Leitlinie zur Informationssicherheit
PCS / GPI CEE

Version: 1.0

Inhaltsverzeichnis

1 Einleitung

Die Informationssicherheitsleitlinie (ISL) beschreibt den Stellenwert, die verbindlichen Prinzipien und das angestrebte Niveau der Informationssicherheit für PCS und GPI CEE (im Folgenden kurz „Organisation“). Ziel ist es, die **Vertraulichkeit, Integrität** und **Verfügbarkeit** aller Informationen sicherzustellen, Risiken zu minimieren und gesetzlichen sowie vertraglichen Anforderungen zu entsprechen. Die ISL definiert die erforderlichen Sicherheitsziele sowie den organisatorischen Rahmen, in dem diese Ziele umgesetzt werden. Sie basiert auf den Vorgaben des IT-Grundschutz-Standards des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und A_SIT.

2 Stellenwert der Informationssicherheit

Informationssicherheit umfasst neben IT-Systemen auch Papierunterlagen in Form von Akten und sonstigen Unterlagen sowie Daten im allgemeinen Sinn. Sie umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um die Informationssicherheit zu gewährleisten.

Der Tätigkeitsbereich der Organisation als Zulieferer für Gesundheitsdienste-Anbieter sowie als Anbieter von gehosteten Applikation (Cloud) im Gesundheitswesen erfordert den höchstmöglichen Stellenwert für Informationssicherheit und Verfügbarkeit der angebotenen Applikationen. Die Organisation betreibt ein umfangreiches Informationssicherheitsmanagementsystem (ISMS), das den Anforderungen des BSI (DE) und A_SIT (AT) entspricht. Die Geschäftsführung und alle Mitarbeiter und werden regelmäßig auf Informationssicherheit geschult und sind vertraglich zur Geheimhaltung verpflichtet.

3 Geltungsbereich

Diese Leitlinie gilt für:

- alle internen und externen Mitarbeitenden und Führungskräfte der Organisation
- alle Standorte der Organisation
- sämtliche IT-Systeme, Anwendungen, Kommunikationsmittel und physischen Informationsquellen
- alle Arten von Informationen, unabhängig von Medium oder Format
- alle Lieferanten, Dienstleister und sonstige involvierten externe Parteien

4 Grundsätze der Informationssicherheit

Die Informationssicherheit betrifft Informationen, die in elektronischer oder gedruckter/schriftlicher Form vorliegen, aber auch mündlich übermittelte Informationen, z. B. in Telefonaten oder Gesprächen.

Zur Wahrung der Informationssicherheit dienen die folgenden Schutzziele:

Vertraulichkeit

- Informationen dürfen nur von berechtigten Personen eingesehen oder verarbeitet werden
- Zugriffe sind nach dem Need-to-Know-Prinzip zu gewähren

Integrität

- Informationen müssen vollständig, korrekt und unverändert sein
- Änderungen dürfen nur durch autorisierte Personen erfolgen
- Änderungen müssen nachvollziehbar dokumentiert werden

Verfügbarkeit

- Informationen und Systeme müssen für berechtigte Nutzer*innen zum notwendigen Zeitpunkt zugänglich sein.
- Entsprechende Backup-, Redundanz- und Notfallmaßnahmen müssen vorhanden sein

5 Rollen und Verantwortungen

Geschäftsführung
- Trägt die Gesamtverantwortung für die Informationssicherheit
- Stellt die notwendigen Ressourcen zur Aufrechterhaltung der angestrebten Informationssicherheit bereit
- Genehmigt Leitlinien und wesentliche Maßnahmen
- Überwacht und prüft das ISMS in Managementbewertungen

Chief Information Security Officer (CISO)
- Entwickelt, überwacht und verbessert laufend das ISMS
- Koordiniert Schulungen und Sensibilisierungsmaßnahmen
- Ist Ansprechperson für Sicherheitsvorfälle

Mitarbeiter*innen
- Halten diese Leitlinie sowie weitere Vorgaben des internen Information Security Management Systems ein
- Melden Sicherheitsvorfälle unverzüglich
- Behandeln vertrauliche Informationen entsprechend den Vorgaben der DSGVO

Externe Parteien
- Sind vertraglich zur Einhaltung der Sicherheitsstandards der Organisation verpflichtet

6 Schutzmaßnahmen

Zur Gewährleistung der Informationssicherheit sind folgende Schutzmaßnahmen umgesetzt:

Zugangskontrolle
- Passwortrichtlinie für starke Passwörter
- Multi-Faktor-Authentifizierung (MFA), wenn technisch möglich
- Zugang nur auf Daten/Systeme, die zur Arbeit unbedingt nötig sind (Need-to-Know Prinzip)
- Regelmäßige Kontrolle der Benutzerrechte
- Sperrung von nicht mehr benötigten Konten
- Einsatz von Passwort Tresor

Datensicherung und Wiederherstellung
- Regelmäßige Backups gemäß Backup-Plan
- Test der Wiederherstellungsprozesse

Physische Sicherheit
- Zutrittskontrollen zu Gebäuden
- Streng geregelter Zugang zu Serverräumen
- Schutz der IT-Assets vor Feuer, Wasser, Diebstahl

IT- und Netzwerksicherheit
- Vulnerability und Patch Management
- Firewall- und Virenschutzsysteme
- Netzwerk-Segmentierung
- Systemhärtung
- Verschlüsselte Datenübertragung, sofern technisch möglich

Mobile Geräte und Home-Office
- Verschlüsselung von allen Datenträgern
- Mobile Device Management
- Zero Trust Access von Home-Office Geräten
- Externer Zugang nur über VPN

Umgang mit sensiblen Daten

- Klassifizierung von Informationen
- Sichere Aufbewahrung und ordnungsgemäße Vernichtung

7 Schulungen und Sensibilisierung

Alle Mitarbeitenden werden regelmäßig in Informationssicherheit geschult.
Dazu zählen u.a.:

- Phishing-Erkennung
- Sicheres Passwortmanagement
- Social Engineering
- Meldewege für Vorfälle
- Rechtliche Anforderungen (z. B. Datenschutz)

8 Sicherheitsvorfälle

Ein Sicherheitsvorfall liegt vor, wenn Informationen oder Systeme kompromittiert, beschädigt oder manipuliert wurden oder dies vermutet wird.

- Vorfälle müssen **unverzüglich** an den CISO gemeldet werden.
- Externe Meldepflichten werden eingehalten.
- Der Vorfall wird behoben und dokumentiert.
- Ursachenanalyse und Maßnahmen zur Vermeidung ähnlicher Vorfälle werden eingeleitet.

9 Gesetzliche und regulatorische Anforderungen

Alle Aktivitäten müssen folgenden Anforderungen entsprechen:

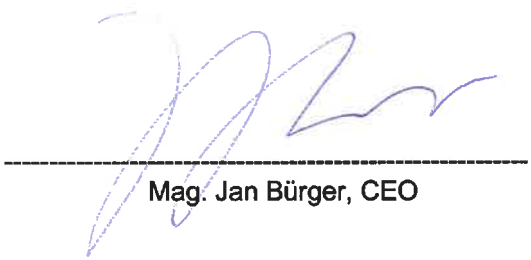
- Datenschutzgesetze (z. B. DSGVO)
- Vertragliche Vereinbarungen mit Kunden, Dienstleistern und Partnern
- Branchenspezifische Standards (BSI-Grundschutz)
- NIS2 Gesetz
- C5 Testat für Cloud Betrieb
- ISO 9001
- ISO 13485 (für Medizinprodukte)

10 Überprüfung und Aktualisierung

Die Leitlinie wird mindestens einmal jährlich oder bei wesentlichen Veränderungen der Prozesse, Systeme oder Bedrohungslage überprüft und ggf. aktualisiert. Die Freigabe erfolgt durch die Geschäftsführung.

11 Freigabe und Inkrafttreten

Diese Informationssicherheits-Leitlinie tritt am 01.07.2026 in Kraft und ist für alle Beteiligten laut Kapitel Geltungsbereich verbindlich.



Mag. Jan Bürger, CEO

Version: 1.0
Stand: 11.06.2026

Kontakt: security@pcs.at