1 Zweck/Ziel

Für das Universitätsklinikum Jena (UKJ) hat Informationssicherheit einen außerordentlich hohen Stellenwert erreicht. Der Vorstand legt mit dieser Leitlinie die verbindlichen Vorgaben und Ziele zur laufenden Überwachung und Verbesserung der Informationssicherheit am UKJ fest.

Das Informationssicherheitsmanagementsystem (ISMS) unterstützt den Vorstand dabei, seiner gesetzlichen Verantwortung für die Informationssicherheit gerecht zu werden. Ein wesentlicher Bestandteil des ISMS ist die Integration des Datenschutzmanagements mit den Schnittstellen zu den technischen und organisatorischen Maßnahmen. Die Informationssicherheitsrichtlinie nimmt dabei Bezug auf die „Richtlinie zur Umsetzung der gesetzlichen Datenschutzanforderungen am UKJ“ vom 07.04.2021

Diese Informationssicherheitsleitlinie und das damit verbundene ISMS schafft für jeden Mitarbeiter eine Grundlage für das Verständnis von Informationssicherheit am UKJ. Jeder Mitarbeiter kann sein Sicherheitsbewusstsein stärken und aktiv das Informationssicherheitsniveau mitgestalten.

2 Geltungsbereich

Diese Leitlinie gilt für alle Bereiche des UKJ einschließlich seiner Tochtergesellschaften, welche mit der Erhebung, Verarbeitung, Überprüfung und Löschung von Informationen befasst sind.

Dieses Dokument ist in der Schutzklasse „öffentlich“ klassifiziert und somit nach Freigabe für den Gebrauch durch beliebige Personen bestimmt.

3 Abkürzungen/Begriffe

Abk.	Beschreibung
ISB	Informationssicherheitsbeauftragter
DSB	Datenschutzbeauftragter
ISMS	Informationssicherheitsmanagementsystem
IT-SB	IT-Sicherheitsbeauftragter
PDCA	Plan-Do-Check-Act Zyklus
ThürHG	Thüringer Hochschulgesetz
UKJ	Universitätsklinikum Jena

4 Verantwortungsregelung

Funktion	**Verantwortlichkeiten**

Klinikumsvorstand	- Verantwortlich für die Umsetzung der Leitlinie - Bereitstellung der benötigten Ressourcen - Systematische Einbindung des ISB bei relevanten Entscheidungen im Rahmen der Informationssicherheit durch entsprechende Regelungen und Verfahrensweisen
Informationssicherheits-beauftragter (ISB)	- Verantwortlich für die Steuerung des ISMS und dem damit verbundenen Risikomanagement - Maßnahmenplanung und –controlling zur Erfüllung der Ziele nach § 7 - Unterstützung und Beratung des Klinikumsvorstandes zu strategischen Themen der Informationssicherheit - Leitung und Verantwortung der Stabstelle Informationssicherheits- und Datenschutzmanagement am UKJ
Stabstelle Informationssicherheits- und Datenschutzmanagement (ISM/DSM)	- Schnittstelle zur Stabstelle des DSB - Vertretungsfunktion des ISB und des DSB - operative Umsetzung von Belangen der Informationssicherheit und des Datenschutzes
GB Informationstechnologie/ GB Betreibung und Beschaffung	- operative Umsetzung von Belangen der Informationssicherheit - Unterstützung des ISB und des Vorstandes bei der Wahrnehmung ihrer Aufgaben im ISMS

5 Bedeutung der Informationssicherheit

Moderne Patientenversorgung, Forschung und Lehre erfordern zunehmend den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung des UKJ im Sinne der Patienten und weiterer Partner effizient und effektiv zu gestalten. Patienteninformationen, Forschungs- und technische Daten sind dabei wertvolle Ressourcen, deren Schutz für das Ansehen und die Aufgabenerfüllung maßgeblich sind.

Aufgaben, Prozesse und die Aufbauorganisation unterliegen dabei einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten.

In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen und der damit verbundenen Risiken ist es essentiell, stetig ein angemessenes Informationssicherheitsniveau zu schaffen. Beim Umgang mit Informationen aller Art wird im UKJ darauf geachtet, dass dem Schutzbedarf entsprechend Rechnung getragen wird.

6 Bezug zu Geschäftszielen und -aufgaben

Sowohl bei der Erbringung der Pflichtaufgaben der kritischen Dienstleistung „medizinische Patientenversorgung“ als auch der Forschungsaufgaben und der Lehre werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit besonders schützenswerte Güter darstellen. Hierbei handelt es sich um Informationen, die entsprechend gesetzlicher Anforderungen geschützt werden müssen oder auch um wettbewerbsrelevante Informationen von Unternehmen, die Unbefugten nicht bekannt werden dürfen. Informationssicherheit umfasst somit die Summe aller organisatorischen, personellen und technischen Maßnahmen am UKJ, um eine sichere Patientenversorgung zu gewährleisten und die § 98 ThürHG verbundenen Geschäftsziele zu erreichen.

Es ist daher notwendig, die Infrastruktur der Informationstechnik und der Kommunikationskanäle im Zusammenspiel mit Informationen, IT-Verfahren, Aufgaben und Prozessen ganzheitlich zu betrachten.

Für die Umsetzung der Informationssicherheit am UKJ ist der Kaufmännische Vorstand verantwortlich, der sich mit den ressort-verantwortlichen Vorständen zu den Zielen und Maßnahmen der Informationssicherheit insoweit abstimmt und sich der operativen Umsetzung der zuständigen Geschäftsbereiche und Stabsstellen bedient.

7 Ziele der Informationssicherheit in der Patientenversorgung

Für die Sicherstellung der medizinischen Patientenversorgung ist die Wahrung der Grundwerte zur Informationssicherheit **Verfügbarkeit**, **Vertraulichkeit** und **Integrität** im jeweils erforderlichen Maße und nach dem Stand der Technik zu erreichen.

Als primäres Sicherheitsziel wird die medizinische Patientenversorgung mit ihren dazugehörigen Prozessen und Aufgaben, die der Erhaltung und Wiederherstellung der Gesundheit des Patienten dienen, betrachtet.

Dabei wird das primäre Ziel von folgenden strategischen Zielen ergänzt:

- Gewährleistung der Einhaltung von gesetzlichen und vertraglichen Vorgaben,
- Risikooptimiertes Handeln in allen Geschäftsprozessen,
- Identifizierung und Behandlung von Risiken,
- Reduzierung von Risiken, die sich aus einer unzureichenden Berücksichtigung von Vertraulichkeit, Verfügbarkeit und Integrität ergeben,
- effektive Betreibung eines Business-Continuity-Managementsystems unter Berücksichtigung der Informationssicherheit,
- die kontinuierliche Weiterentwicklung des Managementsystems für Informationssicherheit und Datenschutz,
- eine hohe Qualität der angebotenen Dienstleistungen, besonders im Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit von Informationen unter Berücksichtigung der ökonomischen Randbedingungen,
- Bestätigung des Vertrauens der externen Partner und Dienstleister in die informationsverarbeitenden Struktureinheiten,

- Schutz der Unternehmensreputation in der Öffentlichkeit

8 Sicherheitsstrategie

Das UKJ betreibt zur Wahrung seiner Aufgaben ein ISMS. Dieses dient dazu, die Informationssicherheit zu definieren, zu steuern, zu kontrollieren, aufrechterhalten und fortlaufend zu verbessern.

Diese Informationssicherheitsleitlinie gibt den Rahmen für das Management der Informationssicherheit des UKJ vor. Dabei wird ein angemessenes Sicherheitsniveau angestrebt, welches durch das ISMS umgesetzt wird.

Das ISMS ist nach der Norm ISO/IEC 27001:2013ff ausgerichtet. Die Wirksamkeit wird durch eine Auditierung nach ISO/IEC 27001:2013ff mindestens einmal jährlich überprüft.

Die Sicherheitsstrategie wird durch den Klinikumsvorstand und dem ISB unter Einbeziehung der verantwortlichen Struktureinheiten des UKJ mindestens einmal jährlich analysiert und ggf. angepasst.

Um ein geeignetes Informationssicherheitsniveau zu erreichen, richten sich alle technisch-organisatorischen Maßnahmen nach dem Stand der Technik aus. Die Beschäftigten des UKJ werden kontinuierlich geschult und sensibilisiert, um aktiv an der Informationssicherheit mitzuwirken.

9 Aufbauorganisation

9.1 Kaufmännischer Vorstand

Nach dieser Leitlinie ist für die Umsetzung der Informationssicherheit am UKJ der Kaufmännische Vorstand verantwortlich, der sich mit den ressort-verantwortlichen Vorständen zu den Zielen und Maßnahmen der Informationssicherheit insoweit abstimmt. Für die Erfüllung seiner Aufgaben und Verantwortung unterstützt die Stabsstelle Informationssicherheits- und Datenschutzmanagement unter Leitung des Informationssicherheitsbeauftragten.

9.2 Stabsstelle Informationssicherheits- und Datenschutzmanagement

Diese zentrale Stabsstelle unter dem Kaufmännischen Vorstand steuert das ISMS sowie das operative Datenschutzmanagement, deren Anforderungen sich aus dem IT-Sicherheitsgesetz und der Datenschutzgrundverordnung ergeben.

Diese Stabsstelle dient zur Sicherstellung und Weiterentwicklung eines hohen Informationssicherheits- und Datenschutzstandards am UKJ.

Der Aufgabenbereich des operativen Datenschutzmanagements unterstützt den DSB in einer direkten Schnittstellenfunktion.

9.3 Informationssicherheitsbeauftragter

Als zentrale Sicherheitsinstanz ernennt der Kaufmännische Vorstand einen Informationssicherheitsbeauftragten (ISB), der für alle relevanten Fragen der Informationssicherheit zuständig ist. Dieser ist dem Vorstand in dieser Rolle direkt unterstellt und berichtet unmittelbar. Die Stabsstelle Informationssicherheits- und Datenschutzmanagement unterliegt der Leitung des ISB.

Als Schnittstelle zum ISB fungiert ebenfalls der Geschäftsbereich Informationstechnologie mit dem Arbeitsbereich IT-Security.

Dem ISB werden alle erforderliche Ressourcen bereitgestellt. Ein Austausch mit der Leitung der Geschäftsbereiche und dem IT-Sicherheitsbeauftragten (IT-SB) findet kontinuierlich statt, um die Informationssicherheitsziele des UKJ zu erfüllen.

10 Geltungsbereich des ISMS (Scope)

Der Geltungsbereich des ISMS umfasst die Betreibung von informationstechnischen Systemen und Prozessen, die zur Aufrechterhaltung der Kritischen Dienstleistung nach § 6 Absatz 1 BSI-KritisV der stationären medizinischen Versorgung dienen.

Dies beinhaltet die Prozesse der Patientenaufnahme, der Diagnostik, der Therapie, der stationären Allgemein-, Intensivpflege, der Entlassung sowie der Ambulanz und der Tagesklinik.

Daraus leiten sich technische und behandlungsunterstützende Prozesse und (IT-) Services der zentralen Verwaltungsbereiche des UKJ ab.

Das ISMS und die damit verbundenen Anforderungen werden auch durch die Tochterunternehmen des UKJ angewendet.

11 Umsetzung der Informationssicherheitsleitlinie

Der Vorstand stellt im erforderlichen Rahmen Personal- und Finanzmittel bereit, um ein angemessenes Informationssicherheitsniveau bei der Verarbeitung schützenswerter Informationen sicher zu stellen. Diese werden durch die Geschäftsbereiche in Abstimmung mit dem Informationssicherheitsbeauftragten eingeplant.

Die Sicherheitsmaßnahmen müssen in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch Sicherheitsvorfälle verursacht werden kann. Diese Maßnahmen und deren Auswirkungen ergeben sich aus dem etablierten Risikomanagement zur Informationssicherheit, welches in der Richtlinie Risikomanagement ISMS beschrieben ist.

Die Darstellung und Umsetzung des ISMS sind in der Richtlinie ISMS definiert.

Die ausgewählten Sicherheitsmaßnahmen werden regelmäßig hinsichtlich Effektivität und Vollständigkeit geprüft und weiterentwickelt.

12 Verpflichtung zur kontinuierlichen Verbesserung

Durch ständige Weiterentwicklungen von gesetzlichen, technischen und organisatorischen Gegebenheiten prägen die Entwicklungen, denen sich die Ansätze zum Management der Informationssicherheit anpassen.

Der ISB trägt dafür Sorge, dass das ISMS und die damit verbundene Sicherheitsstrategie anhand des PDCA-Zyklus (Planen – Umsetzen – Überprüfen – Handeln) kontinuierlich weiterentwickelt wird und ist bei allen organisatorisch-technischen Neuerungen oder Änderungen, die Auswirkungen auf die Informationssicherheit haben können, durch die entsprechenden Geschäftsbereiche frühzeitig einzubinden.

13 Querverweise

Richtlinie Informationssicherheitsmanagementsystem (R)

Richtlinie zum Risikomanagement der Informationssicherheit (R)

Richtlinie zur Umsetzung der gesetzlichen Datenschutzanforderungen am UKJ (R)

Mitgeltende Unterlagen

→

Link:

Verknüpfte Dokumente

→

Ablage unter:

,