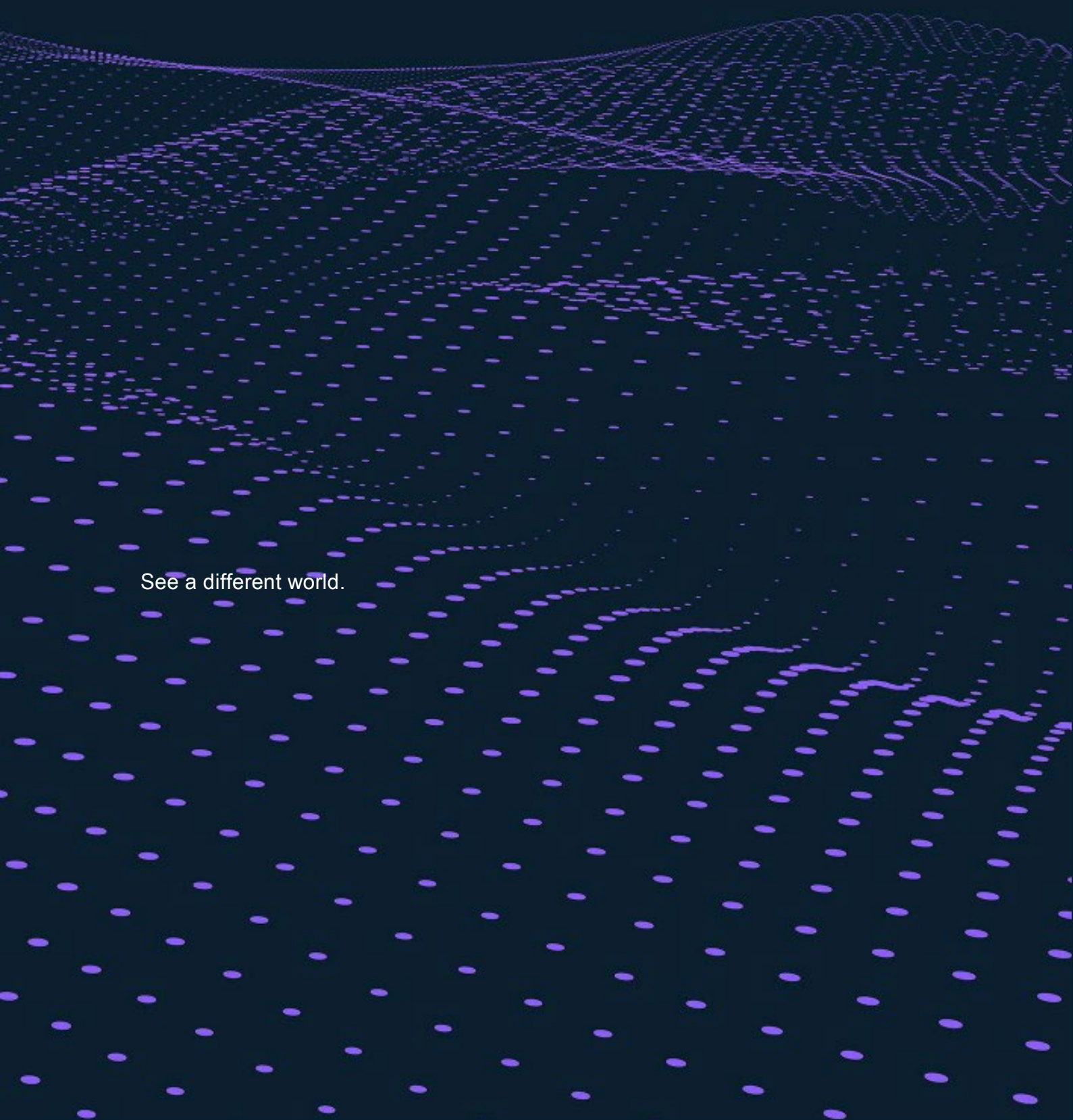
Securitas

IT-Sicherheitsanforderungen

Für Kunden, Lieferanten und Geschäftspartner

Securitas Österreich



1 Inhalt

Version	Datum	Autor	Beschreibung
1.0	30.01.2025	Wolfgang Maierhofer	Veröffentlicht

2 Allgemeine Informationen

Dieses Dokument listet die Anforderungen an IT-Systeme von Lieferanten und oder Geschäftspartnern der Securitas Sicherheitsdienstleistungen GmbH.

3 Geltungsbereich

IT-Systeme und oder digitale Dienste von Lieferanten oder Geschäftspartnern, die über eine oder mehrere digitale Schnittstellen mit der Securitas Sicherheitsdienstleistungen GmbH IT-Infrastruktur dauerhaft oder zeitlich begrenzt verbunden sind.

DEFINITIONEN:

"SECURITAS-Daten" bezeichnet alle Daten oder Aufzeichnungen jeglicher Art und in welcher Form auch immer, die sich auf das Geschäft der Securitas-Gruppe, ihre Tätigkeiten, Einrichtungen, Vermögenswerte, Mitarbeiter, Kunden, bei denen Securitas eine Lieferantenlösung implementiert hat, oder anderweitig auf das Geschäft von Securitas oder eines Mitglieds der Securitas-Gruppe beziehen, unabhängig davon, ob diese Daten vor Beginn des Vertrags bestanden oder im Rahmen von oder im Zusammenhang mit den Dienstleistungen, die der Anbieter erbracht hat, einschließlich vertraulicher Informationen und personenbezogener Daten von Securitas;

"Personenbezogene Daten von Securitas": bezeichnet alle personenbezogenen Daten, die vom Lieferanten oder einem Unterauftragsverarbeiter im Auftrag oder einer mit Securitas verbundenen Gesellschaft oder im Namen eines Kunden von Securitas oder einer mit Securitas verbundenen Gesellschaft gemäß oder in Verbindung mit der Vereinbarung verarbeitet werden;

"Resilienz" bezeichnet die Fähigkeit, sich auf veränderte Bedingungen vorzubereiten und sich an diese anzupassen sowie Risiken zu widerstehen und sich schnell von ihnen zu erholen. Resilienz umfasst die Fähigkeit, vorsätzlichen Angriffen, Unfällen oder natürlich auftretenden Bedrohungen oder Vorfällen, die die Sicherheit beeinträchtigen oder beeinträchtigen können, standzuhalten und sich davon zu erholen.
"Datensätze": alle Datensätze, die von Securitas oder durch die Erbringung von Dienstleistungen für Securitas an Lieferanten zur Verfügung gestellt werden und bei der Entwicklung des KI-Systems verwendet werden
Vernünftigerweise vorhersehbarer Missbrauch: die Nutzung des KI-Systems in einer Weise, die nicht seiner Zweckbestimmung entspricht, die sich aber aus vernünftigerweise vorhersehbarem menschlichem Verhalten oder der Interaktion mit anderen Systemen ergeben kann;
Wesentliche Änderung: eine Änderung des KI-Systems nach der Lieferung, die sich auf die Konformität des KI-Systems mit den in diesen Klauseln festgelegten Anforderungen auswirkt oder zu einer Änderung des beabsichtigten Zwecks führt

"Risiko" bezeichnet jeden vernünftigerweise identifizierbaren Umstand oder jedes Ereignis, das eine potenzielle nachteilige Auswirkung hat.

"Sicherheitsereignis" bezeichnet eine Änderung, die Auswirkungen auf den Betrieb (einschließlich Mission, Fähigkeiten oder Reputation) und/oder die Sicherheit von Systemen oder Securitas-Daten haben kann, die sich auf die Vertraulichkeit, Integrität oder Verfügbarkeit der Daten auswirkt.

"Sicherheitsvorfall" bezeichnet jedes Ereignis, das sich tatsächlich nachteilig auf die Sicherheit auswirkt.

"Sicherheit" bezeichnet den Zustand, in dem die Integrität, Vertraulichkeit und Zugänglichkeit von Informationen, Diensten oder Netzwerkeinheiten gewährleistet ist.

"Systeme" bezeichnet die Computerumgebung, die Kommunikationsumgebung und/oder die Informations- und Aufzeichnungsumgebung (bestehend aus, aber nicht beschränkt auf Hardware, Software, Netzwerk- und Informationssysteme, Papier- und/oder andere physische Aufzeichnungen), Daten oder Räumlichkeiten, die vom Lieferanten oder (je nach Kontext) Securitas im Zusammenhang mit der Erbringung von

Dienstleistungen oder der Wartung der von Securitas implementierten Lösung verwendet werden können

"Gute Branchenpraxis" bezeichnet Maßnahmen, die nach dem Konsens der Fachmeinung über die Sicherheit und die Sicherheitsrisiken, die von Zeit zu Zeit gelten können, als angemessen erachtet werden.

1 SICHERHEITSANFORDERUNGEN

Der Lieferant muss die folgenden technischen und organisatorischen Sicherheitsmaßnahmen einhalten, die in seinen Informationssicherheitsrichtlinien näher erläutert werden.

1.1 Der Lieferant bestätigt, dass er zum Zeitpunkt des Vertragsabschlusses über die technischen und organisatorischen Maßnahmen verfügt und verfügen wird, die erforderlich sind, um die Risiken für die Sicherheit von Securitas-Daten zu bewältigen, einschließlich solcher Maßnahmen, die nach dem Konsens der professionellen Sicherheitsmeinung unter Berücksichtigung des Stands der Technik als angemessen erachtet werden.

1.2 Der Lieferant ergreift geeignete und verhältnismäßige Maßnahmen, um die Auswirkungen von Sicherheitsvorfällen, die sich auf die Bereitstellung der Dienstleistungen und/oder der Lösung auswirken, zu verhindern und zu minimieren, um den Schutz der Securitas-Daten zu gewährleisten.

1.3 Ungeachtet der vorstehenden Absätze 1.1 und 1.2 muss der Lieferant (auf eigene Kosten):

- Technische und organisatorische Maßnahmen zum Management der Risiken für Securitas-Daten zu ergreifen, die ihr von Securitas von Zeit zu Zeit schriftlich und in Übereinstimmung mit der Guten Branchenpraxis mitgeteilt werden;
- Der Lieferant überprüft jährlich (oder sofern zwischen den Parteien nichts anderes vereinbart wurde) den Grad der Einhaltung und Wirksamkeit der von ihm ergriffenen technischen und organisatorischen Maßnahmen und führt Aktualisierungen, Verbesserungen oder Sanierungsarbeiten durch, die vernünftigerweise erforderlich sind, um die Vereinbarung zu erfüllen, vorausgesetzt, dass er keine Änderungen vornimmt, die dazu führen könnten, dass ein geringeres Schutzniveau für ein betroffenes System im Zusammenhang mit der Bereitstellung gewährt wird von Dienstleistungen; und
- Die 18 CIS Critical Security Controls oder ISO 27001 (oder einen ähnlichen branchenweit gleichwertigen Standard mit vorheriger Zustimmung von Securitas) in der jeweils aktualisierten Fassung einzuhalten und einzuhalten.

1.4 Der Lieferant muss technische und organisatorische Maßnahmen gemäß den Absätzen 1.1, 1.2 und 1.3 ergreifen, die unter anderem die Möglichkeit umfassen:

- Identifizierung von Sicherheitsrisiken
- Die Systeme des Lieferanten und die Daten von Securitas zu schützen
- Erkennen des Auftretens eines Sicherheitsereignisses
- Auf einen Sicherheitsvorfall zu reagieren
- Wiederherstellung nach einem Sicherheitsvorfall

2 Identifizierung von Sicherheitsrisiken

2.1 Der Lieferant stellt sicher:

- Er verfügt über ein angemessenes Verständnis seiner Organisation, um Sicherheitsrisiken zu managen, einschließlich, aber nicht beschränkt auf Risiken für die Systeme des Lieferanten, die Securitas-Daten, die Personen, die Vermögenswerte und die Dienstleistungen.
- Bedrohungen für die Sicherheit der Systeme des Lieferanten und der Securitas-Daten, sowohl intern als auch extern, werden identifiziert und dokumentiert.

- Risiken, die durch Systemschwachstellen verursacht werden, werden identifiziert, dokumentiert und behoben.
- Gewonnene Erkenntnisse und prädiktive Indikatoren werden verwendet, um das Bewusstsein für Sicherheitsrisiken zu schärfen.
- Es gibt einen Prozess der kontinuierlichen Verbesserung, einschließlich, aber nicht beschränkt auf die Integration fortschrittlicher Sicherheitstechnologien und -praktiken, um auf Sicherheitsrisiken zu reagieren.
- Es passt sich aktiv an eine sich verändernde Bedrohungs- und Technologielandschaft an und reagiert zeitnah und effektiv auf sich entwickelnde und ausgeklügelte Bedrohungen.
- Es gibt einen unternehmensweiten Ansatz für das Management von Sicherheitsrisiken, der risikoinformierte Richtlinien, Prozesse und Verfahren verwendet, um potenzielle Sicherheitsereignisse zu bewältigen.
- Die Beziehung zwischen Sicherheitsrisiken und der Erbringung der Dienstleistungen wird klar verstanden und bei Entscheidungen berücksichtigt, die sich auf die Sicherheit der Systeme und Securitas-Daten des Anbieters auswirken können.
- Das Risikomanagement ist Teil der Unternehmenskultur und entwickelt sich aus dem Bewusstsein für frühere Aktivitäten und dem kontinuierlichen Bewusstsein für Aktivitäten in den Systemen des Lieferanten.
- Es empfängt, generiert und prüft priorisierte Informationen, die in die kontinuierliche Analyse von Sicherheitsrisiken einfließen, wenn sich die Bedrohungs- und Technologielandschaften weiterentwickeln, einschließlich der Erfassung und Nutzung von Cyber- und Informationssicherheitsbedrohungsinformationen aus Foren zum Informationsaustausch und anderen Quellen.
- Das Unternehmen nutzt Echtzeitinformationen, um Risiken in der Informationssicherheit in der Lieferkette zu verstehen und konsequent darauf zu reagieren, die mit den von ihm angebotenen und verwendeten Produkten und Dienstleistungen verbunden sind.
- Dass die Securitas-Daten, das Personal und alle Systeme, die es dem Lieferanten ermöglichen, die Dienstleistungen zu erbringen, entsprechend ihrer relativen Bedeutung für die Sicherheit der Systeme und der Securitas-Daten identifiziert und verwaltet werden. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Physische Geräte und die Lieferantensysteme innerhalb der Organisation werden inventarisiert;
  - Softwareplattformen und Anwendungen innerhalb der Organisation werden inventarisiert;
  - Organisatorische Kommunikation und Datenflüsse werden abgebildet;
  - Externe Informationssysteme des Lieferanten sind katalogisiert;
  - Ressourcen (z. B. Hardware, Geräte, Daten, Zeit, Personal und Software) werden auf der Grundlage ihrer Klassifizierung und Kritikalität für die Dienste und den Schutz der Systeme des Lieferanten, der Securitas-Systeme (in dem in den Diensten angegebenen Umfang) und der Securitas-S-Daten priorisiert;
  - Cyber- und Informationssicherheitsrollen und -verantwortlichkeiten für die gesamte Belegschaft und externe Stakeholder (z. B. Lieferanten, Kunden, Partner) werden festgelegt;
  - Abhängigkeiten und kritische Funktionen für die Bereitstellung der Dienste festgelegt werden; und
  - Resilienzanforderungen zur Unterstützung der Bereitstellung der Dienste werden für alle Betriebszustände festgelegt (z. B. unter Zwang/Angriff, während der Wiederherstellung, normaler Betrieb).
- Die Richtlinien, Verfahren und Prozesse zur Verwaltung und Überwachung der regulatorischen, rechtlichen, risikobezogenen, umweltbezogenen und betrieblichen

Anforderungen des Unternehmens werden verstanden und dienen dem Management von Sicherheitsrisiken. Dazu gehört unter anderem, dass sichergestellt wird, dass:

- Cyber- und Informationssicherheitsrichtlinien werden festgelegt und kommuniziert;
- Die Rollen und Verantwortlichkeiten der Cyber- und Informationssicherheit werden mit internen Rollen und externen Partnern koordiniert und abgestimmt.
- Gesetzliche und behördliche Anforderungen in Bezug auf Cyber- und Informationssicherheit, einschließlich der Verpflichtungen in Bezug auf Privatsphäre, Datenschutz und bürgerliche Freiheiten, werden verstanden und verwaltet. und
- Governance- und Risikomanagementprozesse befassen sich mit Sicherheitsrisiken.

- Ein Prozess zur Identifizierung, Bewertung und Steuerung von Risiken in der Lieferkette wird etabliert, implementiert und aufrechterhalten. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Risikomanagementprozesse in der Lieferkette werden identifiziert, etabliert, bewertet und verwaltet, um Sicherheitsrisiken zu reduzieren.
  - Lieferanten und Drittpartner der Systeme des Lieferanten, Komponenten solcher Systeme und Dienstleistungen werden mithilfe eines Risikobewertungsprozesses in der Lieferkette identifiziert, priorisiert und bewertet.
  - Die Reaktions- und Wiederherstellungsplanung und -tests werden mit Lieferanten und Drittanbietern durchgeführt.
  - Die Standorte, an denen personenbezogene Daten von Securitas gespeichert werden, einschließlich Rechenzentren, Büros und externe Speichereinrichtungen, verfügen über angemessene und vereinbarte physische Sicherheitskontrollen; und
  - Sicherstellen, dass Risikobewertungen für alle Lieferanten unter Verwendung branchenweit anerkannter Methoden durchgeführt werden.
- Das Unternehmen kommuniziert proaktiv und nutzt formelle und informelle Mechanismen, um Sicherheitsrisiken zu reduzieren, die von Dritten in seiner Lieferkette ausgehen. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Verträge mit Lieferanten und Drittpartnern werden verwendet, um geeignete technische und organisatorische Maßnahmen zur Reduzierung von Sicherheitsrisiken zu implementieren; und
  - Lieferanten und Drittanbieter werden routinemäßig anhand von Audits, Testergebnissen oder anderen Formen von Bewertungen bewertet, um zu bestätigen, dass sie die Sicherheitsanforderungen erfüllen.

3 Schutz von Systemen und Securitas-Daten

3.1 Der Lieferant stellt sicher:

- Er entwickelt, implementiert und unterhält geeignete technische und organisatorische Maßnahmen zum Schutz der Systeme des Lieferanten, der Securitas-Systeme (soweit in den Dienstleistungen angegeben), der Securitas-Daten und der Erbringung der Dienstleistungen.
- Seine Fähigkeit, die Auswirkungen eines potenziellen Sicherheitsereignisses auf Systeme, Securitas-Systeme (in dem in den Services angegebenen Umfang), Securitas-Daten und die Risiken für die Rechte und Freiheiten der betroffenen Personen zu begrenzen oder einzudämmen.
- Der Zugriff auf physische und logische Vermögenswerte und zugehörige Einrichtungen ist auf autorisierte Benutzer, Prozesse und Geräte beschränkt und wird in Übereinstimmung mit dem bewerteten Risiko eines unbefugten Zugriffs auf autorisierte Aktivitäten und Transaktionen verwaltet. Dazu gehört unter anderem, dass sichergestellt wird, dass:

- Identitäten und Anmeldeinformationen werden für autorisierte Geräte, Benutzer und Prozesse ausgestellt, verwaltet, verifiziert, widerrufen und geprüft.
- Der physische Zugang zu Vermögenswerten wird verwaltet und geschützt;
- Der Fernzugriff auf die Lieferantenumgebung, die Securitas-Daten verarbeitet, wird durch Multi-Faktor-Authentifizierung verwaltet.
- Zugriffsberechtigungen und -berechtigungen werden unter Berücksichtigung der Prinzipien der geringsten Rechte und der Aufgabentrennung verwaltet.
- Passwörter werden weder digital noch auf Papier im Klartext übermittelt, auf dem Bildschirm angezeigt oder aufgeschrieben;
- Die Netzwerkintegrität ist geschützt (z. B. Netzwerktrennung, Netzwerksegmentierung);
- Identitäten werden überprüft und an Anmeldeinformationen gebunden und in Interaktionen bestätigt. und
- Benutzer, Geräte und andere Vermögenswerte, die Securitas-Daten verarbeiten, werden entsprechend den Sicherheitsrisiken authentifiziert (z. B. Multi-Faktor-Authentifizierung).

- Die Mitarbeiter und Partner des Unternehmens erhalten Schulungen zum Sicherheitsbewusstsein und werden darin geschult, ihre sicherheitsbezogenen Aufgaben und Verantwortlichkeiten in einer Weise zu erfüllen, die mit der Good Industry Practice vereinbar ist. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Alle Mitarbeiter werden branchenüblichen Hintergrundüberprüfungen nach bewährten Einstellungspraktiken unterzogen.
  - Alle Entwickler von KI-Systemen bieten Schulungen zu KI-Sicherheitsrisiken und Best Practices an
  - Alle Nutzer der Systeme des Lieferanten und/oder der Securitas-Daten werden über Sicherheitsrisiken informiert und entsprechend geschult, um diese Risiken zu reduzieren;
  - Privilegierte Benutzer verstehen ihre Rollen und Verantwortlichkeiten in Bezug auf die Sicherheit der Systeme des Anbieters und der Securitas-Daten, einschließlich, aber nicht beschränkt auf ihre Verantwortung in Bezug auf den Schutz ihres Benutzerkontos und ihrer Passwortdaten;
  - Externe Stakeholder (z. B. Lieferanten, Kunden, Partner) verstehen ihre Rollen und Verantwortlichkeiten in Bezug auf die Sicherheit der Systeme des Lieferanten und der Securitas-Daten;
  - Führungskräfte verstehen ihre Rollen und Verantwortlichkeiten in Bezug auf die Sicherheit der Systeme des Lieferanten und der Securitas-Daten; und
  - Das physische, Cyber- und Informationssicherheitspersonal versteht seine Rollen und Verantwortlichkeiten in Bezug auf die Sicherheit der Systeme des Lieferanten und der Securitas-Daten.
- Die Systeme des Lieferanten werden effektiv verwaltet, um Sicherheitsrisiken zu reduzieren und die Vertraulichkeit, Integrität und Verfügbarkeit von Securitas-Daten zu schützen. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Ruhende Daten sind geschützt (Message-Digest-Algorithmus (Hash-Funktion) SHA-256; Symmetrischer Schlüsselalgorithmus AES-256 / rijndael-256 oder asymmetrischer Schlüsselalgorithmus (wird für die Verteilung des öffentlichen Schlüssels bei mindestens RSA-1024 verwendet);
  - Daten während der Übertragung sind geschützt (mindestens Secure Transport Protocol TLS v1.2);
  - Die Systeme des Lieferanten werden, während der gesamten Entfernungs-, Übertragungs- und Entsorgungsaktivitäten formell verwaltet;
  - Schutzmaßnahmen werden implementiert und aufrechterhalten, um Datenlecks zu verhindern.
  - Für Securitas Data werden separate Datenbanken geführt; und

- Alle Mitarbeiter, Auftragnehmer und andere Dritte unterzeichnen Vertraulichkeitsvereinbarungen, bevor sie auf Securitas-Daten zugreifen.

- Sicherheitsrichtlinien (die sich mit Zweck, Umfang, Rollen, Verantwortlichkeiten, Managementverpflichtung und Koordination befassen), Prozesse und Verfahren werden gepflegt und verwendet, um den Schutz der Systeme und Securitas-Daten des Lieferanten zu verwalten. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Es wird eine grundlegende Konfiguration der Informationstechnologie und der Steuerungssysteme unter Berücksichtigung von Sicherheitsprinzipien und guter Branchenpraxis (z. B. Konzept der geringsten Funktionalität) erstellt und gepflegt.
  - Ein Systementwicklungslebenszyklus zur Verwaltung der Systeme des Lieferanten wird implementiert und gepflegt und für die Entwicklung der generativen KI übernommen
  - Richtlinien und Vorschriften in Bezug auf die physische Betriebsumgebung für organisatorische Vermögenswerte eingehalten werden;
  - Reaktionspläne (Incident Response und Business Continuity) und Wiederherstellungspläne (Incident Recovery und Disaster Recovery) sind vorhanden, verwaltet und werden routinemäßig getestet. und
  - Ein Vulnerability Management Plan wird entwickelt und umgesetzt.
- Die Wartung und Reparatur der Systeme des Lieferanten und der Komponenten dieser Systeme hat keinen Einfluss auf die Sicherheit dieser Systeme oder der Securitas-Daten.
- Schutz vor GenAI-Würmern und anderer bösartiger Software
  - Nur vertrauenswürdige Daten werden für das Training des KI-Systems verwendet
  - Es werden keine Securitas-Daten für das Training des KI-Systems verwendet
  - Prompt Sanitization ist implementiert – Filter zur Überprüfung und Bereinigung von Prompts, um die Einschleusung bösartiger Inhalte zu verhindern, werden implementiert
  - Behavioral Monitoring ist vorhanden - Verhalten des KI-Systems bei ungewöhnlichen Aktivitäten, die darauf hindeuten könnten, dass ein Wurm oder andere Malware überwacht wird
  - Das KI-System und seine Umgebungen werden mit den neuesten Sicherheitspatches aktualisiert, um bekannte Schwachstellen zu minimieren
  - Das KI-System wird anhand von gegnerischen Beispielen trainiert, um seine Widerstandsfähigkeit gegen Angriffe zu verbessern
  - Der Lieferant hat Algorithmen für maschinelles Lernen implementiert, die anomales Verhalten erkennen können, das auf eine Sicherheitsverletzung oder Infektion hindeutet
- Technische Sicherheitslösungen werden verwaltet, um die Sicherheit und Belastbarkeit der Systeme des Lieferanten und der Securitas-Daten zu gewährleisten. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Backups von Informationen werden durchgeführt, gepflegt und getestet.
  - Audit-/Protokollaufzeichnungen werden in Übereinstimmung mit der Good Industry Practice ermittelt, dokumentiert, implementiert und überprüft.
  - Sicherstellen, dass technische Schwachstellenmanagementprozesse eingehalten werden, um die Software auf dem neuesten Stand zu halten, indem Sicherheitspatches angewendet werden, sobald sie verfügbar sind. Dieser Prozess umfasst (1) eine Richtlinie zum Schwachstellenmanagement, einschließlich der Zielbereitstellungszeiten für Patches mit unterschiedlichen Kritikalitätsstufen; (2) Bekanntheit von Patch-Releases; (3) dokumentiertes Bewusstsein für fehlende Flecken in der Umgebung; (4) einen Mechanismus zum Bereitstellen von Patches in der gesamten Umgebung; und (5) die Anforderung, dass die kritischsten Patches sofort angewendet werden;
  - Das Prinzip der geringsten Funktionalität wird dadurch berücksichtigt, dass die Systeme des Lieferanten so konfiguriert werden, dass sie nur wesentliche Funktionen bereitstellen.

- Kommunikations- und Steuerungsnetze sind geschützt;
- Perimeter-Abwehrmaßnahmen wie Firewalls, Intrusion-Prevention-/Detection-Systeme und Data Loss Prevention-Lösungen werden implementiert und gewartet;
- Antiviren- oder Anti-Malware-Systeme werden für alle Systeme implementiert und gewartet.
- Alle Systeme des Lieferanten verfügen über eine sichere Konfiguration.
- Alle Festplatten von Laptops und Desktop-PCs, tragbaren Medien, Servern/Festplatten und/oder Datenbanken werden gemäß der Good Industry Practice verschlüsselt.
- Sicherstellung, dass Software zur Verwaltung mobiler Geräte verwendet wird, um Sicherheitskontrollen auf vom Unternehmen bereitgestellten und mitarbeitereigenen Geräten zu verwalten, die für geschäftliche Zwecke verwendet werden;
- Wenn die Systeme des Lieferanten öffentlichen Netzwerken wie dem Internet ausgesetzt sind, sind sie angemessen vor einer Reihe von Bedrohungen geschützt, die für diese mögliche Gefährdung relevant sind. Dazu gehören eine angemessene logische oder physische Trennung der Systeme des Lieferanten, Authentifizierungsanforderungen sowie klar definierte Ports und Protokolle, die zur Unterstützung der für Securitas erbrachten Dienstleistungen offengelegt werden müssen, einschließlich Schwachstellen-Scans und Penetrationstests durch einen spezialisierten Dritten.
  Sofern zwischen dem Lieferanten und Securitas in Bezug auf eine Schwachstelle/Schwachstelle, die infolge eines Schwachstellen-Scans in den Systemen des Lieferanten aufgedeckt wird, nichts anderes vereinbart wurde, hat der Lieferant Securitas unverzüglich zu benachrichtigen und alle kritischen Schwachstellen/Schwachstellen zu erkennen, die innerhalb eines mit Securitas vereinbarten Zeitrahmens vollständig zur Zufriedenheit von Securitas behoben werden müssen.

4 Erkennen des Auftretens eines Sicherheitsereignisses

4.1 Der Lieferant stellt sicher:

- Sie entwickelt, implementiert und unterhält geeignete technische und organisatorische Maßnahmen, um das Eintreten eines Sicherheitsereignisses zu erkennen.
- Es ist in der Lage, Sicherheitsereignisse zeitnah zu erkennen.
- Anomale Aktivitäten werden erkannt, und die potenziellen Auswirkungen von Sicherheitsereignissen werden verstanden. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Eine Baseline des Netzwerkbetriebs und der erwarteten Datenflüsse für Benutzer und Systeme wird erstellt, verwaltet und getestet.
  - Erkannte Ereignisse werden analysiert, um Angriffsziele und -methoden zu verstehen.
  - Daten zu Sicherheitsereignissen werden aus mehreren Quellen und Sensoren gesammelt und korreliert. und
  - Die Schwellenwerte für die Alarmierung von Vorfällen werden in Übereinstimmung mit den Best Practices der Branche festgelegt.
- Systeme werden überwacht, um Sicherheitsereignisse zu identifizieren und die Wirksamkeit von Schutzmaßnahmen zu überprüfen. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Netzwerke werden auf potenzielle Sicherheitsereignisse überwacht.
  - Die physische Umgebung wird auf potenzielle Sicherheitsereignisse überwacht.
  - Die Aktivitäten des Personals werden auf potenzielle Sicherheitsereignisse überwacht.
  - Überwachung auf bösartigen Code;

- Überwachung auf nicht autorisierte mobile Codes;
- Die Aktivitäten externer Dienstleister werden überwacht, um potenzielle Sicherheitsereignisse zu erkennen.
- Überwachung auf unbefugtes Personal, Verbindungen, Geräte und Software durchgeführt wird; und
- Es werden Schwachstellen-Scans durchgeführt.

- Erkennungsprozesse und -verfahren werden aufrechterhalten und getestet, um sicherzustellen, dass anomale Ereignisse erkannt werden. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Die Rollen und Verantwortlichkeiten für die Erkennung sind klar definiert, um die Rechenschaftspflicht zu gewährleisten.
  - Die Erkennungsprozesse entsprechen allen geltenden Anforderungen und stehen im Einklang mit der Good Industry Practice.
  - Detektionsprozesse werden getestet;
  - Informationen zur Ereigniserkennung werden an die relevanten Parteien weitergegeben, um sicherzustellen, dass auf Ereignisse wie erforderlich reagiert wird. und
  - Die Detektionsprozesse werden im Einklang mit der Good Industry Practice kontinuierlich aktualisiert.

5 Reaktion auf Sicherheitsvorfälle

5.1 Der Lieferant stellt sicher:

- Sie entwickelt, implementiert und unterhält geeignete technische und organisatorische Maßnahmen, um auf einen Sicherheitsvorfall zu reagieren, einschließlich, aber nicht beschränkt auf die Fähigkeit, die Auswirkungen von Sicherheitsvorfällen auf die Rechte und Freiheiten der betroffenen Personen zu verringern.
- Der Lieferant stellt sicher, dass er in der Lage ist, die Auswirkungen eines potenziellen Sicherheitsvorfalls einzudämmen.
- Reaktionsprozesse und -verfahren werden ausgeführt und aufrechterhalten, um eine effektive und zeitnahe Reaktion auf erkannte Sicherheitsvorfälle zu gewährleisten.
- Die Reaktionsmaßnahmen werden mit internen und externen Akteuren und erforderlichenfalls mit den Strafverfolgungsbehörden koordiniert. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Das Personal kennt seine Rollen und die Reihenfolge der Operationen, wenn eine Reaktion erforderlich ist. und
  - Sicherheitsvorfälle werden in Übereinstimmung mit festgelegten Kriterien gemeldet.
- Die Analyse wird durchgeführt, um sicherzustellen, dass die Reaktion auf einen Sicherheitsvorfall effektiv ist und die Wiederherstellung von Systemen und Securitas-Daten unterstützt und potenzielle Schäden für die Rechte und Freiheiten der betroffenen Personen mindert. Dazu gehört unter anderem, dass sichergestellt wird, dass:
  - Benachrichtigungen von Erkennungssystemen werden untersucht;
  - Die Auswirkungen von Sicherheitsvorfällen sind bekannt;
  - Forensik wird bei Bedarf durchgeführt;
  - Vorfälle werden in Übereinstimmung mit Reaktionsplänen und Melde-/Meldepflichten kategorisiert. und
  - Es werden Prozesse eingerichtet, um Schwachstellen zu empfangen, zu analysieren und darauf zu reagieren, die dem Unternehmen aus internen und externen Quellen (z. B. interne Tests,

Security Bulletins oder Sicherheitsforscher) mitgeteilt werden.

- Es werden Aktivitäten durchgeführt, um die Ausbreitung eines Ereignisses zu verhindern, seine Auswirkungen zu mindern und den Vorfall zu beheben.
- Die Reaktionsaktivitäten werden verbessert, indem die Erkenntnisse aus aktuellen und früheren Erkennungs-/Reaktionsaktivitäten nach einer detaillierten und dokumentierten Post-Mortem-Überprüfung einbezogen werden.

6 Wiederherstellung nach Sicherheitsvorfällen

6.1 Der Lieferant stellt sicher:

- Es entwickelt, implementiert und wartet geeignete technische und organisatorische Maßnahmen zur Aufrechterhaltung der Resilienz und zur Wiederherstellung von Fähigkeiten oder Diensten, die aufgrund eines Sicherheitsvorfalls beeinträchtigt wurden.
- Es ist in der Lage, die Auswirkungen eines Sicherheitsvorfalls zu reduzieren und eine zeitnahe Wiederherstellung des normalen Betriebs zu ermöglichen.
- Wiederherstellungsprozesse und -verfahren werden ausgeführt und aufrechterhalten, um die Wiederherstellung von Systemen und Securitas-Daten zu gewährleisten, die von Sicherheitsvorfällen betroffen sind.
- Die Wiederherstellungsplanung und -prozesse werden verbessert, indem die gewonnenen Erkenntnisse in zukünftige Aktivitäten einbezogen werden.
- Die Wiederherstellungsaktivitäten werden mit internen und externen Parteien koordiniert (z. B. Koordinierungszentren, Internetdienstanbieter, Eigentümer von Angriffssystemen, Opfer, andere CSIRTs und Anbieter).

7 Benachrichtigung über Vorfälle

7.1 Der Lieferant benachrichtigt Securitas unverzüglich, spätestens jedoch innerhalb von 48 (achtundvierzig) Stunden, wenn er tatsächliche, drohende oder potenzielle Sicherheitsereignisse und Sicherheitsvorfälle vermutet oder Kenntnis davon erlangt, und stellt sicher, dass alle diese Mitteilungen vollständige und vollständige Angaben zu einem solchen Verstoß enthalten, insbesondere:

- Die Art und den Sachverhalt eines solchen Verstoßes, einschließlich der Kategorien und der Anzahl der Securitas-Datensätze und gegebenenfalls der betroffenen Personen, der Kategorien und der ungefähren Anzahl der betroffenen Personen (und der Identität der betroffenen Personen, falls bekannt);
- Die Kontaktdaten des Datenschutzbeauftragten oder eines anderen vom Lieferanten ordnungsgemäß benannten Vertreters, von dem Securitas weitere Informationen in Bezug auf einen solchen Verstoß erhalten kann;
- Die wahrscheinlichen Folgen oder potenziellen Folgen eines solchen Verstoßes und Einzelheiten darüber, ob die personenbezogenen Daten verschlüsselt wurden; und
- Die Maßnahmen, die vom Lieferanten und/oder dem Lieferantenpersonal ergriffen oder vorgeschlagen werden, um einen solchen Verstoß zu beheben und mögliche nachteilige Auswirkungen zu mindern, sowie die Umsetzungstermine für solche Maßnahmen.

und wenn, aber nur insoweit, als es nicht möglich ist, die in diesem Unterabsatz genannten Informationen zu übermitteln 7.1 gleichzeitig mit der Meldung werden diese Informationen schrittweise zur Verfügung gestellt, sobald sie verfügbar sind (und zwar in einer Weise, die es Securitas oder dem jeweiligen Securitas-Unternehmen ermöglicht, ihren Melde- und Dokumentationspflichten nachzukommen).

7.2 Der Lieferant wird mit Securitas und allen anderen mit Securitas verbundenen Unternehmen (soweit erforderlich) zusammenarbeiten und angemessene kommerzielle Schritte unternehmen, die von Securitas angewiesen werden, um Securitas (oder das betreffende Securitas-Tochterunternehmen) bei der Untersuchung, Minderung und Behebung jedes Verstoßes zu unterstützen und (sofern nicht anders mit Securitas vereinbart) unverzüglich Maßnahmen zu ergreifen, um den Verstoß zu stoppen, Securitas-Daten oder andere Informationen wiederherzustellen und Schwachstellen zu beheben, um weitere Verstöße zu verhindern.

7.3 Im Falle eines Verstoßes darf der Lieferant Dritte nicht informieren, ohne zuvor die schriftliche Zustimmung von Securitas eingeholt zu haben, es sei denn, die Benachrichtigung ist nach den lokalen Gesetzen (wie z. B. dem Recht der Europäischen Union), denen der Lieferant unterliegt, erforderlich, in welchem Fall der Lieferant Securitas über diese gesetzliche Verpflichtung informieren wird (es sei denn, das Gesetz verbietet eine solche Benachrichtigung aus wichtigen Gründen des öffentlichen Interesses), eine Kopie der vorgeschlagenen Meldung zur Verfügung zu stellen und etwaige Stellungnahmen von Securitas zu berücksichtigen, bevor der Verstoß gemeldet wird.

8 Revisionsrechte

- Zusätzlich zu diesen Verpflichtungen in diesem Vertrag hat Securitas das Recht, die IT-Sicherheitskontrollen des Lieferanten mit einer angemessenen Frist von mindestens 30 Tagen zu überprüfen;
- Der Lieferant nimmt an Umfragen und Fragebögen teil, um die für die Bewertung der IT-Sicherheit von Securitas erforderlichen Nachweise zu erbringen;
- Der Lieferant hat den Nachweis über regelmäßige Schwachstellen-Scans seiner IT-Umgebungen sowie Sicherheitsaudits von KI-Systemen und Pentests zu erbringen;
- Für den Fall, dass während des Scannens oder Testens Schwachstellen gefunden werden, wird der Lieferant Zeitrahmen für die Behebung solcher Fehler durch den Lieferanten festlegen.