# Grundlegende Informationssicherheitsanforderungen für Geschäftspartner

**Die folgenden Informationssicherheitsanforderungen gelten für alle Geschäftspartner (nachfolgend "Geschäftspartner") von Securitas.**

1. Der Geschäftspartner muss geeignete organisatorische und technische Maßnahmen ergreifen, um die Vertraulichkeit, Authentizität, Integrität und Verfügbarkeit des Betriebs des Geschäftspartners sowie seiner Produkte und Dienstleistungen zu gewährleisten. Diese Maßnahmen müssen der guten Branchenpraxis entsprechen und ein angemessenes Informationssicherheitsmanagementsystem umfassen, das Normen wie die ISO/IEC 27001 oder dem BSI-Grundschutz entspricht, und für die Mitarbeitenden mindestens folgendes umfasst:
   i. Allgemeine Schulung zum Sicherheitsbewusstsein;
   ii. Authentifizierungsanforderungen für Mitarbeitende;
   iii. Zugriffsberechtigungen, die den Grundsätzen der "geringsten Privilegien" („Least Privilege“) und gegebenenfalls der "Aufgabentrennung" („Segregation of Duties“) entsprechen;
   iv. Endpunkt-Cybersicherheitsmaßnahmen, die Virenschutz, Anwendungskontrollen oder andere, geeignete Systeme umfassen können;
   v. Audit-Protokollierung von Systemen, die auf kritische Daten des Geschäftspartners zugreifen, diese speichern oder verarbeiten;
   vi. Backup-, Wiederherstellungs- und Business-Continuity-Maßnahmen zur Sicherstellung des laufenden Geschäftsbetriebs (z. B. während eines Ransomware-Ereignisses).

   Der Begriff „Betrieb des Geschäftspartners“ bezeichnet alle Vermögenswerte, Prozesse und Systeme (einschließlich Informationssysteme), Daten (einschließlich Daten von Securitas und deren Kunden), Personal und Standorte, die der Geschäftspartner von Zeit zu Zeit bei der Erfüllung dieses Vertrags nutzt oder verarbeitet.

2. Sollten Produkte oder Dienstleistungen Software, Firmware, Chipsätze oder integrierte Schaltkreise enthalten, gilt folgendes:
   i. Der Geschäftspartner muss sichere, dem Stand der Technik entsprechende Softwareentwicklungsmethoden einhalten, einschließlich sicherer Kodierungsstandards, z. B. OWASP-Standards;
   ii. der Geschäftspartner setzt geeignete Standards, Verfahren und Methoden ein, um Schwachstellen, bösartigen Code und Sicherheitsvorfälle in Produkten und Dienstleistungen zu verhindern, zu identifizieren, zu bewerten und zu beheben, die mit bewährten Branchenpraktiken und Standards wie ISO/IEC 27001 oder BSI-Grundschutz übereinstimmen;
   iii. der Geschäftspartner wird des weiteren Support und Dienstleistungen zur Reparatur, Aktualisierung, Aufrüstung und Wartung der Produkte und Dienstleistungen erbringen, einschließlich der Bereitstellung von Patches für Securitas, zur Behebung von Schwachstellen während der angemessenen Lebensdauer der Produkte und Dienstleistungen;
   iv. der Geschäftspartner räumt Securitas das Recht ein, die von ihm gelieferten Produkte oder Softwarekomponenten jederzeit auf Schadcode und Schwachstellen zu testen und wird Securitas dabei angemessen unterstützen;
   v. der Geschäftspartner stellt Securitas einen Ansprechpartner für alle Fragen der Informationssicherheit zur Verfügung (erreichbar während der Geschäftszeiten).
   vi. Falls Künstliche Intelligenz verwendet wird, dürfen die Securitas Daten nicht für das Training der KI verwendet werden.

3. Der Geschäftspartner ist verpflichtet, der ihm genannten Securitas Ansprechperson und den folgenden Securitas Informationssicherheit-Kontaktadressen unverzüglich und zeitnah alle relevanten Informationssicherheitsvorfälle zu melden, die eingetreten sind oder bei denen der Verdacht besteht, dass sie eingetreten sind, sowie Schwachstellen, die in den Betriebsabläufen, Dienstleistungen und Produkten des Geschäftspartner entdeckt wurden, wenn und soweit Securitas davon wesentlich betroffen ist oder betroffen sein könnte:
   i. für Sicherheitsvorfälle und Sicherheitsschwachstellen („Vulnerabilities“): informationssicherheit@securitas.de
4. Der Geschäftspartner ergreift geeignete Maßnahmen, um sicherzustellen, dass seine Subunternehmer und Lieferanten innerhalb eines angemessenen Zeitraums ähnliche Verpflichtungen, wie in diesen Informationssicherheitsanforderungen gefordert, eingehen.
5. Falls „Securitas-Daten“ verarbeitet und gespeichert werden, müssen sie DSGVO-konform sein - EU-Standort.
6. Für den privilegierten Zugriff auf Securitas-Systeme oder -Anwendungen müssen die Rollen und Verantwortlichkeiten für das Privileged Access Management der Anbieteradministratoren (Identitätsmanagement, Zugriffsgewährung, Zugriffsentzug, Zugriffsüberprüfung) angewendet werden, und der Geschäftspartner muss die Richtlinie zur akzeptablen Nutzung für privilegierte Konten einhalten.
7. Der Geschäftspartner hat einen Failover-Plan, Backups und DRM/BCM implementiert, die die für Securitas erbrachte Dienstleistung betreffen.
8. Es besteht eine Cyber-Versicherung oder ein relevanter Incident-Response-Plan, der Verluste durch Sicherheitsverletzungen auf Seiten des Geschäftspartners abdeckt.
9. Beim Verbinden mit Securitas-Systemen dürfen nur sichere Protokolle verwendet werden.
10. Der Geschäftspartner ist verpflichtet, Securitas auf Anfrage einen schriftlichen Nachweis über die Einhaltung der Informationssicherheitsanforderungen vorzulegen, einschließlich allgemein anerkannter Auditberichte (z.B. ISO 27001, SoA und Scope Dokumente).
11. Securitas hat das Recht, die Einhaltung der Bestimmungen dieser Informationssicherheitsanforderungen durch den Geschäftspartner an dessen Standort(en), nach angemessener Vorankündigung, zu überprüfen, wenn Securitas den begründeten Verdacht hegt, dass der Geschäftspartner diese nicht einhält.