

---

# INFORMATIONSSICHERHEITSLITLINIE

## der

## Universitätsmedizin Halle (Saale)

### Präambel

- (1) Das Universitätsklinikum Halle (Saale) und die Medizinische Fakultät der Martin-Luther-Universität Halle-Wittenberg, im Folgenden zusammengefasst als Universitätsmedizin Halle (Saale) bezeichnet, benötigt zur Erfüllung ihrer Aufgaben und zur Erreichung ihrer Ziele eine Vielzahl von Daten und Informationen.<sup>1</sup> Sie unterliegen einem bestimmten Schutzbedarf<sup>2</sup>, welcher sich aus gesetzlichen Vorgaben, dem Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus, dem Patient\*innengeheimnis sowie eigenen Zielen gegenüber Patient\*innen, Beschäftigten, Studierenden und Dritten ergibt.
- (2) Maßgeblich hierbei ist das BSI-Gesetz, das IT-Sicherheitsgesetz (IT-SiG) sowie die KRITIS-Verordnung. Speziell sind der „Stand der Technik“ bzw. der „Branchenspezifische Sicherheitsstandard“ umzusetzen und einzuhalten.<sup>3</sup>
- (3) Primäre Schutzziele der Informationssicherheit an der Universitätsmedizin Halle (Saale) sind die Vertraulichkeit, Verfügbarkeit und Integrität, sowie (als Spezialfall der Integrität) die Authentizität. Sie dienen dazu, die übergeordneten Schutzziele (Schutz der Patient\*innen, Schutz von Beschäftigten und Dritten, Schutz der Einrichtung) aus Sicht der Informationssicherheit zu gewährleisten. Dem Schutzbedarf der Schutzziele soll in wirtschaftlich und rechtlich angemessener Form Rechnung getragen werden.
- (4) Diese Leitlinie hat zum Ziel, einen Rahmen für den Umgang mit den bei Geschäftsprozessen sowohl elektronisch als auch nicht elektronisch verarbeiteten Daten und Informationen sowie der eingesetzten Informationstechnik festzulegen, um deren sichere Nutzung sowie die weitgehend unterbrechungsfreie Verfügbarkeit zu ermöglichen.

### § 1

#### Stellenwert der Informationsverarbeitung

- (1) Nahezu alle Prozesse der Krankenversorgung, der Lehre und der Forschung sind von Informationen direkt oder indirekt abhängig. Verfälschte oder nicht vorhandene Informationen führen kurzfristig zu Störungen im Betriebsablauf, längerfristig oder großflächig zu einem Betriebsstillstand.
- (2) Mit der Verabschiedung dieser Leitlinie wird das Thema Informationssicherheit vom Vorstand aufgegriffen und es wird ein kontinuierlicher Informationssicherheitsprozess etabliert.

### § 2

#### Verantwortung der Vorstandsmitglieder

Die Vorstandsmitglieder des Klinikums tragen die Gesamtverantwortung für die Informationssicherheit, können jedoch Befugnisse delegieren. Sie stehen vollständig zu den in der Leitlinie formulierten Zielen und unterstützen sowohl die Sicherheitsorganisation als auch den Sicherheitsprozess aktiv.

### § 3

#### Gültigkeit

- (1) Die Leitlinie gilt für alle Beschäftigten der Universitätsmedizin Halle (Saale) sowie für alle Personen, die Daten und Informationen der Universitätsmedizin Halle (Saale) nutzen, unabhängig vom bestehenden Vertragsverhältnis. Alle Nutzer\*innen sollen sich der Notwendigkeit der Informationssicherheit und deren Ziele bewusst sein und entsprechend verantwortungsvoll im jeweiligen Arbeitsumfeld handeln.
- (2) Die Leitlinie gilt auch für vertraglich gebundene Unternehmen, die eine Auftragsdatenverarbeitung für die Universitätsmedizin Halle (Saale) erbringen. Für diese wird die Leitlinie zum Vertragsbestandteil.

## **§ 4 Ziele**

- (1) Grundlegende Schutzziele der Informationssicherheit der Universitätsmedizin Halle (Saale) sind:

- a) Vertraulichkeit (Confidentiality)

In der Universitätsmedizin Halle (Saale) werden überwiegend höchst sensible Daten verarbeitet, die einem besonderen Schutz unterliegen.<sup>4</sup> Die berechtigten Interessen der Patient\*innen, der Studierenden, der Beschäftigten und vertraglich gebundenen Unternehmen müssen dabei berücksichtigt werden. Eine Verletzung der Vertraulichkeit geht i.d.R. mit einem großen Ansehens- und Vertrauensverlust einher, verletzt die Rechte der Betroffenen und muss daher vermieden werden.

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Daten oder Informationen. Sie ist gegeben, wenn die schützenswerten Daten und Informationen nur in zulässiger Art und Weise ausschließlich für Befugte zugänglich sind.

- b) Verfügbarkeit (Availability)

Eine Einschränkung oder Unterbrechung der Verfügbarkeit von Dienstleistungen, Funktionen eines IT-Systems, IT-Netzinfrastruktur bzw. von Informationen führt zu Störungen des Betriebsablaufs; bei längerfristigen oder großflächigen Störungen kann der gesamte Betrieb zum Erliegen kommen.

Um Auswirkungen einer Betriebsunterbrechung zu minimieren, sind Ausfallkonzepte zu erstellen, die den handelnden Personen bekannt sein müssen. Insbesondere in Bereichen, bei denen die Nichtverfügbarkeit von Informationen zu einer Gefährdung von Leib und Leben, zum Verstoß gegen gesetzliche Vorgaben oder zu größeren finanziellen Schäden führt, müssen Vorsorgemaßnahmen getroffen werden.

Die Verfügbarkeit von Daten und Informationen ist gegeben, wenn keine Beeinträchtigungen beim Zugriff auf notwendige Informationen oder Ressourcen auftreten und diese stets gemäß ihrem vorgesehenen Zweck und Funktionsumfang nutzbar sind.

- c) Integrität (Integrity)

Die Verlässlichkeit und Konsistenz der verarbeiteten Daten ist sowohl im klinischen, im wissenschaftlichen als auch im kaufmännischen Kontext zu wahren. Falsche Daten führen in allen genannten Bereichen zu Fehlentscheidungen, die nicht toleriert werden können.

Integrität von Daten und Informationen ist gegeben, wenn diese korrekt, d.h. unverfälscht und vollständig erfasst bzw. empfangen wurden, unveränderlich gespeichert und vollständig weiterverarbeitet bzw. unveränderlich und vollständig weitergeleitet werden sowie gültig und widerspruchsfrei sind.

Integrität von Anwendungen und IT-Systemen ist gegeben, wenn diese wie vorgesehen funktionieren.

- d) Authentizität (Authenticity)

Authentizität ist gegeben, wenn sichergestellt ist, dass die an der Kommunikation oder Datenübertragung beteiligten Personen bzw. Komponenten autorisiert und

eindeutig identifizierbar sind. Insbesondere im klinischen und wissenschaftlichen Bereich ist die Authentizität der Daten/Informationen maßgeblich. Eine etwaige Bedrohung der Authentizität ist hauptsächlich bei elektronisch übertragenen Dokumenten gegeben. Dem kann durch Verfahren begegnet werden, bei denen die Herkunft der Daten/Informationen nachvollziehbar ist.

(2) Die in (1) benannten Ziele müssen jeweils auf die übergeordneten Ziele der Universitätsmedizin Halle (Saale) angewendet werden:

a. Schutz der Patient\*innen (Patient\*innensicherheit und Behandlungseffektivität)

Der gesundheitliche Zustand eines\*r Patient\*in darf sich nicht aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter Behandlung, bedingt durch informationssicherheitsbezogene technische, organisatorische und menschliche Fehlerquellen in der Universitätsmedizin Halle (Saale), verschlechtern.

b. Schutz von Beschäftigten und Dritten

Die Gewährleistung der dem Arbeit- bzw. Auftraggeber auferlegten Fürsorgepflicht darf sich nicht aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter Arbeitsbedingungen bzw. -ressourcen, bedingt durch informationssicherheitsbezogene technische, organisatorische und menschliche Fehlerquellen in der Universitätsmedizin Halle (Saale), verschlechtern.

c. Schutz der Einrichtung

Die wirtschaftliche und rechtliche Existenz der Universitätsmedizin Halle (Saale) darf sich nicht aufgrund unterbleibender oder qualitativ/quantitativ eingeschränkter betriebswirtschaftlicher sowie Compliance-bezogener Prozesse bzw. Arbeitsabläufe, bedingt durch informationssicherheitsbezogene technische, organisatorische und menschliche Fehlerquellen in der Universitätsmedizin Halle (Saale), verschlechtern.

## § 5 Umsetzung<sup>5</sup>

(1) Die Universitätsmedizin Halle (Saale) betreibt eine geeignete Informationssicherheitsorganisation, bestehend aus einem Informationssicherheitsmanagement-Team, sowie IT-Beauftragten- und Koordinator\*innen und verfügt über eine\*n benannte\*n Informationssicherheitsbeauftragte\*n.<sup>6</sup> Diese Person gehört zum Zentralen Dienst 16 und ist gleichzeitig Leiter\*in des Sachgebiets Informationssicherheit. Die\*der Informationssicherheitsbeauftragte hat direktes Vortragsrecht gegenüber den Vorstandsmitgliedern. Die\*der Informationssicherheitsbeauftragte steuert den Informationssicherheitsprozess und überwacht die geeignete und wirtschaftliche Umsetzung der in dieser Leitlinie beschriebenen Ziele.

(2) Bei der Umsetzung der Informationssicherheit muss der Aufwand in Relation zu den wirtschaftlichen Auswirkungen beachtet werden.

(3) Der\*dem Informationssicherheitsbeauftragten werden für die Aufgabenerfüllung ausreichende zeitliche, finanzielle und personelle Ressourcen gewährt.

(4) Die\*der Informationssicherheitsbeauftragte erlässt Regelungen (Informationssicherheits-Richtlinien) in Bezug auf die Informationssicherheit in Abstimmung mit der Leitung des ZD1-luK.

(5) Die\*der Informationssicherheitsbeauftragte ist frühzeitig in Beschaffungen und Projekte, welche Auswirkungen auf die IT-Sicherheit der Universitätsmedizin Halle (Saale) haben, einzubeziehen.

(6) Die\*der Informationssicherheitsbeauftragte ist berechtigt, nicht freigegebene IT-Systeme oder IT-Systeme, die den Richtlinien zur Informationssicherheit nicht entsprechen, in

Abstimmung mit der Leitung des ZD1-luK bzw. des ZD14-Technik von der IT-Infrastruktur zu trennen bzw. außer Betrieb nehmen zu lassen. Geeignete Maßnahmen zum Erreichen und zur dauerhaften Einhaltung der Schutzziele §4 Absatz 1 a) bis d) von Daten, Informationen, Anwendungen und IT-Systemen werden in einem gesonderten Informationssicherheitskonzept ausführlich dargestellt.

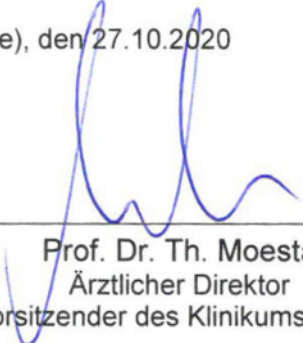
## § 6 Kontinuierlicher Verbesserungsprozess

- (1) Die\*der Informationssicherheitsbeauftragte ist verpflichtet, regelmäßig die Einhaltung des „Standes der Technik“ an der Universitätsmedizin Halle (Saale) durch – geplante und ungeplante – Audits zu überprüfen und entsprechende Anpassungen zu veranlassen. Die konkrete Gestaltung der Audits wird in der Informationssicherheitsrichtlinie 14 dargestellt.
- (2) Um auf neue technische, gesetzliche, organisatorische oder anderweitige Anforderungen reagieren zu können, unterliegt der Informationssicherheitsprozess einer kontinuierlichen Neubewertung.

## § 7 In-Kraft-Treten

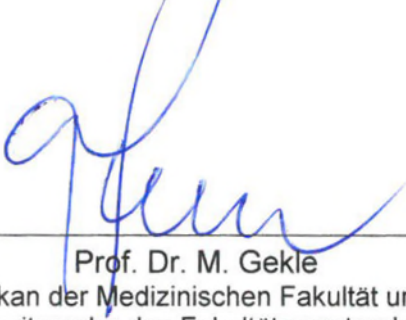
- (1) Diese Leitlinie tritt einen Tag nach Beschlussfassung durch die Vorstandsmitglieder in Kraft.
- (2) Diese Leitlinie wird im Intranet veröffentlicht und ist für alle Beschäftigten der Universitätsmedizin Halle (Saale) verbindlich.
- (3) Dieses Dokument ersetzt die bisher geltende IT-Sicherheitsleitlinie der Universitätsmedizin Halle (Saale).

Halle (Saale), den 27.10.2020




---

Prof. Dr. Th. Moesta  
Ärztlicher Direktor  
und Vorsitzender des Klinikumsvorstandes




---

Prof. Dr. M. Gekle  
Dekan der Medizinischen Fakultät und  
Vorsitzender des Fakultätsvorstandes




---

M. Bohn  
Kaufmännischer Direktor




---

Ch. Becker  
Direktorin des Pflegedienstes

Anlagen:

1. Klassifizierung der Schutzziele; Eigentümerschaft von Daten/Informationen und Anwendungen

### Anlage 1: Klassifizierung<sup>7</sup> der Schutzziele

#### 1) Schutzziel Vertraulichkeit (Confidentiality)

Stufe	Inhalt
-------	--------

sehr hoch	<p><b>Zutreffend:</b> Verwendung besonders schützenswerter Daten/Informationen (nur einem abgegrenzten, namentlich festgelegten Personenkreis zugänglich), deren Missbrauch Gesundheit, Leben oder Freiheit der betroffenen Person bzw. die finanzielle oder marktwirtschaftliche Situation oder die Existenz der UMH erheblich beeinträchtigen kann (z.B. Adressen, Schwachstellen in Konfigurationen)</p> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Existenzielle Beeinträchtigung des Geschäftsablaufs u./o.</li> <li>• Systematische Verletzung von Gesetzen/Regularien mit Geld- und Haftstrafen u./o.</li> <li>• Ggf. Einstellen des Betriebs der UMH durch Verordnung u./o.</li> <li>• Globaler Imageschaden der UMH in der Öffentlichkeit u./o.</li> <li>• Existenzgefährdende/katastrophale finanzielle Auswirkungen [<math>&gt; 10</math> Mio. €]</li> </ul>
hoch	<p><b>Zutreffend:</b> Verwendung (besonders) schützenswerter Daten/Informationen (nur einem dem jeweiligen Zweck zugeordneten Personenkreis zugänglich), deren Missbrauch die betroffene Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen erheblich beeinträchtigen kann (z.B. Aufzeichnungen mit direktem Personenbezug, Konfigurationen, geschäftsstrategische Entscheidungen)</p> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Schwerwiegende Einschränkung des Geschäftsablaufs u./o.</li> <li>• (Wiederholte) Verletzung von Gesetzen/Regularien mit Haftstrafen oder erheblichen Geldbußen u./o.</li> <li>• Regionaler Imageschaden der UMH in der Öffentlichkeit u./o.</li> <li>• Beträchtliche finanzielle Auswirkungen [<math>\leq 10</math> Mio. €]</li> </ul>
mittel	<p><b>Zutreffend:</b> Verwendung (besonders) schützenswerter Daten/Informationen (nur einem dem jeweiligen Zweck zugeordneten Personenkreis zugänglich), deren Missbrauch die betroffene Person in ihrer gesellschaftlichen Stellung oder ihren wirtschaftlichen Verhältnissen beeinträchtigen kann (z.B. Daten/Informationen über Vertragsbeziehungen, Höhe des Einkommens)</p> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Ernsthafte Folgen für den Geschäftsablauf u./o.</li> <li>• Verletzung von Gesetzen/Regularien mit spürbaren Geldbußen/Vertragsstrafen u./o.</li> <li>• Imageschaden der UMH für einzelne Bereiche in der Öffentlichkeit u./o.</li> <li>• Begrenzte/überschaubare finanzielle Auswirkungen [<math>\leq 5</math> Mio. €]</li> </ul>
gering	<p><b>Zutreffend:</b> Verwendung nicht schützenswerter Daten/Informationen (intern keine besonderen Zugangsbeschränkungen), deren Missbrauch zwar keine besondere Beeinträchtigung erwarten lässt, deren Kenntnisnahme jedoch einem unberechtigten Interesse der Einsicht nehmenden Person folgt (z.B. interne Telefonnummern/Zuständigkeiten)</p> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Mäßige Behinderung des Geschäftsablaufs u./o.</li> <li>• Verletzung interner Regularien mit Verwarnungen oder geringen Geldbußen u./o.</li> <li>• Interner Imageschaden der UMH (z.B. Beschäftigte, Partner*innen) u./o.</li> <li>• Mäßige finanzielle Auswirkungen [<math>\leq 3</math> Mio. €]</li> </ul>
sehr gering	<p><b>Zutreffend:</b> Betroffen sind frei zugängliche, nicht schützenswerte Daten/Informationen, in die Einsicht gewährt wird, ohne dass die Einsicht nehmende Person ein berechtigtes Interesse geltend machen muss (z.B. Internetauftritt der UMH, Presseveröffentlichungen)</p> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Leichte Behinderung des Geschäftsablaufs u./o.</li> <li>• Keine Verletzung von Gesetzen/Regularien u./o.</li> </ul>

	<ul style="list-style-type: none"> <li>• Kein Imageschaden der UMH u./o.</li> <li>• Keine oder geringe finanzielle Auswirkungen [&lt; 1 Mio. €]</li> </ul>
--	--

## 2) Schutzziel Verfügbarkeit (Availability)

Stufe	Inhalt
sehr hoch	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Der Prozess zur Patient*innensicherheit/Behandlungseffektivität kann nicht durchgeführt werden</li> <li>• Max. tolerierbare Ausfallzeit: ≤ 12h</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Existenzielle Beeinträchtigung des Geschäftsablaufs u./o.</li> <li>• Systematische Verletzung von Gesetzen/Regularien mit Geld- und Haftstrafen u./o.</li> <li>• Ggf. Einstellen des Betriebs der UMH durch Verordnung u./o.</li> <li>• Globaler Imageschaden der UMH in der Öffentlichkeit u./o.</li> <li>• Existenzgefährdende/katastrophale finanzielle Auswirkungen [&gt; 10 Mio. €]</li> </ul>
hoch	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Der Prozess kann nur mit erheblichen Mehraufwand zur Patient*innensicherheit/Behandlungseffektivität betrieben werden</li> <li>• Max. tolerierbare Ausfallzeit: ≤ 48h</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Schwerwiegende Einschränkung des Geschäftsablaufs u./o.</li> <li>• (Wiederholte) Verletzung von Gesetzen/Regularien mit Haftstrafen oder erheblichen Geldbußen u./o.</li> <li>• Regionaler Imageschaden der UMH in der Öffentlichkeit u./o.</li> <li>• Beträchtliche finanzielle Auswirkungen [≤ 10 Mio. €]</li> </ul>
mittel	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Der Prozess kann mit tolerierbarem Mehraufwand zur Patient*innen-sicherheit/Behandlungseffektivität betrieben werden• Max. tolerierbare Ausfallzeit: ≤ 1 Woche</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Ernsthafte Folgen für den Geschäftsablauf u./o.</li> <li>• Verletzung von Gesetzen/Regularien mit spürbaren Geldbußen/Vertragsstrafen u./o.</li> <li>• Imageschaden der UMH für einzelne Bereiche in der Öffentlichkeit u./o.</li> <li>• Begrenzte/überschaubare finanzielle Auswirkungen [≤ 5 Mio. €]</li> </ul>
gering	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Kaum spürbarer Mehraufwand zum Betreiben des Prozesses zur Patient*innensicherheit/ Behandlungseffektivität</li> <li>• Max. tolerierbare Ausfallzeit: ≤ 1 Monat</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Leichte bis mäßige Behinderung des Geschäftsablaufs u./o.</li> <li>• Verletzung interner Regularien mit Verwarnungen oder geringen Geldbußen u./o.</li> <li>• Interner Imageschaden der UMH (z.B. Beschäftigte, Partner*innen) u./o.</li> <li>• Mäßige finanzielle Auswirkungen [≤ 3 Mio. €]</li> </ul>
sehr gering	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Keine relevanten Auswirkungen auf den betroffenen Prozess zur Patient*innensicherheit/ Behandlungseffektivität</li> <li>• Max. tolerierbare Ausfallzeit: ≤ 6 Monate</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Keine Behinderung des Geschäftsablaufs u./o.</li> <li>• Keine Verletzung von Gesetzen/Regularien u./o.</li> </ul>

	<ul style="list-style-type: none"> <li>• Kein Imageschaden der UMH u./o.</li> <li>• Keine oder geringe finanzielle Auswirkungen [&lt; 1 Mio. €]</li> </ul>
--	--

### 3) Schutzziel Integrität (Integrity)

Stufe	Inhalt
sehr hoch / hoch	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Eine Kompromittierung von Daten/Informationen u./o. IT-Systemen hat stattgefunden</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Leichte bis existenzgefährdende/katastrophale Beeinträchtigung des Geschäftsablaufs u./o.</li> <li>• Verletzung von Gesetzen/ Regularien mit möglichen Geldbußen, Haft- u./o. Geldstrafen zur Folge u./o.</li> <li>• Imageschaden der UMH (in der Öffentlichkeit) u./o.</li> <li>• Leichte bis existenzgefährdende/katastrophale finanzielle Auswirkungen[n/a €]</li> </ul>

### 4) Schutzziel Authentizität (Authenticity)

Stufe	Inhalt
sehr hoch / hoch	<p><b>Zutreffend:</b></p> <ul style="list-style-type: none"> <li>• Die Herkunft bzw. angegebene Quelle von Daten/Informationen u./o. IT-Systemen ist nicht eindeutig bzw. nicht sicher nachvollziehbar und nicht zuordenbar u./o.</li> <li>• Die Identität der Kommunikationspartner*innen ist nicht sichergestellt bzw. nicht eindeutig</li> </ul> <p><b>Kann zutreffen:</b></p> <ul style="list-style-type: none"> <li>• Leichte bis existenzgefährdende/katastrophale Beeinträchtigung des Geschäftsablaufs u./o.</li> <li>• Verletzung von Gesetzen/ Regularien mit möglichen Geldbußen, Haft- u./o. Geldstrafen zur Folge u./o.</li> <li>• Imageschaden der UMH (in der Öffentlichkeit) u./o.</li> <li>• Leichte bis existenzgefährdende/ katastrophale finanzielle Auswirkungen [n/a €]</li> </ul>

#### Informationseigentümer\*in:

Informationseigentümer\*innen sind die Ersteller\*innen eines Datums oder einer Information oder diejenigen, denen ein Datum oder eine Information zur weiteren Bearbeitung zur Verfügung gestellt wird. Sie legen fest, ob und wer Zugriff auf die ihnen anvertrauten Daten oder Informationen bekommen soll. Dieser Zugriff auf Daten oder Informationen wird – üblicherweise – durch Anwendungen oder Software ermöglicht.

#### Anwendungseigentümer\*in:

Anwendungseigentümer\*innen sind die Nutzer\*innen der Anwendungen oder Software, die zur Erfassung, Weiterverarbeitung oder Auswertung eines Datums oder einer Information eingesetzt werden. Sie legen fest, ob und wer Zugriff auf Anwendungen oder Software und damit auf die, durch die Anwendungen oder Software verarbeiteten und gespeicherten Daten oder Informationen bekommen soll. Dieser Zugriff wird durch die, die Anwendung oder Software administrierende Person, bei zentral administrierten Lösungen durch ZD1-luK oder ZD14-Technik, erteilt.

Insoweit gehen Zugriff auf Daten/Informationen und Anwendungen/Software häufig zusammen. Informations- und Anwendungseigentümer\*innen im Sinne der Festlegung von Schutzklassen und der Bewertung der Einhaltung/Nichteinhaltung der Schutzklassen in den Schutzzielen ist die jeweilige Einrichtungsleitung.

#### Informationstreuhänder\*in:

Informationstreuhänder\*innen sind für die Verwaltung oder Verarbeitung der Daten oder Informationen zuständig. Dabei sind sie für die Einhaltung der Vorgaben durch die Informationseigentümer\*innen/ Anwendungseigentümer\*innen verantwortlich. Informationstreuhänder\*innen sind – üblicherweise – die

interne IT (ZD1-luK, ZD14-Technik) oder ein\*e externe\*r Dienstleistende\*r. Bei selbstverwalteten IT-Systemen der Einrichtungen können Informationseigentümer- und -treuhänderschaft zusammenfallen.

#### Anwender\*in (Nutzer\*in):

Anwender\*innen verpflichten sich zum bestimmungsgemäßen, zweckgebundenen und sicherheitsbewussten Umgang mit den ihnen anvertrauten und zur Verfügung gestellten Daten und Informationen gemäß den Vorgaben der Informationseigentümer\*innen.

<sup>1</sup> Zu unterscheiden ist zwischen Informationssicherheit und IT-Sicherheit. Die erste ist Obermenge der zweiten; Informationssicherheit als Erweiterung zu IT-Sicherheit wird hier betrachtet (umfasst zusätzlich z.B. Papierarchive und -registraturen, d.h. „analog“ gespeicherte und verfügbare Informationen und/oder Informationen in mündlicher Form).

<sup>2</sup> Der Schutzbedarf ist eine objektive Größe; dieser muss – nach der Strukturanalyse – im Rahmen einer Schutzbedarfsfeststellung für

- **Daten/Informationen:** d.h. für sämtliche Datenbestände, unabhängig von deren Struktur ermittelt werden. Beispiele: Patient\*innendaten (ORBIS), Mitarbeiter\*innendaten, Beschaffungs- und Verwaltungsdaten, auch technische Daten (Facility Management, AD, LDAP, etc.)

Zur Ermittlung des Schutzbedarfs von Informationen ist die Definition einer „Informationseigentümerschaft“ (analog „Risikoeigentümerschaft“) sehr hilfreich

- **Anwendungen:** d.h. sämtliche Programme, Anwendungen und Software
- **IT-Systeme** (PC's, Notebooks, Server, Netzkomponenten, [vernetzte] Medizintechnik, etc.)
- **Räume** (mit „IT“, Daten, Informationen oder auch nur einer LAN-Dose)

bestimmt werden.

<sup>3</sup> Der „Stand der Technik“ ist im IT-SiG gefordert und in einer Handreichung des TeleTrusT (relativ präzise) beschrieben. Der „Branchenspezifische Sicherheitsstandard“ (B3S) liegt aktuell in der vom BSI freigegebenen Version 1.1 vor.

<sup>4</sup> Personenbezogene Daten/Informationen sind alle Daten/Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Unter sachbezogenen Daten/Informationen werden Daten/Informationen verstanden, die Tatsachen oder Bewertungen von Sachverhalten sind (z.B. Geschäftsgeheimnisse, Aktivierungszeiträume). Schützenswert sind alle Daten/Informationen, die isoliert oder durch eine Verknüpfung mit weiteren Informationen und damit verbundener Ausnutzung Schaden verursachen können – unabhängig davon, ob es sich um personenbezogene oder sachbezogene Daten/Informationen handelt. Als schützenswert werden im Geltungsbereich der Informationssicherheit "Universitätsmedizin Halle (Saale)" alle Daten/Informationen betrachtet, die personen- bzw. zum Schutz der Einrichtung dienlich sachbezogen sind. Aufgrund der Partnerschaften/Vertragsbeziehungen mit Dritten sollen ebenso schützenswerte Daten/Informationen von Unternehmen bzw. des eigenen Unternehmens, d.h. juristischen Personen, einbezogen werden; somit auch schützenswerte betriebswirtschaftliche bzw. Compliance-bezogene Daten/Informationen. Als besonders schützenswert gelten gemäß § 46 Ziffer 14 a-e BDSG-neu, vgl. auch Art. 4, 9 DSGVO Daten/Informationen, die Auskunft über die ethnische und kulturelle Herkunft, politische, religiöse und philosophische Überzeugungen, Gesundheit, Sexualität und Gewerkschaftszugehörigkeit sowie Genetik und Biometrie geben.

<sup>5</sup> Es sollte klar ersichtlich werden, dass:

- eine **Informationssicherheitsorganisation** aufgebaut und „betrieben“ wird,
- eine **Sicherheitskonzeption** erstellt, umgesetzt und betrieben/vorangetrieben (Aufrechterhaltung und Verbesserung) wird.

**Die Gesamtheit, bestehend aus dem Sicherheitsprozess** (dieser wiederum bestehend aus der vorliegenden Leitlinie, einem Sicherheitskonzept [incl. der Umsetzung desselben] einerseits, sowie einer Informationssicherheits-Organisation), **Mitarbeiter\*innen** (für das SG Informationssicherheit, bei ZD1-luK und für die Umsetzung der „Projekte“ aus dem Sicherheitskonzept), **Ressourcen** (hier: Budget, Zeit) **sowie allgemeinen Management-Prinzipien bilden das ISMS**, dessen Wirksamkeit (außerdem) nachgewiesen werden muss, z.B. durch jährliche Kontrollen/Audits/Pentests etc., welche in einen kontinuierlichen Verbesserungsprozess münden!

<sup>6</sup> Die Erfahrung zeigt, dass bei/nach der Einführung standardisierter Informationssicherheit die Anforderungen an die IT hinsichtlich Logging-Auswertung, Identity-/Zugriffs-Management (need-to-know-Prinzip), IT-Sicherheits-Dienstleistungen (u.a. Passwort-Rücksetzungen, Daten-Im und Export), usw. steigen.

<sup>7</sup> Die Schadenspotentiale basieren auf Informationssicherheitsrisiken. Die Erfassung und das Management der Informationssicherheitsrisiken der Universitätsmedizin Halle (Saale) finden Eingang in die Erfassung und das Management der unternehmensweiten Risiken der Universitätsmedizin Halle (Saale). Der Umgang mit Informationssicherheits- sowie unternehmensweiten Risiken ist in der Risikostrategie/SOP zum Umgang mit Informationssicherheitsrisiken der Universitätsmedizin Halle (Saale) beschrieben.