Medizinische Universität
Lausitz – Carl Thiem

Leitlinie zur Informationssicherheit

1. Ziel und Zweck

Stellenwert der Informationssicherheit

Informationen befinden wesentlich über eine qualitativ hochwertige Versorgung unserer Patienten.

Medizinische Prozesse, Geräte und Anlagen verschmelzen zusehend mit der Informations- und Kommunikationstechnik, um die vielfältigen, hochkomplexen Analyse-, Behandlungs- und Pflegevorgänge im Medizinischen Universität Lausitz – Carl Thiem (MUL-CT) zu bewältigen. Digitale Informations- und Steuerungssysteme bilden die unerlässliche Basis für digitale medizinische Prozesse, für ein sicheres, wirtschaftliches und am Patienten orientiertes Handeln.

Die MUL-CT sichert nicht nur die medizinische Versorgung der Stadt Cottbus, sondern versorgt als Universitätsklinikum im Einzugsgebiet über 500.000 Menschen und gilt somit als ein Unternehmen der Kritischen Infrastruktur für die Bundesrepublik Deutschland.

Ziele der Informationssicherheit

Die Informationssicherheit soll die Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit jeglicher Informationen (digital und analog) sowie in deren Zusammenhang die Patientensicherheit und Behandlungseffektivität im Rahmen des Krankenhausbetriebes bewahren. Insbesondere sind alle Informationen unserer Patienten nach diesen Grundwerten zu behandeln. Die Ziele des Datenschutzes gelten formal weiter und sind integraler Bestandteil der Informationssicherheitsziele.

- Vertraulichkeit schützt Informationen vor unberechtigtem Zugriff von Personen, IT-Systemen oder Anlagen.
  Beispiel: Patientendaten sind sehr vertrauliche Informationen! Patientendaten sollen nicht frei zugänglich im Internet stehen. Nicht jeder Mitarbeit muss alle Patientendaten lesen können.

- Integrität sorgt für die Richtigkeit und Vollständigkeit der Informationen.
  Beispiel: Im Krankenhausinformationssystem gespeicherte Informationen müssen richtig und vollständig sein. Wenn diese Informationen versehentlich oder vorsätzlich geändert würden, könnten die Daten zu falschen Diagnosen oder Behandlungen führen und lebensbedrohliche Situationen für den Patienten bedeuten.

- Verfügbarkeit sichert die erforderliche Nutzbarkeit von Informationen, IT-Systeme oder Anlagen.
  Beispiel: Das Krankenhausinformationssystem fällt aus, sodass geführte klinische Prozesse nicht in gewohnter Qualität erbracht werden können.

- Authentizität bedeutet die Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit von Informationen.
  Beispiel: Mitarbeiter, die das Krankenhausinformationssystem nutzen, müssen eindeutig als diese Person identifiziert werden können. Informationen, wie ein Arztbrief, müssen eindeutig und zweifelsfrei der erstellenden Person zugeordnet werden können.

- Patientensicherheit wird definiert als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.
  Beispiel: Die Beeinträchtigung der Verfügbarkeit oder Integrität eines Steuerrechners einer Medizinischen Anlage kann eine Patientengefährdung zur Folge haben.

- Behandlungseffektivität stellt das zielgerichtete Zusammenwirken der beteiligten Prozesse und Informationen zur medizinischen Behandlung des Patienten, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.
  Beispiel: Die Beeinträchtigung der Verfügbarkeit oder Authentizität eines Informationssystems kann wesentliche medizinische Prozesse und damit die Behandlung vieler Patienten negativ beeinflussen.

2. Geltungsbereich

Diese Leitlinie gilt verbindlich für alle Mitarbeiterinnen und Mitarbeiter sowie externe Mitarbeiter bzw. Lieferanten des Medizinischen Universität Lausitz – Carl Thiem samt der Tochterunternehmen (CTK-Poliklinik GmbH, Thiem Care GmbH, Thiem Research GmbH und Thiem-Service-Gesellschaft).

Alle Geschäftsprozesse, Informationen, Anwendungen, IT-Systeme, Infrastrukturen und medizinische Anlagen unterliegen dieser Leitlinie.

3. Informationssicherheitsmanagement

Zur Wahrung der Informationssicherheit betreibt die MUL-CT ein Informationssicherheits-managementsystem und richtet dies an dem internationalen Standard DIN ISO/IEC 27001 aus. Zusätzlich müssen die branchenspezifischen Sicherheitsstandards des Gesundheitssektors berücksichtigt werden.

Grundsätze:

- Sicherheit als integraler Bestandteil: *Anforderungen an die Informationssicherheit sind in allen Prozessen und Projekten zu berücksichtigen.*
- Digitale Medizin und Patientenorientierung*: Informationssicherheit soll digitale Prozesse unterstützen und auf den Patienten und Mitarbeiter fokussierend schützen.*
- Schutz der individuellen Selbstbestimmung: *Personenbezogene Daten, wie Patientendaten, bedürfen besonderer Informationssicherheitsmaßnahmen.*
- Zuständigkeit: *Jeder Prozess und jedes IT-System oder Anlage besitzt einen Verantwortlichen.*
- Aktualität: *Eingesetzte IT-Systeme und Anlagen sollen nach aktuellen Informationssicherheitsempfehlungen betrieben werden.*
- Datensicherheit: *Daten müssen auch in außergewöhnlichen Situationen (beispielsweise Pandemie oder Großbrand) zur Verfügung stehen.*
- Bewusstsein für die Informationssicherheit: *Alle Mitarbeiter kennen die für sie geltenden Regelungen zum Umgang mit Informationen und zur Wahrung der Informationssicherheit.*
- Angemessenheit: *Informationssicherheitsmaßnahmen sollen risikoorientiert mit Augenmaß (Kosten-Nutzen-Benutzerfreundlichkeit-Verhältnis) ausgewählt werden.*
- Kontinuierliche Verbesserung des Informationssicherheitsmanagementsystems.

Informationssicherheitsorganisation

Die Gesamtverantwortung für die Informationssicherheit liegt beim Vorstandsvorsitzenden der MUL-CT. Zur operativen Umsetzung wurde ein Informationssicherheitsbeauftragter bestellt und eine Informationssicherheitsorganisation bestimmt.

Vorstandsvorsitzenden

- initiiert, steuert und kontrolliert den Informationssicherheitsprozess,
- bestellt den Informationssicherheitsbeauftragten,
- stellt ausreichend Ressourcen zur Umsetzung von Informationssicherheitsmaßnahmen zur Verfügung,
- übernimmt aktiv die Restrisiken in der Informationsverarbeitung.

Informationssicherheitsbeauftragter (ISB)

- ist zentrale Ansprechstelle für alle Belange der Informationssicherheit,
- berät den Vorstand zur Informationssicherheit,
- berichtet regelmäßig dem Vorstand zum Status der Informationssicherheit,
- beitreibt das Informationssicherheitsmanagementsystem (ISMS),
- verantwortet operativ den Informationssicherheitsprozess,
- überwacht die wirksame Umsetzung der Informationssicherheitsmaßnahmen,
- identifiziert Restrisiken in der Informationsverarbeitung,
- sensibilisiert und schult zu Themen der Informationssicherheit,
- leitet und koordiniert die Arbeiten des Informationssicherheitsmanagementteams.

Informationssicherheitsmanagementteam (ISM-Team)

- unterstützt den ISB beim Betrieben des ISMS,
- erarbeitet Lösungsansätze zur Umsetzung der Anforderungen zur Informationssicherheit.

Führungskräfte

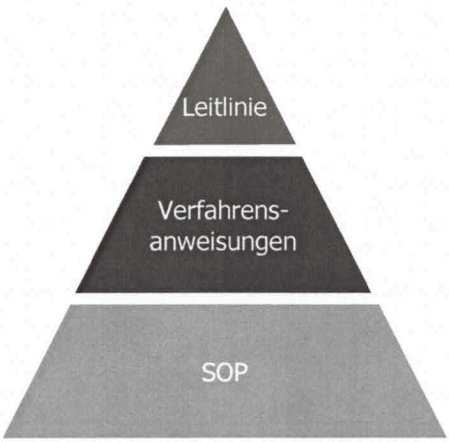
- verantworten die Wahrung der Informationssicherheitsziele in ihrem Zuständigkeitsbereich,
- bewerten die Anwendungen und Informationen hinsichtlich der Kritikalität für verantwortete Prozesse,
- informieren ihre Mitarbeiter regelmäßig und bedarfsorientiert über die Regeln der Informationssicherheit.

Mitarbeiter

- wenden bewusst die Regelungen zur Informationssicherheit an,
- melden Informationssicherheitsvorfälle an die verantwortliche Stelle.

Umsetzung und Regelwerk

Das Regelwerk der Informationssicherheit umfasst folgendes dreistufiges Modell. Die Leitlinie gibt den Rahmen der Informationssicherheit vor und wird durch Verfahrensanweisungen präzisiert. Standardarbeitsanweisung (SOP) beschreiben Abläufe und Handlungsweisen zu einzelnen Bereichen der Informationssicherheit.



Die vorliegende Leitlinie zur Informationssicherheit und das ergänzende Regelwerk der Informationssicherheit dienen der Erreichung der Informationssicherheitsziele. Der Vorstand hat diese Leitlinie beschlossen und unterstützt die erforderlichen Maßnahmen zur Umsetzung der Informationssicherheit.

4. Verteiler

Alle Mitarbeiter des MUL-CT inkl. der Tochterunternehmen

Ersetzt Leitlinie zur Informationssicherheit vom 12.07.2023

Gültig ab 01.08.2024:

Cottbus,

Prof. Eckhard Nagel
Vorstandsvorsitzender