Landesamt für Sicherheit in der Informationstechnik

Orientierungshilfe „IT-Sicherheit in Kliniken“

Vorgehensmodell zur Umsetzung

Stand: 12.07.2022

Version: 1.5

Landesamt für Sicherheit in der Informationstechnik, Keßlerstraße 1, 90489 Nürnberg
beratung-kritis@lsi.bayern.de, Telefon: 0911 21549-525

INHALTSVERZEICHNIS

Vorwort zum Vorgehensmodell 4

Stufe 0: Voraussetzung für den Start 6

Stufe 1: Organisatorische Maßnahmen und erste dringliche Absicherungen 7

I.1 Organisation des Informationssicherheitsmanagements 7

I.1.A Rolle des ISB 7
I.1.B Aufgaben des ISB 7
I.1.C Informationssicherheitsmanagement-Team 8
I.1.D Beziehungen des Informationssicherheitsmanagements 8

I.3 Kritische Dienstleistungen in Zusammenarbeit mit den Fachabteilungen identifizieren 8

I.4 Notfallkonzept zur Aufrechterhaltung kritischer Dienstleistungen erstellen 9

I.5 Umsetzung weiterer grundlegender Absicherungen 9

I.5.A Gegen physische Schäden absichern 9
I.5.B Zugangs- und Zutrittsrechte 10
I.5.C Administratoren 10
I.5.D Allgemeine Netzwerksicherheit 10
I.5.E Sicherer Betrieb von Clients und Server 11
I.5.F Software mit Updates und Patchmanagement sichern 11
I.5.G Accounts absichern 11
I.5.H Personal in Informationssicherheit einbinden 12

Stufe 2: Weitere wichtige Absicherungen und Richtlinien 13

II.1 Technische Vorkehrungen 13

II.1.A Backups absichern 13
II.1.B Mobile Systeme, insbesondere Bring Your Own Device (BYOD) und IoT Geräte, absichern 13
II.1.C Protokollierung einrichten 14
II.1.D Virtualisierung sicher konzipieren 14
II.1.E Fernzugriffe absichern 14
II.1.F Schwachstellenscans aus dem Internet und von intern 14
II.1.G Sicheres Basiskonfigurationskonzept erstellen und umsetzen 15
II.1.H Weitere Systemhärtung 15
II.1.I Kryptokonzept definieren und ausbauen 15
II.1.J Verwendung von Datenträgern absichern 15
II.1.K Datenschutzkonforme Löschung von Daten 15
II.1.L Cloud-Dienste 16

II.2 Informationssicherheitsvorfälle 17

II.2.A Behandlung von Informationssicherheitsvorfällen 17
II.2.B Meldung von Informationssicherheitsvorfällen ermöglichen 17
II.2.C Nachbehandlung von Informationssicherheitsvorfällen 17

II.3 Softwarefreigabe 17

II.4 Beschaffung absichern 17

II.5 Zusammenarbeit mit externen Partnern regeln 18

II.6 Aufrechterhaltung des Administrator-Qualifikationsniveaus und weitere Absicherung der Admin-Tätigkeiten 18

II.7 Organisatorische Maßnahmen 18
II.7.A Zugangs- und Zugriffsrechte regeln 18
II.7.B Datenschutzaspekte 18
II.7.C Personal noch stärker in Informationssicherheit einbinden 19
II.7.D Identifizieren und Verwalten aller Prozesse 19
II.8 Richtlinien zur Aufrechterhaltung der Sicherheit erstellen 19
Stufe 3: Gesamtabsicherung, Überprüfung und finale Dokumentation 20
III.1 Assets im Asset-Verzeichnis erfassen 20
III.2 Ausbau von Systemen zur zentralen Verwaltung und Administration 20
III.3 Externe Kooperation für Informationssicherheit aufbauen 20
III.4 Regelmäßigkeit und Aktualität sichern 20
III.5 Umfassende Dokumentation 21
Stufe 4: Auditierung und Zertifizierung 22

Vorwort zum Vorgehensmodell

Im Folgenden finden Sie ein **Vorgehensmodell** für eine zeitliche Reihenfolge zur Umsetzung empfohlener Informationssicherheitsmaßnahmen.

Eher ungewöhnlich wäre es, wenn in Ihrer Klinik nicht schon bereits technische, organisatorische und einzelne punktuelle Awareness-Maßnahmen umgesetzt worden sind. Vielleicht wurden auch schon eine Leitlinie und erste Richtlinien verfasst und an die Mitarbeiter kommuniziert.

Falls Sie einzelne Punkte bereits umgesetzt haben, können Sie die folgende Anleitung verwenden, um noch einmal zu überprüfen, ob Sie an mancher Stelle die vorgeschlagenen Maßnahmen verstärken und erweitern wollen.

Identifizieren Sie als erstes die aktuell relevanten Bedrohungen für die Sicherheit Ihrer Klinik und priorisieren Sie diese für die in der Folge zu treffenden Maßnahmen. Je nachdem, welche Maßnahmen in der Klinik bereits getroffen wurden, kann die Liste der aktuell relevanten Bedrohungen für Sie bzw. Ihr Sicherheitsmanagement-Team und Ihre Klinikleitung unterschiedlich aussehen.

Bitte stellen Sie hier die für Ihre Klinik aktuell relevanten Bedrohungen/Gefährdungen zusammen (dies können z.B. auch eine veraltete Firewall, teilweise veraltete Serversysteme, ungenügendes Backup, Nutzerverhalten etc. sein):

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____

Bitte nutzen Sie dieses Vorgehensmodell und ebenso den Fragenkatalog, um die von Ihnen identifizierten aktuell relevanten Bedrohungen/Gefährdungen durch angemessene Gegenmaßnahmen zu adressieren, d.h. um einen für Sie spezifischen Maßnahmenplan zu entwickeln. Der Fragenkatalog ist in 34 Handlungsfelder gegliedert. Der fünfstufige Aufbau des Vorgehensmodells orientiert sich an der Kritikalität der Gefährdungen und schlägt daher eine zeitliche Reihenfolge vor.

Sobald Sie Konsens zu den für Ihre Klinik aktuell relevanten Bedrohungen/Gefährdungen erzielt haben, gilt es die Klinikleitung für den weiteren systematischen Auf- und Ausbau der Informationssicherheit zu gewinnen.

Hinweis 1: Im folgenden Dokument werden in Anlehnung an RFC 2119 die Schlüsselwörter MUSS, SOLL und KANN verwendet, um die unterschiedlichen Anforderungslevel zu kennzeichnen. Dies kann Ihnen als Orientierung für Ihre eigene Einschätzung der Wichtigkeit der genannten Punkte für die Aufrechterhaltung der Informationssicherheit dienen.

MUSS: Die Erfüllung der Anforderung ist aus Sicht des LSI zwingend erforderlich, um die Schutzziele für Krankenhäuser zu erreichen.

SOLL: Die Einhaltung der Anforderung ist grundsätzlich erforderlich. Sofern durch die Nicht-Umsetzung die Informationssicherheit nicht gefährdet wird, kann auf die Umsetzung verzichtet werden. Das LSI empfiehlt, dass

Sie die Nicht-Umsetzung auf jeden Fall dokumentieren, der Klinikleitung zur Kenntnis und zur Genehmigung bringen und deren Entscheidung darüber ebenfalls dokumentieren.

KANN: Die Einhaltung der Anforderung wird vom LSI empfohlen.

Hinweis 2: Im folgenden Dokument referenzieren die Zahlen am rechten Rand jeweils auf die zugehörigen Fragen im Fragenkatalog. Bei einigen der genannten Maßnahmen wird jeweils auf mehrere Fragen verwiesen. Sie finden die Fragen sowie die dazugehörigen Beschreibungen im Fragenkatalog.

Hinweis 3: Bei Bedarf finden Sie einzelne Fachbegriffe im Glossar des Fragenkatalogs erläutert.

Hinweis 4: Diese Orientierungshilfe ist eine Vorstufe zu einer Zertifizierung. Für die Auditierung bzw. Zertifizierung wird von Ihnen ein ISMS-Standard (z.B. B3S, IEC/ISO 2700x, IT-Grundschutz) ausgewählt, nach dem diese interne oder externe Auditierung bzw. Zertifizierung stattfinden kann. Dazu sind noch weitere, über diese Orientierungshilfe hinausgehende, spezifische von diesem Standard geforderte Vorbereitungen, Richtlinien und Maßnahmen umzusetzen.

Stufe 0: Voraussetzung für den Start

Bevor mit dem systematischen Auf- und Ausbau der Informationssicherheit begonnen werden kann, MUSS die tatsächliche Unterstützung der Klinikleitung sichergestellt werden. Dies ist ein beständiger, haus- und fachbereichsübergreifender Prozess und kein isoliertes, einmaliges Projekt. Insbesondere die Unterstützung von kaufmännischer wie auch medizinischer Geschäftsführung ist hier maßgeblich.

Hierfür MUSS die Klinikleitung:

☐	die Gesamtverantwortung für die Informationssicherheit, den Informationssicherheitsmanagementprozess und die kontinuierliche Weiterentwicklung der Informationssicherheit übernehmen,	1.1a
☐	die Informationssicherheitsziele glaubhaft nach außen vermitteln,	1.1b
☐	die Verantwortung für die Umsetzung der Informationssicherheitsziele übernehmen,	
☐	die zur Verbesserung der Informationssicherheit benötigten Ressourcen zur Verfügung stellen,	1.1c
☐	den Informationssicherheitsprozess aktiv unterstützen.	

Stufe 1: Organisatorische Maßnahmen und erste dringliche Absicherungen

Sie können erst mit Stufe 1 zum systematischen Auf- und Ausbau der Informationssicherheit beginnen, sobald Sie die Stufe 0 möglichst vollständig umgesetzt haben. Die Orientierungshilfe unterstützt Sie dabei.

Vorhandene und zukünftige potentielle Bedrohungen der Informationssicherheit können im schlimmsten Fall die Sicherheit von Patienten bei Aufnahme, Diagnose, Therapie, Unterbringung/Pflege oder Entlassung gefährden und/oder zu einer falschen oder ungenügenden Behandlung mit all ihren möglichen Folgen führen.

Der Informationssicherheitsbeauftragte (ISB) MUSS die Klinikleitung über diese aktuell relevanten Bedrohungen/Gefährdungen informieren.

Wir empfehlen, den Bericht an die Klinikleitung so vorzubereiteten, dass ein Maßnahmen-Umsetzungsplan inkl. der dafür benötigten Ressourcen gleich mit kommuniziert wird. In Situationen, in denen evtl. Gefahr in Verzug ist, MUSS sogleich die Klinikleitung darüber in Kenntnis gesetzt werden. Es SOLL dokumentiert werden, wann und zu welchen Inhalten die Klinikleitung informiert wurde und welche Entscheidungen diese dazu getroffen hat.

Falls keine unmittelbaren Gefahren drohen, KANN zunächst das Handlungsfeld „Informationssicherheit" weiter analysiert, strukturiert und systematisiert werden.

I.1 Organisation des Informationssicherheitsmanagements

Mit der Unterstützung der Leitung MUSS nun das Informationssicherheitsmanagement (ISM) so organisiert werden, dass es handlungsfähig wird. Insbesondere MUSS der ISB mit ausreichenden Kompetenzen und Ressourcen ausgestattet werden.

I.1.A Rolle des ISB

Zunächst MUSS die Klinikleitung einen ISB mit klar definierter Rolle ernennen:

☐	Verantwortlichen für die Umsetzung eines ISMS ernennen und eindeutige Verantwortlichkeiten zuweisen	1.1h 2.5a
☐	ISB im Haushalt und im Stellenplan angemessene Ressourcen für die ISB-Aufgaben und eine den Anforderungen entsprechende Fortbildung und kontinuierliche Weiterbildungen zur Verfügung stellen,	2.4b 2.1e 2.2a
☐	Festlegen und Bekanntgeben von Aufgaben, Rechten und Pflichten des ISB, dabei Interessenkonflikte in den Aufgaben des ISB vermeiden.	2.1a 2.3a 2.1f

I.1.B Aufgaben des ISB

Der ISB MUSS die oben definierten Aufgaben erfüllen:

☐	Erfahrung und Wissen auf den Gebieten der Informationssicherheit und IT mitbringen,	2.2b
☐	Konzepte entwickeln und das Sicherheitsmanagement koordinieren,	2.3b
☐	als Ansprechpartner in Fragen der Informationssicherheit fungieren,	2.6a
☐	direkt an die Klinikleitung berichten.	2.1b

I.1.C Informationssicherheitsmanagement-Team

Zur Unterstützung des ISB MUSS ein ISM-Team gebildet werden. So MUSS die Klinikleitung:

- ☐ ein eindeutiges Informationssicherheitsmanagement-Teams (ISM-Team) zur Unterstützung des ISB benennen. 1.1i 2.4d

I.1.D Beziehungen des Informationssicherheitsmanagements

Die Beziehungen des Informationssicherheitsmanagements (ISM) zu anderen Bereichen MÜSSEN klar geregelt sein:

- ☐ Ausreichende Zusammenarbeit von ISB, Klinikleitung (Verantwortliche für IT und kaufmännischer Bereich), IT-Leitung, Fachabteilungen (u.a. Ärztliche Leitung, Medizintechnik, Betriebstechnik, Pflegedienstleitung), Datenschutzbeauftragten und Betriebsrat sicherstellen, 2.4c
- ☐ Zuständigkeiten und Kompetenzen für Informationssicherheit in den Organisationsstrukturen klar definieren und zuweisen, 4.4b
- ☐ alle Ziele des ISM mit der Klinikleitung abstimmen, 2.1c
- ☐ den ISB ausreichend an allen sicherheitsrelevanten Entscheidungen beteiligen, 4.4c
- ☐ die Verantwortlichen für die IT, das ISM und insbesondere den ISB in die für die Informationssicherheit relevanten Prozesse und bei der Projektplanung einbinden, 2.1d 4.4a 2.4a
- ☐ den Datenschutzbeauftragen in alle Informationssicherheitsprozesse einbinden. 3.2a

I.2 Leitlinie

- ☐ Die Klinikleitung MUSS eine Leitlinie zur Informationssicherheit verabschieden. 1.1d
- ☐ Die Informationssicherheitsleitlinie enthält:
  - ☐ Stellenwert der Informationssicherheit, 1.1e
  - ☐ Geltungsbereich der Informationssicherheitsleitlinie, 1.1f
  - ☐ Regelung für die kontinuierliche Verbesserung der Informationssicherheit. 1.2a
- ☐ Die Leitlinie ist allen Mitarbeitern der Klinik schriftlich (z.B. über Mail, online) bekannt zu machen. 1.1g
- ☐ Die Klinikleitung ist für die fortlaufende Kontrolle zur Wirksamkeit und Zielerreichung des Informationssicherheitsmanagements verantwortlich. 1.2b

I.3 Kritische Dienstleistungen in Zusammenarbeit mit den Fachabteilungen identifizieren

Um kritische Dienstleistungen absichern zu können, MÜSSEN diese zuerst identifiziert werden, dies kann man auch als Beginn des IT-Risikomanagements ansehen.

IT-Risikomanagement starten: 5.1a

- ☐ Alle kritischen Dienstleistungen definieren und dokumentieren, 5.1b
- ☐ IT-Systeme und deren Nutzung dokumentieren sowie diese Dokumentation nutzen, aktualisieren und kommunizieren, 5.1c
- ☐ Risikobehandlungsplan regelmäßig überprüfen und aktualisieren, 5.1d
- ☐ für die Erbringung kritischer Dienstleistungen nötige Assets und deren Abhängigkeiten ermitteln und als Informationsverbund dokumentieren. 9.1a 9.1b 9.5a

I.4 Notfallkonzept zur Aufrechterhaltung kritischer Dienstleistungen erstellen

Für die ermittelten kritischen Dienstleistungen MUSS ein Konzept entwickelt werden, um diese im Notfall weiter betreiben zu können.

☐	Zur Aufrechterhaltung kritischer Dienstleistungen benötigte Personen im Notfallplan erfassen und über Vertretungsregelungen redundant auslegen,	6.1b
☐	direkt oder indirekt für kritische Dienstleistungen notwendige IT-Systeme und IT-Infrastruktur-Komponenten angemessen redundant auslegen mit dem Ziel, einen weitgehend unterbrechungsfreien Betrieb zu gewährleisten,	11.4a 11.4b 11.4d
☐	Weiterbetrieb kritischer Systeme bei Netz-/Kommunikationsstörung soweit wie möglich sicherstellen,	28.1b
☐	für wichtige IT-Systeme und Komponenten angemessene organisatorische und technische rechtskonforme Ersatzverfahren einrichten,	11.4c
☐	Ersatzverfahren für einen IT-Ausfall etablieren und bekannt geben,	6.3a
☐	Im Notfallkonzept vorsehen, dass ausgelagerte Systeme sowie Cloud-Dienste ausfallen können und Ersatzverfahren für diese einrichten und regelmäßig testen,	17.3a, 17.A.9a, 17.A.9c
☐	Notfallpläne mit organisatorischen, technischen und papierbasierten Ersatzlösungen und -verfahren für alle kritischen Dienstleistungen mit hohem Schadenspotenzial erstellen,	6.1a
☐	Maßnahmen treffen, um für kritische Dienstleistungen relevante IT-Systeme und Medizingeräte vor Ausfällen externer Versorgungsdienste zu schützen,	11.1a
☐	dabei auch sicherstellen, dass in diesem Fall die Umgebungsanforderungen der Geräte weiterhin eingehalten werden,	11.2a
☐	regelmäßig mehrstufige Datensicherungen durchführen,	29.1b
☐	ein Krisenmanagement-Team benennen und einen Krisenmanagement-Plan erstellen,	6.1d
☐	Kommunikationswege für den IT-Notfall einrichten,	6.2a
☐	Alarmierungsplan für IT-Notfälle erstellen und allen Beteiligten bekanntgeben,	6.2b
☐	allen Beteiligten Zugriff auf Alarmierungs- und Notfallpläne ermöglichen,	6.1c, 17.A.9b
☐	Wiederanlaufpläne für alle kritischen Dienstleistungen mit hohem Schadenspotenzial erstellen und bekanntgeben.	7.1a

I.5 Umsetzung weiterer grundlegender Absicherungen

Mit dem Aufbau des IT-Notfallmanagements wurde die zunächst dringendste Vorsorge getroffen. Implizit wurden dabei bereits Risiken bewertet. Falls gewünscht, KANN jetzt in ein systematisiertes IT-Risikomanagement eingestiegen werden. Der Vorgehensplan selbst enthält keine Anleitung dazu.

Anhand der von Ihnen im Vorwort des Vorgehensmodells erstellten Gefährdungsliste entscheidet der ISB, welche ersten geeigneten Maßnahmen dagegen getroffen werden. Dabei MUSS darauf geachtet werden, dass bestimmte technische Maßnahmen eine sorgfältige vorherige Dokumentation (falls noch nicht geschehen) als Voraussetzung haben können.

I.5.A Gegen physische Schäden absichern

Es MÜSSEN physische Schäden an (insbesondere kritischen) IT-Systemen verhindert werden: 10.1a

☐	Brandschutzkonzept für Serverraum erstellen,	10.1b

- ☐ wenn mehrere Serverräume: Betrieb in unterschiedlichen Gebäuden bzw. Brandabschnitten, 10.1c
- ☐ Serverraum mit unterbrechungsfreier Stromversorgung (USV) und Überspannungsschutz ausstatten, 10.1d
- ☐ Serverraum ausreichend klimatisieren, 10.1e
- ☐ sicherstellen, dass Raumlage unkritisch ist bzw. Schutzmaßnahmen umsetzen, 10.1h
- ☐ wenn möglich keine Versorgungsleitungen durch Serverraum verlaufen lassen bzw. Schutzmaßnahmen umsetzen, 10.1f
- ☐ weitere strukturelle Sicherungsmaßnahmen vornehmen, 10.1g
- ☐ Raumzonenkonzept festlegen, dokumentieren und dabei Risiken einheitlich behandeln und mittels Sicherheitsmaßnahmen reduzieren, 10.3a
- ☐ Maßnahmen treffen, um Beeinträchtigung durch Wechselwirkungen zwischen Systemen und Infrastruktur-/Versorgungseinrichtungen zu vermeiden. 11.3a

I.5.B Zugangs- und Zutrittsrechte

Es MUSS der Zugriff auf IT-Infrastruktur und -Systeme und der Zugang zu schutzbedürftigen Räumen (siehe Raumzonenkonzept) abgesichert werden:

- ☐ Zutrittsrechte zu schutzbedürftigen Räumen, die im Rahmen ihrer Funktion an Personen vergeben werden, regeln und dokumentieren, 10.2a
- ☐ IT-Infrastruktur vor unbefugtem Zutritt und Manipulation schützen, 10.2b
- ☐ Zugang zu IT-Systemen in öffentlich zugänglichen Bereichen schützen, 10.4a
- ☐ Rollen- und Berechtigungskonzept nach dem Minimalprinzip erstellen, 24.1a
- ☐ Rechte nach Minimalprinzip vergeben und regelmäßig überprüfen, 24.1b
- ☐ Daten, Dienste und Programmfunktionalitäten auf Mindestmaß beschränken, 24.1c
- ☐ Rechtevergabe dokumentieren. 24.1d

I.5.C Administratoren

Für die Umsetzung weiterer Absicherungen werden qualifizierte Administratoren mit entsprechenden Ressourcen benötigt:

- ☐ Aufgaben der einzelnen Administratoren klar definieren, 14.2a
- ☐ Qualifikation der Administratoren sicherstellen, 14.1a
- ☐ Administratoren ausreichend Ressourcen zur Verfügung stellen, 14.1b
- ☐ Administratorenteams redundant aufstellen, 14.4b
- ☐ Vertretung der Administratoren festlegen und dokumentieren, 14.4a
- ☐ Zugangsdaten für Administratoren entsprechend sichern, 14.4c
- ☐ Zugriff und Passwörter unbedingt ändern und dokumentieren, falls ein Administrator ausscheidet. 14.5a

I.5.D Allgemeine Netzwerksicherheit

Maßnahmen zur allgemeinen Absicherung des Netzwerks MÜSSEN ergriffen werden:

- ☐ aktuellen IT-Netzstrukturplan für Organisation inkl. Außenstellen erstellen, 19.1a
- ☐ Außenstellen (falls vorhanden) sicher anbinden, 19.2a
- ☐ IT-Netzwerk gemäß der Risikobewertung in verschiedene Schutzzonen segmentieren und entsprechend des Schutzbedarfes absichern, z.B.: 19.3a 19.3b
  - ☐ Verwaltungs-Netz, 28.1a
  - ☐ Server-Netz,
  - ☐ Medizintechnik-Netz,
  - ☐ DMZ,
  - ☐ Client-Netz,

- ☐ VoIP,
- ☐ Gäste-Netz.

☐	Sicher konfigurierte Sicherheitsgateways (u.a. Firewall, IDS/IPS) auf Stand der Technik verwenden.	19.3c, 23.1a
☐	kritische IT-Netzbereiche soweit möglich physikalisch vom restlichen Netz trennen; falls nicht möglich, diese logisch trennen und die Kommunikation zwischen Netzbereichen unterschiedlicher Kritikalität gemäß Risikobewertung gezielt steuern	19.3d
☐	ein NAC-Konzept erstellen,	19.4a
☐	für das NAC sichere Authentifizierungsstandards (nach aktuellem Stand der Technik) verwenden,	19.4b
☐	über das NAC die Sicherheitsanforderungen an die Endgeräte für einen Netzwerkzugang richtlinienkonform umsetzen,	19.4c
☐	die NAC-Ereignisse protokollieren und auswerten,	19.4d
☐	die zentralen NAC-Komponenten hochverfügbar (redundant) vorhalten,	19.4e
☐	aktuelle Sperrlisten und Regeln für Firewall, IDS, IPS und Webproxy verwenden,	23.1b 23.2a
☐	sicheres Verschlüsselungsverfahren für interne WLANs auf Stand der Technik verwenden.	26.1c

I.5.E Sicherer Betrieb von Clients und Server

Maßnahmen zum Schutz vor Schadsoftware MÜSSEN ergriffen werden:

☐	System zur Vorbeugung und Erkennung von verdächtiger und schädlicher Software einrichten,	22.3a
☐	geeignete Endpoint-Protection installieren,	22.3b
☐	Endpoint-Protection zentral administrieren, prüfen und updaten,	22.3c
☐	zentrale Schutzmechanismen (z.B. Sandboxing) für Spam- und Phishing-Mails einrichten,	22.3d
☐	Mails im Mail-Clientprogramm zunächst nur in reinem Text-Format anzeigen lassen,	22.3e
☐	Technische Maßnahmen ergreifen, um die Sicherheit exponierter Server zu gewährleisten.	22.5a

I.5.F Software mit Updates und Patchmanagement sichern

Verwendete Software MUSS mittels Updates und einem geeigneten Patchmanagement abgesichert werden:

☐	Nur freigegebene Software installieren und verwenden,	22.1a 34.1b
☐	Updates nach Test regelmäßig und schnell durchführen,	22.2a
☐	Firmwareupdates regelmäßig durchführen, sobald diese getestet wurden,	22.2c
☐	Regelung für Updates bei eingesetzter Hardware erstellen,	22.2b
☐	Konzept für Patch- und Änderungsmanagement erstellen,	30.1a
☐	Pläne für Roll-Back vor der Durchführung von Systemänderungen erstellen,	30.1b
☐	Soft- und Hardware für kritische Dienstleistungen in Freigabeprozess testen,	30.1c
☐	Maßnahmen ergreifen, um Authentizität eingesetzter Software sicherzustellen.	34.1a

I.5.G Accounts absichern

Die Sicherheit aller Accounts MUSS gewährleistet werden (Minimalprinzip der Rechte):

☐	Prozess für Vergabe von Authentifizierungsdaten erstellen,	25.1a

☐	Übermittlung temporärer Authentifizierungsdaten regeln,	25.1b
☐	Kennwortänderung nach Erstanmeldung erzwingen,	25.1c
☐	Authentifizierungsverfahren auswählen, die angemessene Zugriffssicherheit bieten,	25.2a
☐	Nutzer zur Geheimhaltung ihrer Authentifizierungsdaten verpflichten,	25.3a
☐	Identität bei Zurücksetzung der Authentifizierungsdaten sicherstellen,	25.3b
☐	Nutzer nach angemessenem Inaktivitätszeitraum automatisch ausloggen,	25.3c
☐	Accounts nach mehreren lokalen Login-Fehlversuchen sperren,	25.3d 25.3e
☐	Accounts ausgeschiedener Mitarbeiter zeitnah sperren.	24.3c

I.5.H Personal in Informationssicherheit einbinden

Sämtliches Personal MUSS in die Informationssicherheit mit einbezogen werden.
Dafür MUSS ein Schulungs- und Sensibilisierungskonzept erstellt werden:

☐	Klinikleitung MUSS deutlich machen, dass sie die Schulungen unterstützt,	13.3c
☐	regelmäßige Schulungs- und Sensibilisierungsmaßnahmen gemäß Konzept durchführen,	13.3b
☐	alle Beschäftigten vor Arbeitsaufnahme zur Informationssicherheit unterrichten,	13.2a
☐	auch Klinikleitung schulen,	13.3d
☐	Mitarbeiter MÜSSEN Rahmenbedingungen zu Informationssicherheit und Datenschutz einhalten und Verstöße melden.	13.1a

Stufe 2: Weitere wichtige Absicherungen und Richtlinien

Sie können erst mit Stufe 2 beginnen, sobald Sie die Stufen 0 und 1 möglichst vollständig umgesetzt haben.

Nachdem auf Stufe 1 bereits erste dringliche Maßnahmen umgesetzt wurden, MÜSSEN nun weitere Absicherungen für kleinere, und dennoch wichtige Teilbereiche umgesetzt werden.

Die im folgenden genannten Maßnahmen können parallel bearbeitet werden und bauen nicht zwingend aufeinander auf. Bei Auswahl der Maßnahmenreihenfolge KANN gegebenenfalls die aktualisierte Gefährdungsliste herangezogen werden.

Gegen die von Ihnen eingangs ermittelten Gefährdungen haben Sie wahrscheinlich in Stufe 1 bereits Abwehrmaßnahmen treffen können. Falls trotz der bisher getroffenen Maßnahmen weiterhin Gefährdungen vorhanden sein sollten, so können diese hier nochmals notiert werden. Die Liste KANN verwendet werden, um damit eine Priorisierung geeigneter Stufe 2 - Maßnahmen vorzunehmen:

1. _____

2. _____

3. _____

4. _____

5. _____

6. _____

II.1 Technische Vorkehrungen

Mit weiteren technischen Vorkehrungen MÜSSEN die dringlichen Absicherungen weiter gestützt werden, um die Sicherheit deutlich zu verbessern.

II.1.A Backups absichern

☐	Datensicherungskonzept, in dem Sicherungsverfahren, Zyklus und Verantwortlichkeiten geregelt sind, erstellen,	29.1a
☐	Vertraulichkeit von Backups sicherstellen,	29.4a
☐	Gesundheitsdaten verschlüsselt sichern und die Zugriffrechte dafür regeln,	29.4b
☐	Zugriff auf die Backups nur während Sicherung und Rücksicherung zulassen,	29.2a
☐	Backups physisch sicher lagern,	29.3a
☐	Funktionsfähigkeit der Backups regelmäßig in Recovery-Tests prüfen,	29.5a
☐	sicherstellen, wie noch benötigte Patientendaten vor Außerbetriebnahme bzw. Wechsel von Systemen geeignet gesichert werden,	29.1c
☐	datenschutzkonformes, revisionssicheres Langzeitarchiv aufbauen,	29.3b
☐	bei der Nutzung von Cloud sicherstellen, dass der Dienstanbieter regelmäßig, wie im Vertrag gefordert, ein Backup erstellt	17.A.11a
☐	und zusätzlich zu diesem ein separates, eigenes Backup erstellen.	17.A.11b

II.1.B Mobile Systeme, insbesondere Bring Your Own Device (BYOD), und IoT-Geräte absichern

☐	BYOD nur in Ausnahmefällen zulassen,	27.3a
☐	Freigabeprozess für mobile Geräte und Telearbeitsplätze einrichten,	27.1d
☐	mobile Systeme/Geräte absichern	27.2a 27.4b

☐	zugelassene BYOD-Geräte auf Einhaltung der Sicherheitsvorgaben prüfen,	27.3b
☐	dienstliche Daten und Anwendungen auf BYOD-Geräten in einem eigenen Container betreiben	27.3c
☐	ein Konzept zur Beschaffung, Inbetriebnahme, Betrieb und Außerbetriebnahme von IoT-Geräten,	27.5a
☐	den Zugriff von IoT-Geräten auf das interne Netz nach dem Minimalprinzip konfigurieren.	27.5b

II.1.C Protokollierung einrichten

☐	Protokollierungs- und Analysekonzept erstellen,	31.1a 31.1b
☐	Einhaltung des Datenschutzes und Einbindung des Betriebsrats bei Protokollierung sicherstellen	31.1c
☐	die Möglichkeiten zum Logging und zur Überwachung von kritischen IT-Systemen sinnvoll und ausreichend detailliert nutzen	31.4a
☐	Zugriff auf Gesundheitsdaten soweit möglich protokollieren und überwachen,	24.1e
☐	eine einheitliche Referenzzeitquelle (Atomzeitserver) für alle relevanten Informationssysteme einrichten,	31.2b
☐	Protokollierungsinfrastruktur ausreichend dimensionieren,	31.2a
☐	Protokolldaten vor Manipulation schützen,	31.5a
☐	sicherstellen, dass nur autorisierte Mitarbeiter Zugriff auf die protokollierten Daten haben,	31.5b
☐	Störungen wie ausbleibende Protokollierungsdaten, kritische Betriebssystemereignisse, außergewöhnliche Lastsituationen etc. automatisiert an verantwortliche Personen melden,	31.3a 31.3b
☐	Verfahren zur Beweissicherung etablieren,	31.4b
☐	Löschkonzept für Protokolldaten erstellen.	31.5c

II.1.D Virtualisierung sicher konzipieren

	Virtualisierungsserver und VMs ausreichend groß dimensionieren und eine redundante Auslegung sicherstellen,	19.4a
	für ausreichende Isolation der VMs sorgen,	19.4b
	Virtualisierung in Sicherheitsmechanismen berücksichtigen,	19.4c
	nur notwendige Dienste auf dem Virtualisierungsserver betreiben,	19.4d
	die Virtualisierungsumgebung redundant konzipieren.	19.4e

II.1.E Fernzugriffe absichern

☐	Fernzugriff via VPN sicher konzipieren und dokumentieren,	20.1a
☐	Fernzugriffe nach Minimalprinzip beschränken,	20.1b
☐	Systeme für Fernzugriffnutzung segmentieren und beschränken,	20.2a
☐	Fernwartungszugriffe immer aus dem Krankenhaus initiieren, sichern und wieder trennen,	20.3a
☐	Fernzugriffe von Administratoren durch geeignete Authentifizierungsmechanismen besonders sichern.	20.4a

II.1.F Schwachstellenscans aus dem Internet und von intern

☐	IT-Infrastruktur mit Schwachstellenscans aus dem Internet prüfen,	23.3a
☐	Regelmäßige und anlassbezogene, netzinterne Schwachstellenscans auf netzgebundene Systeme planen und umsetzen, wo dies möglich ist ohne die Patientensicherheit und ggfs. die Betriebssicherheit zu gefährden	23.3b

II.1.G Sicheres Basiskonfigurationskonzept erstellen und umsetzen

- ☐ Basiskonfiguration der Systeme und Maßnahmen zur Systemhärtung konzipieren, 21.1a
- ☐ bei Softwareauswahl nach Minimalprinzip arbeiten, 21.2a
- ☐ Boot-Vorgang einheitlich und sicher konfigurieren. 21.3a

II.1.H Weitere Systemhärtung

Die Endgeräte MÜSSEN weiter gehärtet werden. Mindestmaßnahmen hierfür sind:

- ☐ Ungenutzte Systeme entfernen und nicht benötigte Software deinstallieren lassen, 21.2b
- ☐ Ausführung von Makros und OLE-Objekten auf allen IT-Systemen blocken lassen, 21.4a
- ☐ nur signierte und/oder geprüfte Makros freigeben, 21.4b
- ☐ Windows Skript Host deaktivieren, 21.5a
- ☐ automatische Ausführung von fremden Programmen verhindern, 21.6a
- ☐ PowerShell-Rechte maximal einschränken, 21.7a
- ☐ Schnittstellen für Massenspeicher schützen, 22.3f
- ☐ Minimalprinzip für Anwendungen auf allen kritischen IT-Systemen und medizinischen Geräten umsetzen. 22.4b

II.1.I Kryptokonzept definieren und ausbauen

- ☐ Lokale Datenträger verschlüsseln, 26.1a
- ☐ sensible Daten verschlüsseln und signieren, 26.1b
- ☐ Zugriff auf Webserver nur über https mit sicherer Verschlüsselung zulassen, 26.1d
- ☐ sichere E-Mail-Kommunikation gewährleisten. 26.1e
- ☐ Verwendung eines sicheren Schlüsselmanagements 26.1f

II.1.J Verwendung von Datenträgern absichern

- ☐ Informationssicherheitsprüfung von Datenträgern nach externer Verwendung durchführen, 32.3a
- ☐ sicherstellen, dass Datenträger mit sensiblen Daten für Transport verschlüsselt sind, 32.2a
- ☐ benannte Personen/Kurierdienste für sicheren Umgang mit mobilen Datenträgern und auf entsprechende Gefahren hin schulen, 32.2b
- ☐ Sicherheitsüberprüfungsverfahren für Massenspeicher einrichten, bevor diese genutzt werden incl. genutzter Installationsmedien (auch von Dienstdienstleistern) 22.3g

II.1.K Datenschutzkonforme Löschung von Daten

Die Vorgehensweise bei der Löschung von Daten MUSS geregelt werden:

- ☐ Eine Anleitung zur Datenvernichtung erstellen, 33.1a
- ☐ Verantwortliche für Datenvernichtung benennen, 33.1b
- ☐ sicherstellen, dass von ausgesonderten Datenträgern keine schützenswerten Daten mehr gelesen und rekonstruiert werden können, 33.2a
- ☐ nicht mehr benötigte Inhalte von wiederverwendbaren Datenträgern sicher löschen, 33.2b
- ☐ verhindern, dass bei der Reparatur von Systemen sensible Daten von Externen ausgelesen oder rekonstruiert werden können, 33.2c
- ☐ Löschung von sensiblen Daten protokollieren. 33.2d

II.1.L Cloud-Dienste

☐	Strategie für die Cloud-Nutzung erstellen und eine rechtliche Machbarkeitsstudie oder Vergleichbares durchführen,	17.A.1a, 17.A.1d
☐	alle genutzten Cloud-Dienste dokumentieren,	17.A.1b
☐	eine Risikoanalyse vor der Einführung eines Cloud-Dienstes einführen,	17.A.1c
☐	bei der Auswahl des Dienstleisters auf den Sitz des Dienstleisters achten,	17.A.2b
☐	sicherstellen, dass für alle Cloud-Dienste die relevanten Schnittstellen und Verantwortlichkeiten eindeutig abgegrenzt sind,	17.A.3a
☐	Migrationskonzept für die Einführung eines Cloud-Dienstes erstellen und die (Rück-)Migration regelmäßig nach der Einführung testen,	17.A.4a
☐	ein Sicherheitskonzept für die Cloud-Nutzung erstellen, dieses regelmäßig prüfen und aktualisieren,	17.A.5a, 17.A.5b
☐	bei der Auswahl eines Cloud-Dienstanbieter verschiedene Anbieter und Umsetzungsmöglichkeiten vergleichen, die Zertifikate beachten und eine Anforderungsprofil erstellen, welches bei der Auswahl des Dienstleisters zu beachten ist,	17.A.6a, 17.A.6b, 17.A.6c, 17.A.6d
☐	einen schriftlichen Vertrag, welcher alle relevanten und wichtigen Anforderungen regelt, erstellen und die Vertragsgestaltung auf Rechtsgültigkeit überprüfen,	17.A.7a, 17.A.7b
☐	vor der Inbetriebnahme des Cloud-Dienstes einen Testlauf durchführen und prüfen, ob alle vertraglich vereinbarten Anforderungen an den Cloud-Dienst erfüllt werden,	17.A.8a, 17.A.8b
☐	Konzept erstellen für die Beendigung des Vertragsverhältnisses bzw. dem Wechsel zu einem anderen Anbieter,	17.A.10a
☐	die vertraglich festgelegten Regelungen regelmäßig prüfen,	17.A.12a
☐	die Zugriffe der Cloud ins interne Netz auf das Nötigste beschränken und diese überwachen,	17.A.12b
☐	Rollen und Rechte für die Cloud-Dienste regelmäßig prüfen.	17.A.3b

II.2 Informationssicherheitsvorfälle

Informationssicherheitsvorfällen MUSS unter Berücksichtigung der Versorgungsnotwendigkeiten in einem Krankenhaus (Patientensicherheit und Behandlungseffizienz) höchste Priorität eingeräumt werden, um die Informationssicherheit sowie den ordnungsgemäßen IT-Betrieb wieder zu gewährleisten und ähnliche Vorfälle in Zukunft zu vermeiden.

II.2.A Behandlung von Informationssicherheitsvorfällen

☐	Verfahren zur Beobachtung, Identifikation, Analyse und Beurteilung von Informationssicherheitsvorfällen sowie die Eskalationskriterien festlegen,	8.1a
☐	Kriterien und Entscheidungsprozesse definieren, um zu erkennen, ob es sich um einen Informationssicherheitsvorfall handelt,	8.2a
☐	durchzuführende Maßnahmen bei einem Informationssicherheitsvorfall priorisieren,	8.1b
☐	Verfahren zur Wiederherstellung der Integrität nach einem Informationssicherheitsvorfall bereits präventiv implementieren und testen.	8.4a

II.2.B Meldung von Informationssicherheitsvorfällen ermöglichen

☐	Meldeketten etablieren,	15.1b
☐	Berichterstattung an Klinikleitung sicherstellen,	8.1e
☐	Informationssicherheitsvorfälle an definierte Mitarbeiter melden,	15.1a
☐	den Informierten Rückmeldung ermöglichen,	15.1c
☐	Informationsweitergabe über Informationssicherheitsvorfälle an betroffene Personen und öffentliche Stellen (im Rahmen von Meldepflichten) einführen,	8.1d
☐	Plan mit Priorisierung der Meldewege und darauffolgender Maßnahmen verteilen.	8.2b

II.2.C Nachbehandlung von Informationssicherheitsvorfällen

☐	Prozess zur Nachverfolgung der Behandlung von Informationssicherheitsvorfällen etablieren,	8.3a
☐	Im Rahmen von Informationssicherheitsvorfällen erkannte Schwachstellen zeitnah beheben,	8.4c
☐	prüfen, wie sich ähnliche Vorfälle nach Informationssicherheitsvorfällen in Zukunft vermeiden lassen.	8.4b

II.3 Softwarefreigabe

☐	Regeln für den Einsatz von Anwendungen/Apps aufstellen,	34.1d
☐	Freigabeverfahren für einzuführende Produkte abstimmen,	34.1c
☐	Verantwortlichen für Software-/App-Freigabe benennen,	34.1e
☐	Tests ausschließlich auf isolierten Testsystemen und -umgebungen durchführen,	34.2a
☐	Abhängigkeiten von Betriebssystem/Plattform in Freigabeprozess prüfen.	30.3a

II.4 Beschaffung absichern

☐	Beim Beschaffungsprozess Belange der Informationssicherheit aufnehmen,	12.1a
☐	bei der Projektplanung Sicherheitsaspekte berücksichtigen,	12.1b

☐	bei Beschaffung von netzwerkfähigen Systemen die eigenen Anforderungen an die IT-Sicherheit im Vorfeld definieren, dokumentieren und im Beschaffungsprozess einfordern,	12.1c
☐	Herstellerinformationen zur IT-Sicherheit einholen,	12.1e
☐	die zu beschaffende bzw. neue Soft- und Hardware in Testumgebung testen,	12.2a
☐	prüfen, inwieweit Unterstützung beim Einbinden von Geräten in die Netzumgebung in Anspruch genommen werden soll,	12.1f
☐	Rücksichtnahme auf Sicherheitsbelange beim Einbinden der Geräte,	12.1g
☐	physikalische Störeinflüsse überprüfen.	12.1h

II.5 Zusammenarbeit mit externen Partnern regeln

☐	Sicherheitsniveau darf durch Outsourcing nicht vermindert werden,	17.3b
☐	Dienstleister und Dritte über die Sicherheitsleitlinie informieren,	17.1c
☐	auch Externe sensibilisieren,	17.4a
☐	Wartung durch externes Personal vertraglich regeln,	17.2a
☐	Wartungsarbeiten nur zu speziellen Zeitfenstern durchführen,	17.2b
☐	Fernwartung durch Externe von innen initiieren.	17.2c

II.6 Aufrechterhaltung des Administrator-Qualifikationsniveaus und weitere Absicherung der Admin-Tätigkeiten

Systemadministratoren MÜSSEN über fachliche Qualifikationen, Fortbildungsmöglichkeiten sowie über ausreichend Ressourcen verfügen. Ihre Tätigkeiten MÜSSEN zudem abgesichert sein:

☐	Regelmäßige Schulungen für die Systemadministratoren durchführen,	14.1c
☐	regelmäßige Information von Systemadministratoren über aktuelle IT-Sicherheitsgefährdungen,	14.1d
☐	Einrichten eines lokal gesicherten Administrations-Notfallaccounts,	14.2b
☐	sicherstellen, dass lokale Administrationsrechte nur von den dafür registrierten Personen nutzbar sind und auch nur für die Administratoraufgaben genutzt werden	14.2c 14.2d
☐	klare Zuordnung der Administrator-Accounts zu den Personen.	14.3a

II.7 Organisatorische Maßnahmen

Die zusätzlichen Absicherungen und die Richtlinien MÜSSEN entsprechend der nachfolgenden Punkte organisiert werden.

II.7.A Zugangs- und Zugriffsrechte regeln

☐	Prozesse für alle Beteiligten bei Personal- bzw. Rollenwechsel erstellen,	24.3a
☐	Verfahren für die Vergabe sowie den Entzug von erforderlichen Zugangs- und Zugriffsrechten anfertigen.	24.3b

II.7.B Datenschutzaspekte

☐	Richtlinie zum Schutz personenbezogener Daten mit der Leitlinie zur Informationssicherheit abstimmen,	3.1a
☐	Datenschutzkonzept inklusive Zugriffschutz für die IT-Systeme erstellen.	24.2d

II.7.C Personal noch stärker in Informationssicherheit einbinden

- ☐ Prozessverantwortliche angemessen in die Risikobewertung und die Entwicklung des Maßnahmenplanes einbinden, 4.3a
- ☐ alle Beschäftigten über die aktuell gültigen Informationssicherheitsrichtlinien informieren, 13.3a
- ☐ Durchführen regelmäßiger Schulungs- und Sensibilisierungsmaßnahmen, 13.3b
- ☐ ausreichende Sensibilisierung der Nutzer mobiler Systeme und Telearbeitsnutzer bezüglich der Regelungen zur Verarbeitung von Gesundheitsdaten. 27.2b

II.7.D Identifizieren und Verwalten aller Prozesse

- ☐ Prozesse und deren IT-Abhängigkeiten bekanntgeben und dokumentieren, 4.1a
- ☐ Handlungsanweisungen und Verantwortlichkeiten für kritische Prozesse und Anwendungen festlegen und dokumentieren, 4.2a
- ☐ Regelungen für die Zuständigkeit der jeweiligen Prozesse und Anwendungen bezüglich der Informationssicherheit festlegen, 4.2b
- ☐ diese Zuständigkeiten redundant auslegen, die Personen oder ihre Vertreter SOLLTEN im Notfall erreichbar sein. 4.2c

II.8 Richtlinien zur Aufrechterhaltung der Sicherheit erstellen

Die Reihenfolge bei der Erstellung der Richtlinien SOLL anhand der erfassten Situation bewertet werden. Es sind diverse Richtlinien zu erstellen, unter anderem für:

- ☐ Datensicherung bzw. Backup, 29.1a
- ☐ den Beschaffungsprozess der IT-Infrastruktur, 12.1i
- ☐ den Datenaustausch mit externen Partnern, 17.1a
- ☐ die Aufrechterhaltung der Informationssicherheit im Umgang mit Lieferanten, Dienstleistern und Dritten, 17.1b
- ☐ Cloud-Nutzung 17.A.2a
- ☐ Fernzugriffe, 20.1c
- ☐ Softwarenutzung, 22.1b
- ☐ Nutzung von Internet und E-Mail, 22.4a
- ☐ das Rollen- und Rechtekonzept, 24.2a
- ☐ das Zugriffsrechtekonzept für Datenzugriffe, 24.2b
- ☐ die Datenklassifizierung, 24.2c
- ☐ die Komplexität und Länge der Passwörter, 25.4a
- ☐ die Verwendung mobiler Systeme/Geräte, 27.1a
- ☐ die Telearbeit, 27.1b
- ☐ den Umgang mit Videokonferenzen, 27.1c
- ☐ die Protokollierung, 31.4c
- ☐ den ordnungsgemäßen Umgang mit Datenträgern sowie entsprechende Meldewege bei Verlust oder Diebstahl, 32.1a
- ☐ Löschung von Daten. 33.1a

Stufe 3: Gesamtabsicherung, Überprüfung und finale Dokumentation

Sie können erst mit Stufe 3 beginnen, sobald Sie die Stufen 0, 1 und 2 möglichst vollständig umgesetzt haben.

III.1 Assets im Asset-Verzeichnis erfassen

Regelungen für den Umgang mit Assets aufstellen und umsetzen:

☐	Dokumentation der zu Informationsverbünden zusammengefassten Assets regeln,	9.2a
☐	Assets in einem Werte-Inventarverzeichnis speichern,	9.3a
☐	dabei Abhängigkeiten und Gruppen von Informationswerten darstellen,	9.3b
☐	insbesondere Medizingeräte, die Gesundheitsdaten verarbeiten, im Asset-Verzeichnis darstellen.	9.4b

III.2 Ausbau von Systemen zur zentralen Verwaltung und Administration

Es KÖNNEN Systeme und Software verwendet werden, um bisherige Maßnahmen zentral zu verwalten:

☐	Software-Verwaltungstool (z.B. zum Konfigurationsmanagement und zur Softwareverteilung) verwenden, um z.B. Client-Systeme eines Informationsverbundes nach zentralen Vorgaben einheitlich zu konfigurieren,	21.1b
☐	ein Mobile Device Management implementieren,	27.4a
☐	ein Software-Tool zum betrieblichen Kontinuitätsmanagement (BCM) verwenden.	7.1b

III.3 Externe Kooperation für Informationssicherheit aufbauen

Die externe Informationsversorgung und die externe Unterstützung KANN sichergestellt werden durch:

☐	Etablierung von Informationswegen, um für die Informationssicherheit relevante Informationen zu erhalten und auszutauschen,	16.1a 16.2a
☐	Klärung, wo für Informationssicherheitsvorfälle, die die eigenen Kapazitäten übersteigen, extern Hilfe angefordert werden kann,	16.3a
☐	Sicherstellung, dass im Fall von externer Unterstützung bei akuten Informationssicherheitsvorfällen das IT-Sicherheitsniveau nicht vermindert wird.	16.3b

III.4 Regelmäßigkeit und Aktualität sichern

Die Reihenfolge bei der im Folgenden im Sinne eines kontinuierlichen Verbesserungsprozesses genannten Tätigkeiten SOLL anhand der erfassten Situation gewählt werden. Zu Tätigkeiten, die regelmäßig durchgeführt werden SOLLEN oder die auf dem aktuellsten Stand zu halten sind, zählen Folgende:

☐	Bekannt gewordene Schwachstellen sofort intern prüfen und betroffene Systeme anpassen,	21.8a
☐	das Qualifikationsniveau der Mitarbeiter entsprechend ihrer Aufgaben regelmäßig festlegen und überprüfen,	1.2c
☐	Lernerfolgskontrollen zum Thema Awareness durchführen,	13.3e
☐	ISB: initiieren, dass die operativ verantwortlichen Organisationseinheiten regelmäßig konkrete Verbesserungsvorschläge zum Erreichen des angestrebten Informationssicherheitsniveaus erarbeiten,	2.3b

- ☐ regelmäßig prüfen, ob die Architektur ausreichend robust ist und ob Redundanzen entsprechend funktionieren, 11.5a
- ☐ IT-Netzstrukturplan regelmäßig aktualisieren, 19.1b
- ☐ Autoupdate, Roll-Out und Roll-Back-Konzepte regelmäßig prüfen, 30.2a
- ☐ Notfallübungen in Bezug auf kritische Prozesse und Systeme in regelmäßigen Abständen durchführen, 6.3b
- ☐ externe Dienstleister hinsichtlich der Einhaltung vertraglicher Regelungen prüfen, 17.1d
- ☐ regelmäßig Penetrationstest an redundant ausgelegten Systemen durchführen ohne die Patientensicherheit und ggfs. die Betriebssicherheit zu gefährden. 23.4a

III.5 Umfassende Dokumentation

- ☐ Erfassen und dokumentieren:
  - ☐ Durchgeführte Maßnahmen, Verantwortlichkeiten und Handlungsanweisungen im Falle eines Informationssicherheitsvorfalls, 8.1c
  - ☐ Maßnahmen, die Assets bei der Weitergabe schützen, 9.6a
  - ☐ alle Weiteren noch nicht erfassten Assets u.a. Endgeräte, IT-Systeme, Informationswerte (die kritischen Assets wurden bereits in I.3 dokumentiert), 9.4a
  - ☐ Betriebssystemversionen und Applikations-Systemstände, vor allem bei Medizingeräten, 9.4c
  - ☐ Systeme auf denen keine Betriebssystemaktualisierung durchgeführt werden darf, 30.2b
- ☐ Asset-Verzeichnisse und Dokumentationen der Informationsverbünde aktuell halten, 9.1c
- ☐ Prozess etablieren, der sicherstellt, dass Dokumentationen regelmäßig auf Aktualität überprüft werden, 5.1c
- ☐ es wäre wünschenswert, ein „Inventory and Configuration Management System“ (CMDB) aufzubauen.

Stufe 4: Auditierung und Zertifizierung

Mit Stufe 4 kann erst begonnen werden, sobald die Stufen 0, 1, 2 und 3 möglichst vollständig umgesetzt wurden.

Die Informationssicherheit wird regelmäßig systematisch überprüft und kontinuierlich verbessert (vgl. auch die die mit „KANN“ markierten Hinweise im Fragebogen).

Für die Auditierung bzw. Zertifizierung wird von Ihnen ein ISMS-Standard ausgewählt, nach dem diese interne oder externe Auditierung bzw. Zertifizierung stattfinden kann. Dazu sind noch weitere, über diese Orientierungshilfe hinausgehende, spezifische von diesem Standard geforderte Vorbereitungen, Richtlinien und Maßnahmen umzusetzen.

Die Wirksamkeit von Maßnahmen zur Informationssicherheitsverbesserung ist regelmäßig durch interne oder externe Audits zu überprüfen, hierzu sind folgende Punkte zu beachten:		18.1a
☐	Vorgehen für Audits klar definieren und dokumentieren,	18.1b
☐	sicherstellen, dass diese Audits keine für den Betrieb störenden Änderungen von Daten oder Systemen verursachen,	18.1c
☐	die Kenntnisnahme von Gesundheitsdaten durch Dritte bei Audits ausschließen,	18.1d
☐	die Durchführung der Audits protokollieren,	18.1e
☐	durch Externe durchgeführte Audits vertraglich regeln.	18.2a