



BG Kliniken

Klinikverbund der gesetzlichen
Unfallversicherung

Dienstleister- und Softwareanforderungen Informationssicherheit / Datenschutz

Informationen zur Datei

Bearbeitet von:	Holger Günther
Freigegeben von:	Holger Günther
Version:	20260430
Erstellt am:	26.06.2026
Aktualisiert am:	
Nächste Überprüfung:	

Hinweis

© BG Kliniken / nur zum internen Gebrauch / Druckversionen unterliegen nicht dem Änderungsdienst!

	Anforderungen an das Content Management System		MUSS/KANN
Datenminimierung	DM-1 Speicherfristen für Protokolldaten (Audit-Logs)	Für Audit-Logs (z. B. System-, Sicherheits- und Nutzeraktivitäten) sind separate Speicherfristen zu definieren. Nach Ablauf der Frist werden die Protokolldaten automatisiert gesperrt oder gelöscht; Fristen müssen konfigurierbar sein.	MUSS
Vertraulichkeit	V-1 Rollen- und Berechtigungskonzept	Der Auftragnehmer stellt ein rollen- und rechtsbasiertes Zugriffskonzept bereit, mit dem Zugangs- und Zugriffskontrollen auf verarbeitete Informationen, insbesondere personenbezogene Daten, differenziert und konfigurierbar abgebildet werden können.	MUSS
	V-2 Authentisierung	Das System stellt Authentisierungsmechanismen nach dem Stand der Technik für Personen und Systeme zur Verfügung (z. B. Benutzer*innennamen/Passwort, Mehr-Faktor-Authentisierung, zertifikatsbasierte Verfahren). Die eingesetzten Verfahren sind konfigurierbar.	MUSS
		Es ist eine Passwortrichtlinie festzulegen und systemseitig durchzusetzen, die mindestens folgende Aspekte berücksichtigt:	
		Mindestlänge und Komplexität (z. B. Groß-/Kleinschreibung, Ziffern, Sonderzeichen)	
		Ausschluss trivialer oder fortlaufender Passwörter	
		Passworthistorie	
		Keine Klartextanzeige bei der Eingabe	
		Verzögerung oder Sperrung nach einer definierbaren Anzahl fehlgeschlagener Anmeldeversuche	
		Mindest- und Höchstgültigkeitsdauer	
	V-3 Passwortrichtlinie	Automatisiert erzwungener Passwortwechsel nach Ablauf der Höchstgültigkeitsdauer	MUSS
	V-4 Single Sign-On	Das System unterstützt die Integration einer Single-Sign-On-Lösung.	KANN
	V-5 Sitzungsmanagement	Benutzer:innen werden nach einem konfigurierbaren Inaktivitätszeitraum automatisiert abgemeldet.	KANN
	V-6 Lebenszyklus von Benutzerkonten	Für Benutzer:innenkonten, Rollen und Rechte sind Gültigkeitsdauern festzulegen; deren Ablauf wird automatisiert berücksichtigt.	KANN
	V-7 Schutz von Zugangsdaten	Zugangsdaten werden ausschließlich verschlüsselt übertragen und gehasht gespeichert, jeweils nach dem Stand der Technik.	MUSS
	V-8 Verschlüsselung der Datenübertragung	Die Übertragung aller Daten erfolgt verschlüsselt nach dem Stand der Technik.	MUSS
	V-9 Verschlüsselung gespeicherter Daten (Systemebene)	Alle erzeugten Daten werden auf Festplattenebene verschlüsselt gespeichert. Der Zugriff auf die verschlüsselten Daten ist auf Auftraggeber und Auftragnehmer beschränkt.	MUSS
Transparenz	T-1 Auditlogging	Das System ermöglicht ein nachvollziehbares, skalierbares Auditlogging von personenbezogenen Benutzer*innen- und Systemaktivitäten, insbesondere von Zugriffen auf personenbezogene Daten.	MUSS
	T-2 Log-Export	Alle Protokolldaten können vollständig und automatisiert exportiert werden (z. B. zur Weiterleitung an zentrale Log- oder Auswertesysteme).	KANN
	T-3 Berechtigungsübersichten	Das System stellt eine aktuelle Übersicht aller zugriffsberechtigten Benutzer*innen einschließlich ihrer zugewiesenen Rechte und Rollen exportierbar bereit.	KANN
	T-4 Monitoring-Integration	Die Anbindung an ein zentrales Monitoringsystem des Auftraggebers wird unterstützt.	KANN
Verfügbarkeit	A-1 Hochverfügbarkeit	Für systemkritische Komponenten ist eine Hochverfügbarkeitsarchitektur umzusetzen.	KANN
	A-2 Datensicherungen	Von allen gespeicherten Informationen, insbesondere personenbezogenen Daten, werden regelmäßig Sicherheitskopien angefertigt.	MUSS
Integrität	I-1 Dokumentierte Rechtevergabe	Die Zuweisung von Benutzerrechten und Rollen ist dokumentiert und nachvollziehbar.	MUSS
	I-2 Updates	Sicherheits- und Funktionsupdates werden regelmäßig bereitgestellt.	MUSS
	I-3 Rollback	Für Updates ist eine Rollback-Möglichkeit vorgesehen.	KANN
	I-4 Automatisierte Updates	Das System unterstützt automatisierte Updateprozesse.	KANN
		Die Anwendung wird unter Einhaltung anerkannter Prinzipien der sicheren Softwareentwicklung entwickelt und betrieben. Dabei werden insbesondere die aktuellen Empfehlungen und Anforderungen des OWASP (z. B. OWASP Top 10, OWASP ASVS oder vergleichbare OWASP-Leitlinien) berücksichtigt.	MUSS
	I-5 Sichere Softwareentwicklung		
	I-6 SDLC	Es wird ein strukturierter Software-Development-Life-Cycle umgesetzt, der Sicherheitsmaßnahmen umfasst.	KANN
	I-7 SIEM-Anbindung	Die Anbindung eines SIEM-Systems des Auftraggebers wird unterstützt.	KANN
Nichtverkettung	NV-1 Minimierung von Schnittstellen	Nicht verwendete Schnittstellen oder Funktionen werden deaktiviert oder entfernt.	MUSS
	NV-2 Trennung von Rollen	Administrative und operative Rechte sind klar getrennt abzubilden.	MUSS

			MUSS/ KANN
1. E-Mail-Gateway / E-Mail-Sicherheit	E-1 Schutz vor unerwünschten und schädlichen E-Mails	Eingehende E-Mails werden am E-Mail-Gateway des Dienstleisters automatisiert gegen regelmäßig aktualisierte, externe Reputations- und Spammerkennungslisten geprüft (z. B. DNS-basierte Blacklists oder vergleichbare Verfahren). Die Prüfung erfolgt vor Zustellung an interne Postfächer. Eingehende E-Mails werden am E-Mail-Gateway des Dienstleisters automatisiert auf potenziell schädliche Inhalte geprüft. Hierzu gehören insbesondere:	MUSS
	E-2 Analyse und Blockierung von Dateianhängen und Links	- die Blockierung oder Quarantäne ausführbarer oder aktiver Dateianhänge (z. B. Skript-, Binary- oder makrohaltige Dateitypen) sowie - die Analyse und Blockierung potenziell bösartiger Hyperlinks innerhalb von E-Mails. Die Prüfung erfolgt vor Zustellung an interne Postfächer. E-Mails, die von externen Absendern eingehen, werden für Endanwender*innen eindeutig als externe Kommunikation gekennzeichnet. Die Kennzeichnung erfolgt automatisiert, z. B. durch:	MUSS
	E-3 Kennzeichnung externer E-Mails	- ein Label in der Betreffzeile oder - ein visuelles Banner im E-Mail-Inhalt.	KANN
2. IPS / IDS	N-1 Intrusion Detection	Der Dienstleister betreibt ein Intrusion-Detection-System (IDS) zur Erkennung von Command-and-Control-Kommunikation sowie sonstigen bekannten bösartigen Netzwerkaktivitäten innerhalb der für wesentliche Geschäftsprozesse genutzten Netzwerke.	KANN
	N-2 Intrusion Prevention	Der Dienstleister betreibt ein Intrusion-Prevention-System (IPS), das erkannte bösartige Netzwerkaktivitäten automatisiert unterbinden kann.	KANN
3. Anti-Malware-Schutz	AM-1 Flächendeckender Malware-Schutz	Auf allen informationsverarbeitenden Systemen wird Anti-Malware-Software nach dem Stand der Technik (z. B. verhaltensbasierte Erkennung / EDR-Funktionalitäten) eingesetzt.	MUSS
	AM-2 Aktualität	Signaturen, Erkennungsmechanismen und Programmstände werden automatisiert und regelmäßig aktualisiert.	MUSS
4. Aktive Inhalte	AC-1 Einschränkung aktiver Inhalte	Die Ausführung aktiver Inhalte ist auf Endanwendersystemen grundsätzlich unterbunden, sofern sie nicht zwingend erforderlich ist.	KANN
	AC-2 Makros	Makros sind standardmäßig deaktiviert; alternativ ist ausschließlich die Ausführung vertrauenswürdig signierter Makros erlaubt.	KANN
	AC-3 Skripte in Dokumenten	Die Ausführung insbesondere von JavaScript in PDF-Readern ist unterbunden.	KANN
5. Benutzerrechte	BR-1 Keine Administratorrechte für Standardnutzer:innen	Normale Benutzerkonten verfügen nicht über lokale oder domänenweite Administratorrechte.	MUSS
	BR-2 Softwareinstallation	Die Installation und Deinstallation von Software, Apps und Add-Ins ist ausschließlich Administrator*innen vorbehalten.	MUSS
	BR-3 Administrationskonten	Zur Systemadministration werden separate, dedizierte Administratorkonten verwendet.	MUSS
	BR-4 Need-to-Know	Zugriffsrechte, insbesondere auf Netzressourcen, werden nach dem Need-to-Know-Prinzip vergeben.	MUSS
	BR-5 Privilege-Escalation-Prüfung	Systeme, die für wesentliche Prozesse erforderlich sind, werden regelmäßig auf Möglichkeiten zur Rechteausweitung geprüft; identifizierte Schwachstellen werden möglichst zeitnah behoben.	KANN
6. Identitäts- und Berechtigungsmanagement	IAM-1 Authentisierungsstandards	Authentisierungsverfahren entsprechen anerkannten Sicherheitsstandards (z. B. BSI-Grundschutz).	KANN
	IAM-2 Administrator-Passwörter	Für Administratorkonten gelten erhöhte Passwortanforderungen (z. B. Mindestlänge ≥ 20 Zeichen, Komplexitätsregeln).	MUSS
	IAM-3 Mehrfaktor-Authentisierung	Administratorkonten sind verpflichtend mit einem zusätzlichen Authentisierungsfaktor abgesichert (z. B. TOTP, FIDO2).	MUSS
	IAM-4 Passwortverwaltung	Für privilegierte Konten wird ein Passwort-Tresor eingesetzt.	KANN
7. Backups	BK-1 Backup-Konzept	Es existiert ein dokumentiertes Backup-Konzept für alle systemkritischen Informationen.	MUSS
	BK-2 Durchführung und Tests	Backups werden regelmäßig erstellt und stichprobenartig auf Wiederherstellbarkeit geprüft.	MUSS
	BK-3 Aufbewahrung	Backups werden gemäß der 3-2-1-1-0-Regel vorgehalten.	KANN
8. IP-Netzwerke	NW-1 Netzsegmentierung	Netzwerke sind zweckgebunden segmentiert.	MUSS
	NW-2 Firewalls	Firewall-Regeln werden restriktiv nach dem Minimalprinzip definiert; insbesondere RDP-, VNC- und SMB-Zugriffe sind eingeschränkt.	MUSS
9. Schulungen & Awareness	AW-1 Regelmäßige Schulungen	Beschäftigte erhalten mindestens alle zwei Jahre Awareness-Schulungen zu Datenschutz und Informationssicherheit, insbesondere zu Ransomware.	MUSS
	AW-2 Phishing-Erkennung	Es werden konkrete Beispiele zur Erkennung schadhafter E-Mails vermittelt.	KANN
	AW-3 Meldeverhalten	Beschäftigte werden über Meldewege bei Sicherheitsvorfällen regelmäßig informiert.	KANN
10. Schlüsselpositionen	SP-1 Qualifikation	Entscheidungsträger:innen und Fachverantwortliche verfügen über nachweisbare Kenntnisse im Umgang mit Sicherheitsvorfällen.	KANN
	SP-2 Verfügbarkeit	Die Erreichbarkeit von Schlüsselrollen ist sichergestellt.	KANN
	SP-3 Management-Einbindung	Die Unternehmensleitung ist regelmäßig über den Stand der Informationssicherheit informiert und in wesentliche Entscheidungen eingebunden.	MUSS
11. Updates & Patchmanagement	UP-1 Patchmanagement	System- und Softwareupdates werden zeitnah entsprechend ihrer Kritikalität eingespielt.	MUSS
	UP-2 Testverfahren	Patches für besonders kritische Systeme werden vorab getestet.	KANN
	UP-3 Legacy-Systeme	Nicht mehr wartbare Systeme werden ersetzt oder außer Betrieb genommen.	KANN
	UP-4 Inventarisierung	Der Aktualitätsstand aller Systeme wird regelmäßig überprüft.	KANN
12. Sicherheitsstandards & Hardening	ST-1 Standardkonfigurationen	Systeme werden nach einheitlichen, gehärteten Sicherheitsstandards betrieben.	MUSS
	ST-2 Software-Minimierung	Es ist ausschließlich Software installiert, die für die Leistungserbringung(en) erforderlich ist.	MUSS
13. Schwachstellenscans	VS-1 Regelmäßige Scans	Schwachstellenscans werden mindestens monatlich durchgeführt.	KANN
	VS-2 Externe Scans	Interne Scans werden regelmäßig durch externe Prüfungen ergänzt.	KANN
	VS-3 Vor Inbetriebnahme	Neue Systeme werden vor Produktivsetzung geprüft.	KANN
14. Lieferketten	SC-1 Subdienstleisterpflichten	Subdienstleister sind vertraglich zur Einhaltung gleichwertiger Sicherheitsstandards verpflichtet.	MUSS
	SC-2 Transparenz	Betriebsstätten, Subdienstleister und Leistungserbringungsorte werden offengelegt.	KANN
	SC-3 Drittlandverarbeitung	Für Drittlandverarbeitungen wird ein Transfer Impact Assessment bereitgestellt.	MUSS
	SC-4 Ausschluss bestimmter Staaten	Keine Verarbeitung in Staaten gemäß der BMI-Staatenliste nach § 13 Abs. 1 Nr. 17 SÜG.	MUSS
15. Fernzugriffe	RA-1 Technischer Schutz	Fernzugriffe entsprechen dem Stand der Technik (VPN, MFA, Jump-Server).	MUSS
	RA-2 Protokollierung	Restriktive Handhabung von Fernzugriffen von Subdienstleistern auf Systeme des Dienstleisters und flächendeckende Protokollierung dieser.	MUSS
	RA-3 Initiierung	Fernzugriffe werden ausschließlich vom Auftraggeber initiiert.	KANN
16. Notfallmanagement	BC-1 Notfallmanagementsystem	Es existiert ein Notfallmanagementsystem mit jährlichen Übungen für kritische Systeme.	KANN
	BC-2 Sicherheitsvorfallmanagement	Für Informationssicherheitsvorfälle existieren definierte Melde-, Eskalations- und Reaktionsprozesse einschließlich forensischer Sicherung und Kommunikation.	KANN
17. Security Operations Center (SOC)	SOC-1 Überwachung	Systeme werden kontinuierlich überwacht.	KANN
	SOC-2 Log-Analyse	Logdaten werden zentral erfasst und ausgewertet.	KANN
18. Informationssicherheitsmanagementsys	ISMS-1 Implementierung	Ein ISMS nach anerkanntem Standard (z. B. ISO 27001, BSI C5) ist implementiert.	KANN
	ISMS-2 Scope	Der Geltungsbereich des ISMS ist dokumentiert und relevant für die Leistungserbringung.	KANN
	ISMS-3 Zuständigkeit	Ein Informationssicherheitsbeauftragter (ISB / CISO) ist benannt.	KANN
	ISMS-4 Risikomanagement	Risiken für Verfügbarkeit, Integrität und Vertraulichkeit der für die Leistungserbringung relevanten Systeme werden regelmäßig identifiziert, bewertet und behandelt; Restrisiken werden dokumentiert. Sicherheitsmaßnahmen werden regelmäßig auf Wirksamkeit überprüft und bei Bedarf angepasst (z. B. Audits, Reviews, Kennzahlen). Sicherheitskonzepte, Prozesse und Nachweise werden dokumentiert	KANN
	ISMS-5 Wirksamkeitskontrolle, Nachweisbarkeit	und auf Anfrage bereitgestellt.	KANN
19. Rechenzentrum	RZ-1 Redundanz	Kritische Versorgungs-komponenten sind redundant ausgelegt.	MUSS
	RZ-2 Zutrittskontrolle	Zutritt wird über technische und organisatorische Maßnahmen überwacht.	MUSS
	RZ-3 Brandschutz	Es existieren geeignete Brandmelde- und Löschsysteme.	MUSS
	RZ-4 Physische Sicherheit	Die Infrastruktur bietet Schutz gegen Elementar- und Einbruchsschäden.	MUSS
	RZ-5 Zutritts-Authentisierung	Der Zutritt ist mindestens zweifaktoriell abgesichert.	KANN
	RZ-6 Geografische Redundanz	Redundante RZ-Flächen sind ausreichend geografisch getrennt und verschlüsselt vernetzt.	KANN
	RZ-7 Zutrittsmittel	Vergabe und Inventarisierung der Zutrittsmittel sind prozessual geregelt.	KANN
20. (D)DOS	DD-1 DDoS-Resilienz	Risiken durch (D)DoS-Angriffe werden technisch und organisatorisch mitgiert.	KANN