



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:	28.10.2019
Aktualisiert am:	30.04.2026
Nächste Überprüfung:	

Hinweis

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

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