Inhalt

[Präambel 2](#_Toc86645398)

[1. Stellenwert der Informationssicherheit 2](#_Toc86645399)

[2. Weitere Ziele 3](#_Toc86645400)

[3. Datenschutz 3](#_Toc86645401)

[4. Risikomanagement 3](#_Toc86645402)

[5. Organisation des Informationssicherheitsprozesses 4](#_Toc86645403)

[6. Weiterentwicklung der Informationssicherheit 5](#_Toc86645404)

[7. Inkrafttreten und Veröffentlichung 6](#_Toc86645405)

[8. Dokumentenhistorie 6](#_Toc86645406)

Präambel

**Anwendungshinweis (Bitte vor Benutzung entfernen):**

Die vorliegenden Empfehlungen und Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt die Deutsche Krankenhausgesellschaft keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

Das Direktorium des Klinikum XXXXX hat folgende Leitlinie zur Informationssicherheit als Bestandteil seiner strategischen Ausrichtung verabschiedet. Informationssicherheit umfasst dabei alle Aspekte von Datenschutz und Informationssicherheit.

1. Stellenwert der Informationssicherheit

Die stetige steigende Unterstützung aller medizinischen und nichtmedizinischen Prozesse durch die Informationstechnologie geht mit einer ebenfalls steigenden Abhängigkeit von dieser Unterstützung einher.

Besondere Bedeutung kommt in unserem Klinikum XXXXX den Schutzzielen Patientensicherheit und Behandlungseffektivität zu.

**Patientensicherheit:** Es ist sicherzustellen, dassdie Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen gewährleistet ist. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

**Behandlungseffektivität:** Es ist sicherzustellen, dass Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen erfolgt.

Diese können nur dann gewahrt werden, wenn die Integrität, Verfügbarkeit, Vertraulichkeit und Authentizität von Informationen sowie die Authentizität von Kommunikationspartnern richtig umgesetzt werden.

**Integrität:** Es ist sicherzustellen, dass Informationen während der gesamten Verarbeitung

unversehrt, vollständig und aktuell bleiben.

**Verfügbarkeit:** Es ist sicherzustellen, dass Informationen zeitgerecht zur Verfügung stehen und ordnungsgemäß verarbeitet werden können.

**Vertraulichkeit:** Es ist sicherzustellen, dass nur Befugte Daten und Informationen zur Kenntnis nehmen können.

**Authentizität:** Die Identität der Kommunikationspartner ist jederzeit sicherzustellen.

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

Jeder Beschäftigte trägt die Verantwortung im Rahmen seiner Tätigkeit die Risiken für die IT zu minimieren und die Fortführung der Behandlungs- und Geschäftsprozesse im Notfall sicherzustellen sowie die gesetzlichen Datenschutzanforderungen einzuhalten. Dies gilt im Besonderen für die Führungskräfte.

Die Führungskräfte haben unter Beachtung ihrer maßgebenden Vorbildfunktion in ihrem jeweiligen Verantwortungsbereich insbesondere auch dafür zu sorgen, dass die für das Klinikum bestehenden Regelungen zur Informationssicherheit und zum Datenschutz beachtet und eingehalten werden.

Der/die Klinikumsdirektor/in trägt die Verantwortung für die Informationssicherheit und den Datenschutz im Klinikum XXXXX. Dies umfasst alle im Klinikum betriebenen informationstechnischen Systeme und Verarbeitungsprozesse mit personenbezogenen Daten.

Zur Wahrung der Belange der Informationssicherheit wird ein interner oder externer Informationssicherheitsbeauftragter benannt. Ebenso wird für die Belange des Datenschutzes eine Datenschutzbeauftragter benannt. Die Ernennung kann intern oder extern erfolgen.

In der *Stabsstelle Informationssicherheit* werden alle Belange zu Informationssicherheit und Datenschutz zusammengefasst.

(Anmerkung: Entsprechend der tatsächlichen Gegebenheiten sind andere wirksame Organisationsformen möglich.)

Die Umsetzung und Einhaltung dieser Leitlinie wird vom Direktorium als letzte Kontrollinstanz verantwortet.

1. Weitere Ziele

Über die oben genannten Schutzziele hinaus verbindet das Klinikum XXXXX mit den Aufgaben Informationssicherheit und Datenschutz folgende Ziele:

* Nachvollziehbarkeit und Rechtmäßigkeit der Datenverarbeitung
* Reduzierung von aus dem Betrieb von IT-Systemen entstehenden Risiken
* Erfüllung der gesetzlichen Anforderungen (Datenschutz, BSIG, SGB, etc.)
* Einleitung und Umsetzung sicherheitsfördernder Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung
* Risikominimierung bei der Einführung neuer Technologien
* Vermeidung von Patientengefährdung durch IT-bedingte Störungen
* Wahrung der Schutzrechte von Betroffenen
* Umsetzung von Transparenz-, Informations- und Meldepflichten
* Einbeziehung aller Fachabteilungen und Stabsstellen

1. Geltungsbereich

Die vorliegende Leitlinie zur Informationssicherheit gilt verbindlich für alle Beschäftigten des Klinikums XXXXX.

1. Datenschutz

Die besonderen Belange des Datenschutzes werden in eigenen Regelwerken berücksichtigt.

1. Risikomanagement

Vor der Entscheidung zur Einführung neuer informationstechnischer und medizintechnischer Systeme oder deren Erweiterung wird unabhängig vom vorgesehenen Betreiber über die Stabsstelle Informationssicherheit eine Risikobewertung eingeholt.

Diese erfolgt bereits im Rahmen der Beschaffung unabhängig vom Vergabeverfahren spätestens jedoch vor der Implementierung der neuen Systeme. Besteht eine vom Direktorium verabschiedete Projektbeauftragung ist dieser Bewertungsschritt von der verantwortlichen Projektleitung zwingend einzuleiten und die Stabsstelle Informationssicherheit zu involvieren.

Die Fachabteilungen (IT-Beauftragte/ Datenschutzkoordinatoren aus dem Bereich) des Hauses unterstützen bei der Erstellung der Risikobewertungen.

Sofern sich aus der Risikobewertung die Notwendigkeit zur Durchführung einer Datenschutzfolgeabschätzung gemäß Datenschutzgrundverordnung ergibt, ist diese unter Einbindung der Stabsstelle Informationssicherheit sowie weiterer interner Stellen durchzuführen und zu dokumentieren.

Zum Betrieb von als kritisch bewerteten Systemen aus den Bereichen Medizingeräte, IT-Systeme, IT-Netzwerke, IT-Anwendungen muss eine Freigabe auf Basis einer verbindlichen Risikobewertung vorliegen. Dies gilt ebenso bei relevanten Änderungen an diesen Systemen.

Für bereits im Einsatz befindliche Systeme wird die Risikobewertung mittelfristig nachgeholt.

Darüber hinaus erhält das Direktorium von der *Stabsstelle Informationssicherheit* mindestens jährlich einen Risikobericht. Die Überwachung der daraus resultierenden Risikobehandlung obliegt der *Stabsstelle Informationssicherheit*.

Die verschiedenen Risikomanagementbereiche einschließlich der vernetzten Medizintechnik des Klinikums werden mittelfristig mit dem Ziel einer durchgängigen Kommunikation konsolidiert.

1. Organisation des Informationssicherheitsprozesses

Ein Informationssicherheitsmanagement-Team überwacht die Ausführung der Informationssicherheitsmaßnahmen und entscheidet über die Einleitung von Maßnahmen bei Informationssicherheitsvorfällen in allen IT-Systemen des Klinikums und koordiniert die übergreifenden Maßnahmen in der Gesamtorganisation.

Der/die Informationssicherheitsbeauftragte leitet das Team.

Das Informationssicherheits-Managementteam besteht im Kern aus

* Informationssicherheitsbeauftragter/m
* Benannte/r Vertreter/in dem Betriebsrat (Dienststellenpersonalrat)
* Teamleitung IT
* Benannte/r Vertreter/in für das Risikomanagement
* Benannte/r Vertreter/in aus dem Datenschutzteam

Die Hauptaufgaben umfassen die Aufarbeitung relevanter Störungen.

Das erweiterte Team umfasst auch

* Datenschutzbeauftragte/r
* benannte/r Vertreter/in für das Qualitätsmanagement
* benannte/r Vertreter/in für den Einkauf des Klinikums
* benannte/r Vertreter/in für den Ärztlichen Dienst
* benannte/r Vertreter/in für den Pflegedienst
* benannte/r Vertreter/in für den Technischen Dienst
* benannte/r Vertreter/in für die Medizintechnik
* benannte/r Vertreter/in für das Projektmanagement
* benannte/r Vertreter/in für die Kommunikationstechnik
* benannte/r Vertreter/in für den Betriebsrat (Dienststellenpersonalrat)

Die Hauptaufgaben umfassen die Unterstützung die *Stabsstelle Informationssicherheit* sowohl bei der Organisation des Aufbaus als auch bei der Durchführung und Überwachung der für die Informationssicherheit notwendigen Maßnahmen. Außerdem die Mitwirkung bei der Erarbeitung von Vorgaben (z.B. Schulungskonzept) sowie die Sicherstellung einer themenbezogenen Schnittstelle zwischen den Bereichen.

Bei Bedarf können jederzeit weitere Bereiche hinzugezogen werden.

Für jede Klinik, jedes Institut, die Pflegedienstleitung und jede Abteilung wird vom jeweiligen

Verantwortlichen ein/e IT-Beauftragte/r aus den jeweiligen Bereichen bestimmt, der die Betreuung und Einführung technikunterstützter Informationstechnik unterstützt.

Fragestellungen und technisch-organisatorische Maßnahmen zum Datenschutz werden aufgrund der besonderen Komplexität in einem eigenen Team behandelt und bei Bedarf zeitnah mit dem IS-Managementteam kommuniziert.

Das Datenschutzteam setzt sich zusammen aus

* Datenschutzbeauftragte/r des Klinikums
* benannte/r Vertreter/in der Personalabteilung
* Leitung IT
* Informationssicherheitsbeauftragte/r
* ein Mitglied des Direktoriums

unter der Leitung der/des Klinikumsdirektors/in bzw. des/ der stellvertretenden Klinikumsdirektors/in.

Bei Bedarf können weitere Personen benannt werden.

Für jede Klinik, jedes Institut, die Pflegedienstleitung und jede Abteilung wird vom jeweiligen

Verantwortlichen aus den jeweiligen Bereichen ein/e Datenschutzkoordinator/in bestimmt, der die operative Umsetzung und Einhaltung des Datenschutzes unterstützt.

1. Weiterentwicklung der Informationssicherheit

Der Bereich IT erarbeitet angemessene, allgemeingültige Schutzkonzepte zur Absicherung der technikunterstützten Informationsverarbeitung in enger Abstimmung mit der *Stabsstelle Informationssicherheit*.

Spezifische Maßnahmen und Vorgaben werden in den jeweiligen Konzepten, Dienstvereinbarungen, Dienstanweisungen ausformuliert. Diese sowie die Datenschutzregelwerke unterliegen einer ständigen Weiterentwicklung, basierend u.a. auf den Erkenntnissen des IS-Managementteams bzw. des Datenschutzteams.

Das Direktorium unterstützt die ständige Verbesserung der Informationssicherheitsniveaus sowie des Datenschutzniveaus. Alle Mitarbeiterinnen und Mitarbeiter sind angehalten, Verbesserungsvorschläge oder mögliche Schwachstellen an den Informationssicherheitsbeauftragten bzw. das Datenschutzteam zu melden.

Die *Stabsstelle Informationssicherheit* hat die Aufgabe in Zusammenarbeit mit dem Informationssicherheits-Managementteam, die Informationssicherheitsstrategie und die Wirksamkeit der bisherigen Organisationsform, Maßnahmen und Prozesse für Informationssicherheit kontinuierlich zu überprüfen und weiterzuentwickeln.

Die *Stabsstelle Informationssicherheit* muss dem Direktorium regelmäßig zum Stand der Informationssicherheit berichten. Das Direktorium entscheidet dabei über die empfohlenen Maßnahmen zur Verbesserung und zum Ausbau der Informationssicherheit. Die Entscheidungen des Direktoriums müssen im Sinne der Aufrecherhaltung eines kontinuierlicher Verbesserungsprozess der Informationssicherheit dokumentiert werden.

# Inkrafttreten und Veröffentlichung

Diese Leittlinie tritt zum aa.bb.cccc in Kraft und löst die Leitlinie zur Informationssicherheit vom dd.ee.ffff ab.

8. Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |