KlinikumDarmstadt GmbH Akademisches Lehrkrankenhaus	*Leitlinie* **Informationssicherheitsleitlinie**	**Informationssicherheit**

Inhalt

A. Zweck

Die Informationssicherheitsleitlinie schafft die Grundlage für den Aufbau eines Informationssicherheitsmanagementsystems (ISMS), das die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus aller Daten im Verantwortungsbereich von der Klinikum Darmstadt GmbH und ihren Tochtergesellschaften sicherstellt. Das ISMS beinhaltet Aufbauorganisation, Ablauforganisation (Prozesse) und Regelwerk, die geeignet sind, Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich zu gewährleisten.

B. Allgemein

Die Informationssicherheit hat den Schutz von analogen und digitalen Informationen, Geschäftsprozessen und den dazugehörigen Vermögenswerten (Assets) als Ziel. Der Schutz wird durch Einhaltung der Schutzziele der Informationssicherheit (siehe Abschnitt D) aufrechterhalten.

C. Geltungsbereich

Dieses Dokument gilt für die Klinikum Darmstadt GmbH mit allen Standorten, ihren Tochtergesellschaften und den dazugehörigen Beschäftigten. Auf Grund des überschrittenen Schwellwertes für Krankenhäuser gemäß der BSI-Kritisverordnung nach dem BSI-Gesetz, ist die Klinikum Darmstadt GmbH rechtlich zum Betrieb eines Informationssicherheitsmanagementsystems verpflichtet. Dies beinhaltet angemessene organisatorische und technische Regelungen zum Betrieb informationstechnischer Systeme.
Darüber hinaus ist das medizinisches Versorgungszentrum (MVZ) ab 01.01.2022 durch § 75b SGB V verpflichtet, die angemessene organisatorische und technische Regelungen zum Betrieb informationstechnischer Systeme sicherzustellen.

Es ist flächendeckend bei Planung, Entwicklung, Beschaffung, Einrichtung, Betrieb, Nutzung und Entsorgung informationsverarbeitender Einrichtungen und Prozesse einzuhalten.
Die Anwendungsbereiche für KRITIS und gem. § 75b SGB V, sind in eigenen Dokumenten definiert.

Wird Dritten außerhalb der Klinikum Darmstadt GmbH Zugriff auf Informationen oder andere Werte des Geltungsbereichs gewährt, so sind diese durch entsprechende Vereinbarungen auf sinngemäße Einhaltung dieses Dokuments zu verpflichten. Die Gestaltung der Vereinbarungen obliegt der Klinikum Darmstadt GmbH. Die Dritten haben die Einhaltung auf geeignete Weise nachzuweisen, das Klinikum behält sich eine Überprüfung vor.

D. Ziele und Anforderungen an die Informationssicherheit

Die Zielvorgaben des ISMS im genannten Geltungsbereich sind folgende:

Vertraulichkeit:
Es muss sichergestellt sein, dass ausnahmslos nur berechtigten Personen Zugang zu Informationstechnologien (IT) bzw. Daten gewährt wird.
Es muss sichergestellt sein, dass die auf den IT-Systemen gespeicherten vertraulichen Daten - insbesondere kritische Unternehmens- oder Beschäftigtendaten sowie einer besonderen Verschwiegenheitspflicht unterliegende Patientendaten - nicht unbefugt eingesehen werden können. Die in diesem Zusammenhang einschlägigen gesetzlichen Bestimmungen sind umzusetzen und einzuhalten.

Integrität:
Es muss sichergestellt sein, dass Informationstechnologien bzw. Daten nicht unberechtigt zerstört, in ihrer Funktion beeinträchtigt, vernichtet, gelöscht oder manipuliert werden können.

Verfügbarkeit:
Es muss sichergestellt sein, dass notwendige Informationstechnologien bzw. Daten bei Bedarf und auf Grund eines entsprechenden Nutzungs- und Berechtigungsprofils jederzeit von jedem dazu geeigneten und bestimmten Arbeitsplatz verfügbar und zugänglich sind.

Patientensicherheit:
Bei Assets, die unmittelbar zur Krankenversorgung genutzt werden, ist immer die Patientensicherheit zu beachten. Die Patientensicherheit wird als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen verstanden. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

Behandlungseffektivität
Es ist sicherzustellen, dass eine wirksame Behandlung der Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, inklusive des dazu erforderlichen Informationsaustausches, möglich ist.

Weitere Anforderungen an das ISMS, die berücksichtigt werden sollen, sind:

- Erbringung des Nachweises gemäß §8a (3) BSIG
- Erfüllung der Vorgaben nach § 75b SGB V
- Sicherstellung und Berücksichtigung der besonderen Anforderungen an den Datenschutz in der medizinischen Versorgung
- Sicherstellung der ambulanten und stationären Patientenversorgung
- Berücksichtigung der Anforderungen des branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus
- Sicherstellung der Anforderungen der interessierten Parteien an die Informationssicherheit
- Aufrechterhaltung und kontinuierliche Verbesserung der Informationssicherheit
- Minimierung der Schäden durch ein stetig angepasstes Risikomanagement
- Aufrechterhaltung und Unterstützung der Compliance-Anforderungen der Klinikum Darmstadt GmbH
- Sensibilisierung der Beschäftigten im Bereich der Informationssicherheit und des Datenschutzes
- der Minimalisierung der Gefährdung der Wettbewerbsfähigkeit
- Stetige Verbesserung des Images in der Öffentlichkeit

Diese Ziele und Anforderungen stimmen mit den Geschäftszielen, der Strategie und den Geschäftsplänen der Organisation, die im Leitbild des Klinikums verankert sind, überein. Die Geschäftsführung ist für die Überprüfung dieser generellen ISMS Zielvorgaben und für die Definition neuer Zielvorgaben verantwortlich. Diese Leitlinie und das gesamte ISMS müssen sowohl den rechtlichen und gesetzlichen Anforderungen als auch den vertraglichen Verpflichtungen entsprechen, die für die Organisation auf dem Gebiet der Informationssicherheit maßgeblich sind.

E. Informationssicherheitsstrategie

Die Informationssicherheitsstrategie für die Klinikum Darmstadt GmbH und ihren Tochtergesellschaften besteht darin, mit wirtschaftlich angemessenen Ressourceneinsatz ein höchst mögliches Schutzniveau der Informationssicherheit zu erreichen und verbleibende Restrisiken zu minimieren. Dieser kontinuierliche Prozess wird durch die Geschäftsführung verantwortet und unterstützt. Die Entwicklung und Freigabe dieser Leitline zur Informationssicherheit, die Festlegung von Grenzwerten für tolerierbare Informationssicherheitsrisiken in Form von Vorgaben für die Akzeptanz von Informationssicherheitsrisiken sowie die Übernahme der Verantwortung für die ausgewiesenen Restrisiken durch die Geschäftsführung sollen die Wirksamkeit des ISMS und dieser Informationssicherheitsstrategie sicher stellen.

Das Verhältnis von Aufwand und Behandlung von Informationssicherheitsrisiken ist für den spezifischen Schutzbedarf innerhalb des Geltungsbereiches dieser Leitlinie angemessen zu gestalten. Zur Sicherstellung der kontinuierlichen Ausrichtung der Maßnahmen zur Informationssicherheit an dieser Leitlinie ist ein Risikomanagement für die Informationssicherheit zu implementieren.

F. Verantwortlichkeiten

Die Gesamtverantwortung für die Umsetzung der erforderlichen Maßnahmen zur Absicherung der ambulanten sowie der vollstationären medizinischen Versorgung als kritischer Dienstleister trägt die Geschäftsführung. Die Geschäftsführung hat sicherzustellen, dass alle Beschäftigten der Klinikum Darmstadt GmbH sowie entsprechende externe Parteien mit dieser Leitlinie vertraut sind und diese mittragen.
Die Geschäftsführung benennt einen Informationssicherheitsbeauftragten, der für die Koordination des Betriebes des ISMS verantwortlich ist. Der Informationssicherheitsbeauftragte berichtet in seiner Funktion direkt an die Geschäftsführung.

Ausreichende Ressourcen u.a. Personal, Budget und Zeit für die Umsetzung erforderlicher Maßnahmen zur Informationssicherheit werden von der Geschäftsführung zur Verfügung gestellt.

Der Informationssicherheitsbeauftragte wirkt im Auftrag und in Abstimmung mit der Geschäftsführung auf die Einhaltung und Verbesserung sämtlicher Maßnahmen zur Informationssicherheit hin.

Zentrale Aufgaben des Informationssicherheitsbeauftragten sind in Auftrag der Geschäftsführung die Kontrolle und Überprüfung der getroffenen Maßnahmen zur Informationssicherheit auf Vollständigkeit, Wirksamkeit und Widerstandsfähigkeit sowie Zuverlässigkeit und Angemessenheit unter Berücksichtigung des aktuellen Stands der Technik. Eine solche Bewertung/ Messung wird mindestens einmal jährlich von der Geschäftsführung durchgeführt. Diese können auch im Bedarfsfall oder anlassbezogen überprüft und ggf. angepasst werden.

Der Informationssicherheitsbeauftragte ist frühzeitig in alle Themen und Projekte, die Bezüge zur Informationssicherheit haben, einzubinden, um bereits in der Planungsphase relevante Aspekte für die Informationssicherheit zu beachten. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

In relevanten Fragestellungen zur Informationssicherheit steht den Beschäftigten der Klinikum Darmstadt GmbH und deren Tochtergesellschaften der Informationssicherheitsbeauftragte beratend und begleitend zur Verfügung.

Sicherheitsvorfälle oder Schwachstellen müssen gemäß den internen Vorgaben gemeldet werden.

G. Maßnahmen zur Informationssicherheit

Sämtliche Maßnahmen werden in einem angemessenen wirtschaftlichen Verhältnis zum jeweils angestrebten Schutzbedarf der Daten und Informationen stehen und in Bezug auf die dynamische Entwicklung des Unternehmens sorgfältig ausgewählt.
Die gewählten Maßnahmen und deren Implementierungs-Status sind in entsprechenden Maßnahmenplänen zu dokumentieren. Darüber hinaus ist eine Erklärung zur Anwendbarkeit (SOA) gemäß den Anforderungen des B3S der medizinischen Versorgung zu erstellen, freizugeben und in regelmäßigen Abständen zu aktualisieren.

H. Verbesserung der Informationssicherheit

Die Leitlinie zur Informationssicherheit wird regelmäßig auf ihre Aktualität und Wirksamkeit hin geprüft und gegebenenfalls angepasst.
Die Geschäftsführung unterstützt aktiv die ständige Verbesserung der Informationssicherheit mit geeigneten Ressourcen, um alle genannten Zielvorgaben zu erfüllen.
Alle relevanten Personen des Unternehmens sowie die Geschäftsführung sind angehalten, die Umsetzung und Aufrechterhaltung sämtlicher Maßnahmen aktiv zu unterstützen und sich anbahnende und auftretende Informationssicherheitsvorfälle unverzüglich zu melden.
Darüber hinaus sollen alle relevanten Personen der Klinikum Darmstadt GmbH und Tochtergesellschaften geschult und sensibilisiert werden.

I. Verstöße und Folgen

Ein für die Informationssicherheit oder den Datenschutz der Klinikum Darmstadt GmbH und deren Tochtergesellschaften gefährdendes Verhalten kann disziplinar- vertrags-, straf- oder arbeitsrechtliche Konsequenzen haben.

J. Vermerke

Autor:	**Rojewski Benita Elke (STAB_IN)** **Name**
Prozesseigner:	**Rojewski Benita Elke (STAB_IN)** **Name**
Freigabe:	**von Khaladj Nawid Prof. Dr. med. (GF) am 06.09.2022 von Maurer Clemens (GF) am 08.09.2022** **Name und Datum**