.2	24.09.2025 Änderungen in Formulierungen, Fehlerkorrekturen
3.1	14.06.2024 Update Rollen Sicherheitsbeauftragte, 10.09.2024 Aufnahme Klimawandel, Korrektur Normbezug
3.0	16.06.2023 Update TK Provider, Rolle IT-Sec-Experte
2.4	19.08.2022 Update PCI DSS und Verhaltensregeln
2.3	01.10.2021 Nur Update Kopf- und Fußzeilen
2.2	28.09.2020 Neue Rolle, Cloud Security, Normbezug
2.1	10.10.2019 Neue Freigabe Geschäftsführung
2.0	13.09.2018 Neue Rollen, gesetzliche Grundlagen
1.0	18.08.2015 durch die Geschäftsführung freigegeben

Präambel

Die SoCura ist ein hoch spezialisiertes, modernes Unternehmen, das sich bei allen Aktivitäten auf ihre Kernkundengruppe, das Gesundheitswesen und Non-Profit-Organisationen im Bereich Kirche und Wohlfahrt, konzentriert. Die SoCura erbringt als IT-Dienstleister für ihre Kunden¹ auf Basis einer hybriden Cloud-Architektur maßgeschneiderte IT-Services, die sich durch ein attraktives Preis-Leistungs-Verhältnis sowie eine kontinuierlich hohe Servicequalität auszeichnen.

Die Funktionsfähigkeit und Verfügbarkeit der IT-Systeme und Netze sowie die Vertraulichkeit und Integrität der Geschäftsprozesse, Organisationsverfahren und der zugehörigen IT-Services, IT-Anwendungen und Daten sind durch technische Fehler, Fehlverhalten, Sabotage und Ausspähungen gefährdet. Dies kann zu Imageverlust, wirtschaftlichem Schaden und im Extremfall zur Gefährdung von Menschen führen. Um solchen Gefährdungen wirkungsvoll zu begegnen, müssen geeignete technische und organisatorische Maßnahmen geplant, umgesetzt und kontinuierlich verbessert werden. Hierbei sind auch Gefährdungen durch Auswirkungen des Klimawandels zu berücksichtigen.

Zur Einhaltung gesetzlicher Vorgaben, zur Wahrung des Vertrauens der Kunden und aus Eigeninteresse kommt daher der Wahrung der Informationssicherheit bei den SoCura-Gesellschaften ein hoher Stellenwert zu.

Um ein adäquates Informationssicherheitsniveau zu erreichen und einzuhalten, wird ein Informationssicherheitsmanagementsystem (ISMS) gemäß der Norm ISO/IEC 27001:2022 betrieben, dass die Vertraulichkeit, Verfügbarkeit und Integrität von Informationen und Informationstechnik gewährleistet, die Belastbarkeit der Systeme und Dienste sicherstellt und die Anforderungen des Datenschutzes erfüllt.

¹Hinweis: Mit allen Rollen- und Funktionsbezeichnungen sind jeweils gleichermaßen weibliche und männliche Rollen- bzw. Funktionsinhaber gemeint.

Falls Kreditkartendaten verarbeitet, gespeichert und / oder übermittelt werden, ist zur Erreichung und Einhaltung eines angemessenen Informationssicherheitsniveaus der Payment Card Industry Data Security Standard (PCI DSS) einzuhalten.

Für ihre Mobilfunkkunden fungiert die SoCura als Telekommunikationsanbieter und hält die entsprechenden gesetzlichen Bestimmungen aus dem Telekommunikationsgesetz (TKG) ein.

Geltungsbereich und Verwendung

Diese Informationssicherheitsleitlinie gilt für das gesamte Unternehmen und ist von allen Mitarbeitenden einzuhalten. Sie ist darüber hinaus gegenüber Kunden und Lieferanten anzuwenden.

Dieses Dokument ist neuen Mitarbeitenden und Geschäftspartnern auszuhändigen bzw. in geeigneter Weise bekannt zu machen.

Definitionen

Informationssicherheit liegt vor, wenn die Risiken für die Sicherheitsziele Vertraulichkeit, Integrität und Verfügbarkeit von Informationen und Informationstechnik durch angemessene Maßnahmen auf ein akzeptierbares Maß reduziert sind. Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten und Informationen.

Dabei bedeuten:

- **Vertraulichkeit:** Vertrauliche Daten, Informationen und Programme sind vor unberechtigten Zugriffen und unbefugter Preisgabe zu schützen. Dazu gehören die gespeicherten oder transportierten Nachrichteninhalte, die näheren Informationen über den Kommunikationsvorgang (wer, wann, wie lange, mit wem usw.) sowie die Daten über den Sende- und Empfangsvorgang.
- **Integrität:** Integrität der Informationen bedeutet deren Vollständigkeit und Korrektheit. Zum anderen bezieht sich der Begriff Integrität auch auf IT-Systeme, da die Integrität der Informationen und Daten nur bei ordnungsgemäßer Verarbeitung und Übertragung sichergestellt werden kann.
- **Verfügbarkeit:** Die Funktionen der Hard- und Software im System- und Netzbereich sowie notwendige Informationen stehen dem Anwender zum richtigen Zeitpunkt am richtigen Ort zur Verfügung.

Zielsetzung

Die SoCura strebt folgende Schutzziele an:

- Die Verfügbarkeit der IT-Services, IT-Systeme, Applikationen und Daten muss gewährleistet sein.
- Die Integrität der IT-Systeme, Programme und Daten ist zu schützen.
- Der Missbrauch der IT-Services, IT-Systeme, Applikationen und Daten durch zweckwidrige Nutzung oder Nutzung durch Unbefugte ist zu verhindern.
- Vertrauliche Informationen sind unabhängig von der Art ihrer Aufzeichnung so zu handhaben, dass ihre Vertraulichkeit jederzeit sichergestellt ist.
- Insbesondere sind Informationswerte, die in einer Cloud-Umgebung bereitgestellt oder genutzt werden, zu schützen.
- Alle einschlägigen Gesetze und sonstigen rechtlichen Bestimmungen sind einzuhalten.
- Die Persönlichkeitsrechte von Kunden, Anwendern, Mitarbeitenden und Lieferanten, sowie deren Angehörigen, Mitgliedern, Patienten und sonstigen Vertragspartnern sind jederzeit zu wahren.
- IT-bezogene Geschäftsprozesse sind weitgehend widerstandsfähig gegen innere und äußere Störungen zu machen.

Eine besondere Bedeutung kommen dabei im Gesundheitswesen der Verfügbarkeit und Integrität zu, weil ein Ausfall der IT-Systeme oder eine Verfälschung der Daten im Extremfall zur Gefährdung von Leib und Leben führen kann. Darüber hinaus spielt der Schutz personenbezogener Daten im Bereich Wohlfahrt, Kirche und Gesundheitswesen eine wichtige Rolle, weil die Offenbarung von Gesundheits- oder Sozialdaten gegenüber Unbefugten für die Betroffenen existenzgefährdend sein kann und für die Verantwortlichen möglicherweise hohe Strafen oder einen Imageverlust nach sich zieht.

Rollen und Verantwortlichkeiten

Geschäftsführung

Die Geschäftsführung ist verantwortlich für

- die Erstellung, Verabschiedung und Aktualisierung dieser Informationssicherheitsleitlinie,
- die Bereitstellung der personellen, organisatorischen und finanziellen Mittel zur Gewährleistung der Informationssicherheit,
- die Bewertung des erreichten Standes der Informationssicherheit bezüglich Wirksamkeit und Angemessenheit.

IT-Security Management Board

Das IT-Security Management Board überprüft regelmäßig die Ziele der Informationssicherheit, bewertet die relevanten IT-Risiken für die Geschäftsprozesse und die getroffenen Schutzmaßnahmen. Es überprüft anhand der Berichte des IT-Security Managers den Stand der Informationssicherheit, legt ggf. Korrekturmaßnahmen fest und informiert die Geschäftsführung.

Computer Security Incident Response Team (CSIRT)

Das Computernotfallteam CSIRT entdeckt und bearbeitet IT-Sicherheitsvorfälle. Es überprüft dazu Daten und Systeme, befragt Mitarbeitende, Kunden und Lieferanten. Es weist auf Sicherheitsverstöße hin und leitet diese entsprechend der festgelegten Berichtswege weiter. Darüber hinaus erkennt und bearbeitet das CSIRT IT-Sicherheitsschwachstellen und schlägt geeignete Präventionsmaßnahmen vor.

IT-Security Manager

Der IT-Security Manager ist für den Betrieb des Informationssicherheitsmanagementsystems (ISMS) verantwortlich und berichtet darüber dem IT-Security Management Board und der Geschäftsführung. Im Falle einer Nichtbesetzung der Stelle, werden die Aufgaben vom Senior Experten IT-Security / Sicherheitsbeauftragten TK wahrgenommen.

Informationssicherheitsbeauftragter Operative IT

Der Informationssicherheitsbeauftragte Operative IT unterstützt beim Betrieb des ISMS insgesamt, insbesondere verantwortet er folgende Aufgaben:

- Planung, Überwachung und Begleitung der Umsetzung von Informationssicherheitsmaßnahmen für die einzelnen Geschäftsbereiche innerhalb der SoCura-Gesellschaften,
- Identifizierung, Bewertung und Unterstützung bei der Behebung von Sicherheitsvorfällen und Schwachstellen,
- Einführung und Betrieb von Systemen zur Angriffserkennung (wie z.B. Security Incident and Event Management (SIEM)) und der dazugehörigen Prozesse (wie z.B. Security Operations Center (SOC)),
- Leitung des Computer Security Incident Response Team (CSIRT),
- Übernahme von Koordinations-, Kontroll- und Fachaufgaben,
- Zusammenarbeit mit den relevanten Fachbereichen.

IT-Security Experte

Der IT-Security Experte unterstützt den IT-Security Manager und den Informationssicherheitsbeauftragten Operative IT beim Betrieb des ISMS. Zu den gemeinsamen Aufgaben zählen:

- die Koordinierung des IT-Risikomanagements,
- die Erarbeitung von IT-Sicherheitsrichtlinien und -konzepten,
- die Planung und Überprüfung von IT-Sicherheitsmaßnahmen und -prozessen,
- die Beratung von Führungskräften und Geschäftsführung zu Informationssicherheitsfragen,
- die Sensibilisierung der Mitarbeitenden hinsichtlich der Informationssicherheit.

IT-Abteilungen

Die IT-Abteilungen der SoCura-Gesellschaften sind verantwortlich für die Konzeption, Implementierung und den Betrieb der IT-Security-Maßnahmen.

Führungskräfte

Führungskräfte haben eine Vorbildfunktion und dadurch maßgeblichen Einfluss auf die Sensibilität ihrer Mitarbeitenden für die Informationssicherheit. Sie sind für die Umsetzung der IT-Sicherheitsziele in ihrem Bereich sowie die regelmäßige Schulung ihrer Mitarbeitenden verantwortlich.

IT-Mitarbeitende und Anwendende

Alle Mitarbeitenden sind in ihrem jeweiligen Verantwortungsbereich für den Schutz der ihnen anvertrauten Informationen, Daten, IT-Services und -Systeme verantwortlich.

Geschäftspartner

Geschäftspartner werden gebeten, an der Bewertung von Risiken für die genutzten oder gelieferten Systeme und Dienste sowie an der Planung, Umsetzung und Überprüfung von risikomindernden Maßnahmen mitzuwirken, um gemeinsam ein angemessen hohes IT-Sicherheitsniveau zu erreichen. Dazu zählt insbesondere

- die Sensibilisierung der Mitarbeitenden für IT-Sicherheit und Datenschutz,
- die Unterstützung bei der Bearbeitung von IT-Sicherheitsvorfällen und Datenschutzereignissen,
- die Mitwirkung bei Audits und Überprüfungen.

Weitere Rollen

Datenschutzkoordinator

Der Datenschutzkoordinator plant und steuert das Datenschutz-Managementsystem, das in der Leitlinie zum Datenschutz-Management festgelegt ist.

Datenschutzbeauftragter (DSB)

Der Datenschutzbeauftragte unterrichtet und berät die Geschäftsführung und die Mitarbeitenden hinsichtlich der geltenden Datenschutzvorschriften, z.B. Datenschutzgrundverordnung (DS-GVO), Bundesdatenschutzgesetz (BDSG), Kirchliche Datenschutzregelung der Ordensgemeinschaft päpstlichen Rechts (KDR-OG) und weiterer anwendbarer Vorschriften zum Schutz personenbezogener Daten, und überwacht deren Einhaltung.

IT-Notfallmanager

Der IT-Notfallmanager plant präventive Maßnahmen zur Vorbeugung vor bzw. reaktive Maßnahmen zur Bewältigung von Notfällen und Krisen. Er steuert den IT-Notfallmanagementprozess, dessen Aufbau in der Verfahrensanweisung IT-Notfallmanagement festgelegt ist.

Sicherheitsbeauftragter gem. § 166 Abs. 1 Nr. 1 TKG

Die Aufgaben des Beauftragten umfassen insbesondere:

- Koordinations-, Kontroll- und Fachaufgaben gem. TKG,
- Unterrichtung und Beratung der Organisation zum TKG,
- Mitwirken an der Erstellung des Sicherheitskonzepts,

- Beratung und Unterstützung bei der Umsetzung und Aktualisierung des Sicherheitskonzepts,
- Schnittstelle und direkter Ansprechpartner zur Geschäftsleitung,
- Zusammenarbeit mit der Bundesnetzagentur.

Umsetzung

- Um möglichen Schäden vorzubeugen, sind geeignete technische- und organisatorische Maßnahmen (TOM) zur Informationssicherheit auf Grundlage einer Risikobewertung umzusetzen.
- Die Verantwortlichen haben bei Verstößen und Beeinträchtigungen die zur Aufrechterhaltung des IT-Betriebes und der Informationssicherheit geeigneten und angemessenen Maßnahmen zu ergreifen.
- Der Zugriff auf IT-Systeme, -Anwendungen, Daten und Informationen ist auf den unbedingt erforderlichen Personenkreis zu beschränken. Jeder Mitarbeitende erhält nur auf diejenigen Daten und Informationen die Zugriffsberechtigungen, die zur Erfüllung der dienstlichen Aufgaben erforderlich sind (Need-to-know- bzw. Need-to-use-Prinzip).
- Sofern Verfahren und Tools eingesetzt werden, sind sie nach dem jeweiligen Stand der Technik auszuwählen und einzusetzen.
- Die für die Umsetzung der Informationssicherheitsmaßnahmen erforderlichen Ressourcen und Investitionsmittel sind bereitzustellen.
- Die Wirksamkeit der Sicherheitsmaßnahmen ist regelmäßig zu kontrollieren, zu dokumentieren und weiterzuentwickeln.
- Das Informationssicherheitsmanagement ist an der Norm ISO/IEC 27001:2022 auszurichten.

Überwachung und Sanktionen

Die Einhaltung dieser Leitlinie und daraus abgeleiteter Informationssicherheitsrichtlinien wird regelmäßig überprüft. Verstöße werden dokumentiert und können für den Verursacher schwerwiegende Folgen nach sich ziehen. Auch arbeitsrechtliche, zivilrechtliche, wie z.B. Schadenersatzansprüche und strafrechtliche Konsequenzen sind nicht auszuschließen. Als mitgeltende Unterlage gilt die Verhaltensrichtlinie der Malteser.

Inkraftsetzung

Diese Leitlinie tritt am Tag nach der Veröffentlichung in Kraft und wird regelmäßig auf Aktualität überprüft.

Köln, 24.09.2025

Köln, 24.09.2025

Für die SoCura gGmbH

Thomas Berding-Pniok
Geschäftsführer

Jens Francksen
Prokurist

Für die SoCura MD gGmbH

Thomas Berding-Pniok
Geschäftsführer

Jens Francksen
Prokurist

Für die SoCura Systems gGmbH

Thomas Berding-Pniok
Geschäftsführer

Jens Francksen
Prokurist