Universitätsklinikum Jena
Der Vorstand

Leitlinie Informationssicherheit

Dokumentenname:		ukj_ll_intr_Informationssicherheit.docx	
Autor:		A. Sparbrod	
Status:	genehmigt	Version:	1.0
Gültig von:	19.12.2018	Gültig bis:	
Erstellt am:	28.11.2018	Schutzklasse:	öffentlich
Ersetzt Dokument:		-	
Seiten:	6	Anhänge:	keine
Geltungsbereich:		UKJ	
Berechtigter Personenkreis:			
Auswirkungsbereich:			

1 Zweck/ Ziel

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

Mit dieser Informationssicherheitsleitlinie und das damit verbundene Informationssicherheits-managementsystem (ISMS) wird jedem Mitarbeiter ein Grundverständnis zur Informationssicherheit geschaffen. Dadurch bekommt jeder Mitarbeiter ein Sicherheitsbewusstsein und kann aktiv das Informationssicherheitsniveau mitgestalten.

Das ISMS unterstützt den Vorstand dabei, seiner gesetzlichen Verantwortung für die Informationssicherheit gerecht zu werden.

2 Geltungsbereich

Diese Leitlinie gilt für alle Bereiche des Universitätsklinikums Jena, 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
ISMS	Informationssicherheitsmanagementsystem
IT-SB	IT-Sicherheitsbeauftragter
PDCA	Plan-Do-Check-Act Zyklus
UKJ	Universitätsklinikum Jena

4 Verantwortungsregelung

Funktion	Verantwortlichkeiten
Autor der Leitlinie	■ Sicherstellung der Verständlichkeit, Genauigkeit und Vollständigkeit der Leitlinie in Übereinstimmung mit gesetzlichen und internen Bestimmungen ■ Pflege der Leitlinie
Prüfer	■ Kontrolle der Verständlichkeit, Genauigkeit und Vollständigkeit der Leitlinie ■ Kontrolle der Leitlinie auf Durchführbarkeit und Plausibilität

Funktion	Verantwortlichkeiten
Klinikumsvorstand	■ Verantwortlichkeit für die Umsetzung der Leitlinie ■ Bereitstellung der benötigten Ressourcen

5 Festlegungen/ Ablauf

5.1 Bedeutung der Informationssicherheit

Moderne Patientenversorgung, Forschung und Lehre erfordert zunehmend den Einsatz aktueller Informationstechnologien, um die Aufgabenerfüllung der Uniklinik Jena (UKJ) im Sinne der Patienten und weiterer Partner effizient und effektiv zu gestalten.

Patienteninformationen, Forschungs- und technische Daten sind wertvolle Ressourcen, deren Schutz für das Ansehen und die Aufgabenerfüllung des UKJ maßgeblich sind.

Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten. In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen. Beim Umgang mit Informationen aller Art wird im UKJ darauf geachtet, dass dem Schutzbedarf entsprechend Rechnung getragen wird.

Datenschutz und IT-Sicherheit ordnen sich unter die Informationssicherheit. Für die Umsetzung der Informationssicherheit ist der Kaufmännische Vorstand verantwortlich, der sich mit den ressort-verantwortlichen Vorständen zu den Zielen und Maßnahmen der Informationssicherheit insoweit abstimmt.

5.2 Bezug zu Geschäftszielen und -aufgaben

Es ist notwendig, das Zusammenspiel der Informationen, IT-Verfahren, Aufgaben und Prozesse sowie der Infrastruktur der Informationstechnik und Kommunikationskanäle ganzheitlich zu betrachten. Informationssicherheit umfasst die Summe aller organisatorischen, personellen und technischen Maßnahmen, um die Geschäftsziele des UKJ zu erreichen. Sowohl bei der Erbringung der Pflichtaufgaben der kritischen Dienstleistung „medizinische Patientenversorgung“ als auch der Forschungsaufgaben werden Informationen erhoben und verarbeitet, deren Vertraulichkeit, Integrität und Verfügbarkeit ein hohes Gut darstellen. Hierbei handelt es sich um Informationen, die entsprechend gesetzlicher Anforderungen geschützt werden müssen, oder auch um wettbewerbsrelevante Informationen von Unternehmen, die Unberechtigten nicht bekannt werden dürfen.

5.3 Ziele der Informationssicherheit

Im Sinne der Informationssicherheit wird die medizinische Patientenversorgung, mit den zugehörigen Prozessen und Aufgaben, die der Erhaltung und Wiederherstellung der Gesundheit des Patienten dienen, als primäres Sicherheitsziel betrachtet. 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. Dabei wird das primäre Ziel von folgenden strategischen Zielen ergänzt:

- Gewährleistung der Einhaltung von gesetzlichen und vertraglichen Vorgaben,
- Schutz der Kundenreputation,
- Bestätigung des Vertrauens der Kunden in die informationsverarbeitenden Geschäftsbereiche,
- Gewährleistung des guten Rufs des Universitätsklinikums Jena in der Öffentlichkeit,

- Hohe Qualität der angebotenen Dienstleistungen, besonders im Hinblick auf Verfügbarkeit, Integrität und Vertraulichkeit unter Berücksichtigung der ökonomischen Randbedingungen,
- Nachvollziehbarkeit der Vorgänge, Transparenz der Dienstleistungen gegenüber dem Kunden,
- Risikooptimiertes Handeln in allen Geschäftsprozessen,
- Identifizierung und Behandlung von Risiken und
- Reduzierung von Risiken, die sich aus einer unzureichenden Berücksichtigung von Vertraulichkeit, Verfügbarkeit und Integrität ergeben.

5.4 Sicherheitsstrategie und Aufbauorganisation

Jeder Mitarbeiter ist für Informationssicherheit verantwortlich. Um ein geeignetes Informationssicherheitsniveau zu erreichen, wird die Mitwirkung aller Beschäftigten zur Informationssicherheit vorausgesetzt.

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. Die Wirksamkeit des ISMS wird durch eine Auditierung nach ISO27001:2013ff mindestens jährlich überprüft.

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. Ein Austausch mit der Leitung des Geschäftsbereichs IT und dem IT-Sicherheitsbeauftragten (IT-SB) findet regelmäßig statt.

Dem ISB werden erforderliche Ressourcen bereitgestellt und geeignete Qualifizierungsmaßnahmen ermöglicht, um seine Aufgaben zeitlich und fachlich zu erfüllen.

In regelmäßigen Abständen werden die ausgewählten Sicherheitsmaßnahmen auf Effektivität und Vollständigkeit geprüft. Die Umsetzung ist in entsprechenden Richtlinien und Verfahrensanweisungen des ISMS dokumentiert.

5.5 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.

Mitarbeiterinnen und Mitarbeiter des UKJ werden regelmäßig und bedarfsgerecht auf Informationssicherheit sensibilisiert und geschult.

Die Darstellung und Umsetzung des ISMS sind in der Richtlinie ukj_r_intr_ISMS dokumentiert.

5.6 Verpflichtung zur kontinuierlichen Verbesserung

Durch ständige Weiterentwicklungen von gesetzlichen, technischen und organisatorischen Gegebenheiten ist Informationssicherheit kein unveränderlicher Zustand. Diesen Entwicklungen müssen sich die Ansätze zum Management der Informationssicherheit anpassen. Aus diesem Grund trägt der ISB dafür Sorge, dass die Sicherheitsstrategie kontinuierlich weiterentwickelt wird. Das ISMS wird anhand eines kontinuierlichen Verbesserungsprozesses nach dem PDCA-Zyklus betrieben. Dieser Prozess beschreibt im Kern die Phasen Planen – Umsetzen – Überprüfen – Handeln. Der Informationssicherheitsbeauftragte ist bei allen organisatorisch-technischen Neuerungen oder

Änderungen, die Auswirkungen auf die Informations-sicherheit haben können, durch die Geschäftsbereiche frühzeitig einzubinden.

6 Querverweise

ukj_r_intr_ISMS	Richtlinie Informationssicherheitsmanagementsystem
ukj_r_intr_Risikomanagement_ISMS	Richtlinie zum Risikomanagement der Informationssicherheit

7 Anhänge

-

8 Inkrafttreten

Diese Leitlinie zur Informationssicherheit tritt am 19.12.2018 in Kraft. Sie gilt bis zum Abschluss einer neuen Leitlinie fort.

Jena, den 19.12.2018

Dr. B. Seidel-Kwem	PD Dr. J. Maschmann	Prof. Dr. K. Benndorf
Kaufmännischer Vorstand	Medizinischer Vorstand	Wissenschaftlicher Vorstand