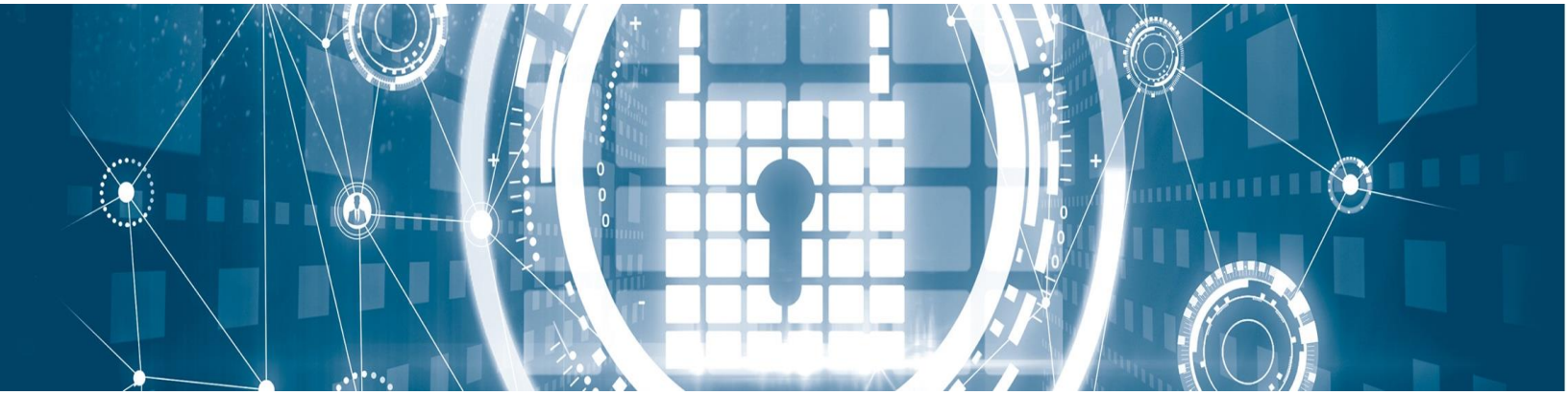
e:los



LEITLINIE
INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM (ISMS)

ASKLEPIOS KLINIKEN BAYERN

STAND 25.08.2023

INHALTSVERZEICHNIS

1. Geltungsbereich

Die Leitlinie zur Informationssicherheit ist für alle Beschäftigten verbindlich. Jeder interne als auch externe Dienstleister oder Kooperationspartner, der Informationen oder Infrastruktur der Einrichtung nutzt, unterliegt dieser Informationssicherheitsleitlinie und ist zu entsprechendem Handeln verpflichtet.

Im besonderen Fokus stehen die Kernprozesse des medizinischen Betriebs sowie relevante Führungs- bzw. Unterstützungsprozesse. Der Kernprozess der Patientenversorgung beinhalt insbesondere die Schritte

- Vorbereitung/Aufnahme
- Diagnostik
- Therapie
- Unterbringung und Pflege
- Entlassung

Relevante Führungs- / Unterstützungsprozesse sind insbesondere Prozesse der Abteilungen bzw. Stabsstellen

- Klinikführung
- IT
- Medizinprodukte und Medizingeräte
- Technik und Gebäudemanagement
- Mitarbeiter
- Einkauf, Beschaffung
- Qualitätsmanagement
- Sicherheit und Notfallpläne (für die Themengebiete Datenschutz und Informationssicherheit)

Die aktuelle Prozesslandkarte der Klinik konkretisiert obige Ausführungen.

2. Politik

Die Klinikführung bestätigt mit dieser Leitlinie den hohen Stellenwert der Informationssicherheit für das Unternehmen.
Dieses Dokument definiert die Zielsetzung der Informationssicherheit und legt den Geltungsbereich, eine allgemeine Sicherheitsstrategie mit kontinuierlicher Verbesserungsabsicht sowie den grundlegenden organisatorischen Rahmen fest.

Die stetig steigende Unterstützung aller medizinischen und nichtmedizinischen Prozesse durch die Informationstechnologie geht mit einer ebenfalls steigenden Abhängigkeit von dieser Unterstützung einher. Die Schutzziele Patientensicherheit und Behandlungseffektivität bekommen dabei eine besondere Bedeutung. Sie können nur dann gewahrt werden, wenn die Vertraulichkeit, Integrität / Authentizität und Verfügbarkeit von Informationen sowie die Authentizität von Kommunikationspartnern gewahrt bzw. richtig umgesetzt werden.

3. Qualitätsziele

Über die oben genannten Grundsätze hinaus verbindet die Klinik mit den Aufgaben der Informationssicherheit u.a. folgende Ziele:

- Vermeidung von Patientengefährdung durch IT-bedingte Störungen.
- Die Verfügbarkeit von wesentlichen Geschäftsprozessen und der dafür erforderlichen Ressourcen und Systeme.
- Reduktion potenzieller Schäden durch eingetretene Beeinträchtigungen mittels effektiver und effizienter reaktiver Maßnahmen (BCM: Betriebliches Kontinuitätsmanagement).
- Sicherstellung der Integrität, Authentizität und Vertraulichkeit von Informationen entsprechend ihrem jeweiligen Schutzbedarf.
- Die Einhaltung der einschlägigen gesetzlichen, regulativen, vertraglichen und normativen Vorgaben.
- Förderung der Mitwirkung der Beschäftigten zur Zielerreichung durch Schulungen und Sensibilisierungsmaßnahmen.

Inhalte Qualitätsmanagementzielplan

Themenkapitel der LSI-Liste werden während der Implementierungsphase (vorauss. 2 Jahre) regelmäßig auf Umsetzung geprüft. Die LSI-Liste inkl. Umsetzungstand wird dem QMB jährlich von dem Informationssicherheitsbeauftragten Hr. Wrobel zur Verfügung gestellt.
Der Umsetzungsstand wird in den Qualitätsmanagementzielplan aufgenommen.

4. Informationssicherheit und Datenschutz

Im Rahmen der Informationssicherheit wird auch den besonderen Datenschutzanforderungen Rechnung getragen. Die gesetzlichen Anforderungen der EU-Datenschutzgrundverordnung sowie die landes- und spezialrechtlichen Regelungen fordern im Rahmen der Verarbeitung von personenbezogenen Daten besondere Schutzmaßnahmen zur Wahrung der Persönlichkeits- und Freiheitsrechte.

Jeder Beschäftigte trägt eine Mitverantwortung im Rahmen seiner Tätigkeit auf eine Minimierung der Risiken für die Informationssicherheit und den Datenschutz hinzuwirken sowie die Fortführung der Behandlungs- und Geschäftsprozesse im Notfall zu unterstützen.

5. Abkürzungen und Definitionen

ISB	Informationssicherheitsbeauftragter
DSB	Datenschutzbeauftragter
Authentizität	Sicherstellung, dass Informationen von der angegebenen Quelle erstellt wurden.
Behandlungseffektivität	Wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen.
ISMS	Informationssicherheitsmanagementsystem; Bestandteil des gesamten Managementprozesses; umfasst die Aufstellung von Verfahren und Regeln innerhalb der Klinik, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern.
Informationssicherheit	Aufrechterhaltung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Informationen.
Integrität	Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.
Vertraulichkeit	Sicherstellung des Schutzes vor unbefugter Preisgabe von Informationen
Verfügbarkeit	Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder Informationen können von den Anwendern wie vorgesehen genutzt werden.
Patientensicherheit	Vermeidung von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

6. Rollen, Verantwortlichkeiten und Pflichten

Das Informationssicherheitsmanagement der Klinik sieht im Folgenden aufgelistete Rollen mit entsprechenden Verantwortlichkeiten vor. Diese werden im Rahmen von Tätigkeitsbeschreibungen und/oder Verträgen festgelegt.

Klinikführung	Um die in dieser Leitlinie formulierten Ziele zu erreichen, initiiert die Geschäftsführung den Informationssicherheitsprozess und stellt Ressourcen im angemessenen Umfang bereit. Sie sorgt für die Zielerreichung und lässt sich dazu vom Informationssicherheitsbeauftragten im Lenkungsausschuss ISMS regelmäßig berichten. Die Klinikführung trägt die Gesamtverantwortung für die Informationssicherheit.
Lenkungsausschuss ISMS	Der Lenkungsausschuss Informationssicherheitsmanagementsystem bezeichnet das interne Gremium, das für das ISMS die strategischen Vorgaben beschließt und sich den aktuellen Stand berichten lässt. Die Besetzung und die Tagungsrhythmen sowie das Berichtswesen sind in der Geschäftsordnung zum Lenkungsausschuss Informationssicherheitsmanagementsystem geregelt. Flankiert wird der Lenkungsausschuss durch die Jour-Fixe des internen ISMS-Koordinators mit dem ISB.
Informationssicherheitsbeauftragter (ISB)	Der Informationssicherheitsbeauftragte ist Stabsstelle der Geschäftsführung. Er soll in seiner Funktion maßgeblich dazu beitragen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von schützenswerten Informationen auf Dauer gewährleistet werden können und diese mit der Patientensicherheit und Behandlungseffektivität in Einklang gebracht werden.
Interner ISMS-Koordinator	Der interne ISMS-Koordinator unterstützt den ISB operativ und berichtet ihm regelmäßig zum Maßnahmenstatus. Der ISMS-Koordinator nimmt an den Sitzungen des Lenkungsausschusses ISMS sowie an Teamsitzungen teil und informiert die jeweiligen Abteilungsleitungen bzw. verantwortlichen Mitarbeiter. Mit dem ISB finden regelhafte Jour-Fixe statt.
ISMS-Team	Das ISMS-Team stellt die Arbeitsebene bei der Einführung des ISMS dar. Es ist mit Vertretern der Bereiche IT, Medizintechnik, Technik, Einkauf, Personal, QM, Ärzte, Pflege, Verwaltung und Betriebsrat besetzt. Die Sitzungen finden anlassbezogen mit den jeweiligen Mitgliedern des ISMS-Teams statt. Geplant werden die Sitzungen über den ISMS-Koordinator.
Datenschutzbeauftragter (DSB)	Der Datenschutzbeauftragte ist Stabsstelle der Geschäftsführung. Er soll in seiner Funktion maßgeblich

	dazu beitragen, dass die Bestimmungen des Datenschutzes eingehalten werden und diese mit der Patientensicherheit und Behandlungseffektivität in Einklang gebracht werden.
Beschäftigte	Alle Beschäftigten sollen sich möglicher Gefährdungen bewusst sein und sich sicherheitsgerecht verhalten. Hierzu sollen Schulungen, Sensibilisierungen (z.B. Warnung vor aktuellen Themen) und Audits beitragen. Zudem finden sich in den erstellten Handlungsanweisungen und Richtlinien Vorgaben für die tägliche Arbeit. Ein Meldeprozess für potentielle Vorfälle ist etabliert.

Weiterhin gibt es interessierte Parteien, deren Belange bei der Entwicklung des Informationsmanagementsystems Berücksichtigung finden.

7. Sicherheitsstrategie

Ziel ist es, ein System aufzubauen und weiterzuentwickeln, mit welchem es gelingt, die Klinik vor den sich ständig verändernden Risiken im Bereich der Informationssicherheit mit einem angemessenen wirtschaftlichen und administrativen Aufwand zu schützen.
Dieser Prozess wird durch die Einführung eines Informationssicherheitsmanagementsystems, orientiert an der ISO 27001, unterstützt. Dabei werden die Vorgaben des branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus (B3S) sowie Ausarbeitungen des Landesamtes für Sicherheit in der Informationstechnik Bayern (LSI) berücksichtigt.

8. Einführung neuer Systeme bzw. Erweiterung

Bei der Entscheidung zur Einführung neuer informationstechnischer und medizintechnischer Systeme oder deren Erweiterung ist der ISB sowie der Datenschutzbeauftragte hierüber zu informieren und in den Prozess ausreichend miteinzubeziehen. Dies betrifft Systeme oder Erweiterungen, die lokal von dem Krankenhaus beschafft werden. Für den Konzern beschaffte Systeme oder Erweiterungen werden zentral von dem Konzernbeauftragten geprüft und freigegeben.
Die Fachabteilungen und Stabsstellen der Klinik unterstützen den Informationssicherheitsbeauftragten bei der Bewertung der lokalen Systeme oder Erweiterungen. Sofern sich aus der Bewertung die Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung gemäß EU-Datenschutzgrundverordnung ergibt, ist diese durchzuführen und zu dokumentieren.
Zum Betrieb von als kritisch bewerteten Systemen aus den Bereichen Medizingeräte, IT-Systeme, IT-Netzwerke, IT-Anwendungen muss verbindlich eine Freigabe auf Basis einer Risikobewertung vorliegen. Dies gilt ebenso bei relevanten Änderungen an diesen Systemen.

9. Meldewege bei Vorfällen

Alle Personen (krankenhausintern als auch extern), die im Geltungsbereich des Dokuments nicht ausdrücklich und begründet ausgeschlossen sind, haben die Pflicht, potentielle sicherheitsrelevante Ereignisse, Beobachtungen und erkannte Sicherheitsvorfälle unverzüglich gemäß des definierten Meldeweges zu melden.

10. Weiterentwicklung der Informationssicherheit

Die Bereiche Technik, Medizintechnik und IT erarbeiten angemessene, allgemeingültige Schutzkonzepte zur Absicherung der technikunterstützten Informationsverarbeitung in enger Abstimmung mit dem ISB und der internen ISMS-Koordinatorin. Spezifische Maßnahmen und Vorgaben werden in den jeweiligen Konzepten, Richtlinien und Vereinbarungen ausformuliert.

Die Geschäftsführung unterstützt die ständige Verbesserung des Informationssicherheitsniveaus sowie des Datenschutzniveaus. Alle Mitarbeiterinnen und Mitarbeiter sind angehalten, Verbesserungsvorschläge oder mögliche Schwachstellen an die interne ISMS-Koordinatorin zu melden.

Der Informationssicherheitsbeauftragte berichtet der Geschäftsführung regelmäßig in den Sitzungen des Lenkungsausschusses zum Stand der Informationssicherheit. Die Geschäftsführung entscheidet über die empfohlenen Maßnahmen zur Verbesserung und zum Ausbau der Informationssicherheit. Die Entscheidungen müssen im Sinne der Aufrechterhaltung eines kontinuierlichen Verbesserungsprozesses dokumentiert werden.

11. Inkrafttreten, Zusicherung und Durchsetzung

Die vorliegende Leitlinie tritt unmittelbar auf Beschluss der Geschäftsführung in Kraft.
Die Geschäftsführung der Klinik bekennt sich zu den in dieser Leitlinie festgelegten Zielen, dem Geltungsbereich und der beschriebenen Sicherheitsstrategien. Verstöße und Zuwiderhandlungen gegen Überzeugungen und Vorgaben der Informationssicherheitsleitlinie werden gemäß eines formellen Prozesses behandelt.