Informationssicherheitsleitlinie der Universitätsmedizin Magdeburg (UMMD)

Stand: 25.01.2023

Verteiler: UMMD

Vertraulichkeitsstufe: Öffentlich

Hinweis: Alle Status-, Stellen- und Funktionsbezeichnungen gelten für alle Geschlechter.

Inhalt

Abkürzungsverzeichnis

DSB ..... Datenschutzbeauftragte

EU-DS-GVO ..... EU-Datenschutzgrundverordnung

FME ..... Medizinische Fakultät der Otto-von-Guericke-Universität

ISB ..... Informationssicherheitsbeauftragte

ISMS ..... Managementsystem der Informationssicherheit

KPI ..... Key Performance Indicator (Kennzahlen zur Messung des Erfüllungsgrades bestimmter Geschäftsziele)

PDCA ..... Plan-Do-Check-Act Zyklus

UKMD ..... Universitätsklinikum Magdeburg A. ö. R.

UMMD ..... Universitätsmedizin Magdeburg

V2 ..... Vorstandsbereich „Informationssicherheit“

1 Generelle Informationen

1.1 Erfüllung von Normanforderungen

Auf dieses Dokument werden folgende Maßnahmen der ISO-Normen angewendet.

DIN ISO/IEC 27001:2017

Maßnahme	Beschreibung
A.5.1.1	Informationssicherheitsrichtlinien
A.5.1.2	Überprüfung der Informationssicherheitsrichtlinien
A 6.1.5	Informationssicherheit im Projektmanagement

1.2 Mitgeltende Unterlagen

[1] 4110_ND_Anwendungsbereich

[2] 1013_LL_ISMS-Team_Geschäftsordnung

[3] 1011_LL_Dokumentenlenkung

[4] DV 1/2017 Dienstvereinbarung zur beruflichen Fort- und Weiterbildung

[5] Protokoll der jährlichen Tagung der Investitionskommission

[6] Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz, 17.07.2015)

[7] Kennzahlen-Konzept der Informationssicherheit (Key Performance Indicator (KPI))

[8] Strategie der UMMD (04.07.2018)

[9] 2037_RL_Schulung_Sensibilisierung

[10] 2020_RL_Kontaktliste_Networking.docx

[11] Datenschutzkonzept der UMMD

[12] Branchenspezifischer Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S)

2 Unternehmen und Geschäftszweck

Das Universitätsklinikum Magdeburg A. ö. R. (UKMD) ist eine rechtlich selbständige juristische Person des öffentlichen Rechts, die in enger Verflechtung mit der Medizinischen Fakultät der Otto-von-Guericke-Universität (FME) die Universitätsmedizin Magdeburg (UMMD) repräsentiert. Das UKMD hat den gesetzlichen Auftrag des Landes Sachsen-Anhalt (Krankenhausgesetz Sachsen-Anhalt, KHG LSA) zur medizinischen Krankenversorgung an den Standorten Leipziger Straße 44 und der Gerhard-Hauptmann-Str.35. Die Aufgaben der Forschung und Lehre gehören zur FME, ebenso wie ein Großteil des wissenschaftlich tätigen ärztlichen Personals. Die Kliniken und krankenversorgenden Institute agieren bei der Krankenversorgung weitestgehend selbständig. Sie unterstützen sich hierbei gegenseitig und werden von den zentralen Einrichtungen der UMMD hinsichtlich Personal, Ressourcen oder bspw. betriebswirtschaftlicher Aspekte unterstützt.

Die UMMD ist bestrebt eine moderne und innovative Organisation zu sein, welche exzellente Ergebnisse in Forschung, Lehre und Krankenversorgung erbringt. Dafür müssen sich die Geschäftsprozesse der UMMD schnell und agil an sich verändernde Markt- und Gesetzesanforderungen anpassen [8]. Das hier beschriebene Managementsystem der Informationssicherheit (ISMS) betrifft daher alle Geschäftsprozesse der UMMD im Allgemeinen mit Hauptfocus auf die vollstationäre Krankenversorgung (siehe Abschnitt 3).

3 Anwendungsbereich

Zur Umsetzung der Leitlinie hat die UMMD ein Managementsystem der Informationssicherheit (ISMS) eingeführt. Das ISMS beruht auf dem internationalen Standard ISO/IEC 27001.

Mit dem ISMS soll sichergestellt werden, dass alle Prozesse, die Auswirkungen auf die Informationssicherheit haben, durchgängig geplant, gesteuert und überwacht werden. Das betrifft alle Informationen, die für die medizinische Versorgung unserer Patienten notwendig sind.

Hauptfokus des ISMS liegt auf der Absicherung der vollstationären medizinischen Versorgung, die das UKMD als kritische Infrastruktur, nach dem IT-Sicherheitsgesetz [6] umsetzen muss. Hierbei werden je nach Kritikalität digitale Dienstleistungen abgesichert. Die Einstufung der Kritikalität der eingesetzten Systeme wird durch die ISB unterstützt durch das ISMS-Team vorgenommen.

Für Mitarbeiter der FME gilt diese Leitlinie ebenso, wenn Sie bei Ihren Forschungsaktivitäten Zugriff auf Informationen der UKMD erhalten und diese verarbeiten.

So erfüllt die UMMD die definierten Anforderungen, wie sie durch unsere Patienten und in Form von Gesetzen, Regelwerken oder sonstigen Vorschriften an uns herangetragen werden.

4 Geltungsbereich

Die vorliegende Leitlinie zur Informationssicherheit gilt verbindlich für alle Beschäftigten des Universitätsklinikums Magdeburg A.ö.R. und der Medizinischen Fakultät der Otto-von-Guericke-Universität Magdeburg, sofern ein Zugriff auf Informationen und die Verarbeitung von Informationen der UKMD erfolgt. Detaillierte Arbeits- und Dienstanweisungen sowie Dienstvereinbarungen, die auf die vorliegende Leitlinie Bezug nehmen, gelten gleichfalls für alle Beschäftigten des Universitätsklinikums Magdeburg A.ö.R. und der Medizinischen Fakultät der Otto-von-Guericke-Universität Magdeburg, sofern in dem Dokument nichts Abweichendes geregelt wird.

Die Leitlinie gilt auch für die gesellschaftsrechtlich verbundenen Einrichtungen (z.B. Tochtergesellschaften) und für vertraglich verbundene Unternehmen, die eine Auftragsverarbeitung für das Universitätsklinikum Magdeburg erbringen. Für diese Unternehmen wird die Informationssicherheitsleitlinie zum Vertragsbestandteil.

5 Stellenwert der Informationssicherheit

Die Informationssicherheit hat einen großen Stellenwert für die UMMD, da fast alle Prozesse der medizinischen Versorgung von der störungsfreien Speicherung, Verarbeitung und Kommunikation von digitalen und analogen Informationen abhängig sind. Das Ziel der Informationssicherheit ist der Schutz von Informationen jeglicher Art und Herkunft. Das sind beispielsweise Informationen auf Papier oder digital wie in Rechnersystemen oder mobilen Geräten.

Somit unterstützt die Umsetzung der Informationssicherheit die Patientensicherheit und Behandlungseffektivität. Beide Vorstände der UMMD, der Klinikumsvorstand und der Vorstand der medizinischen Fakultät, bekennen sich zu den Zielen der Informationssicherheit der UMMD *(Abschnitt 6)*. Sie unterstützten aktiv und in allen Belangen die Organisation und Umsetzung der Informationssicherheit in der UMMD, was einen kontinuierlichen Sicherheitsprozess gewährleistet.

Jeder Beschäftigte der UMMD muss sich der Notwendigkeit der Informationssicherheit bewusst sein bzw. die Sicherheitsziele der UMMD kennen und in seinem Arbeitsumfeld anwenden können. Dafür muss jeder Beschäftigte jährlich an Schulungen zum Datenschutz und der Informationssicherheit teilnehmen [9].

6 Anforderungen und Ziele der Informationssicherheit

Das Vertrauen unserer Patienten und Mitarbeiter beruht darauf, dass wir:

- gesetzliche Vorgaben und insbesondere die datenschutzrechtlichen Bestimmungen einhalten,
- unsere Betriebsgeheimnisse schützen,
- die Vertraulichkeit der Daten unserer Patienten und Mitarbeiter wahren.

Für die UMMD werden folgende vier Ziele der Informationssicherheit festgelegt:

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Daten und Informationen. Nur berechtigte Personen dürfen auf vertrauliche Daten und Informationen zugreifen.

Integrität

Integrität stellt sicher, dass Daten und Informationen korrekt verarbeitet werden bzw. Systeme und Anwendungen wie vorgesehen funktionieren. Die Unversehrtheit von Systemen, Anwendungen sowie Daten und Informationen muss jederzeit gewahrt sein. Nur berechtigte Personen dürfen Daten und Informationen verändern. Fehlerhafte Daten und Informationen sind zu korrigieren bzw. deren Korrektur ist zu veranlassen.

Verfügbarkeit

Genutzte Systeme, Anwendungen, Daten und Informationen müssen allen Berechtigten wie vorgesehen jederzeit zur Verfügung stehen.

Authentizität

Die Echtheit von Daten und Informationen muss sichergestellt sein. Die Authentizität wird anhand einer eindeutigen Identität und bestimmter Eigenschaften überprüft. Nur berechtigte Personen dürfen Daten und Informationen erstellen und weiterleiten.

Die Umsetzung dieser vier Ziele unterstützt die Umsetzung von gesetzlichen Anforderungen der UMMD im Speziellen die Patientensicherheit und Behandlungseffektivität der medizinischen Versorgung der UKMD.

Die genaue Messbarkeit von Zielen der Informationssicherheit wird in einem eigenen Konzept beschrieben [7].

7 Kernelelemente der Sicherheitsstrategie

Folgende Punkte beschreiben die Kernelemente der Sicherheitsstrategie der UMMD:

- Körperliche Unversehrtheit von Patienten, sowie Mitarbeitern und Dienstleistern, sofern diese im Einflussbereich der UMMD tätig sind
- Erfüllung rechtlicher und vertraglicher Anforderungen
- Wahrung der Vertraulichkeit von Informationen der UMMD sowie die unserer Geschäftspartner über alle Kommunikationsschnittstellen hinweg
- Sicherstellung und Wahrung der Integrität und Authentizität von Informationen (insbesondere von Gesundheitsdaten)
- Aufrechterhaltung einer wirksamen betrieblichen Geschäftskontinuität inklusive der Verfügbarkeit von Informationen (insbesondere von Gesundheitsdaten)
- Aufrechterhaltung eines hohen Bewusstseins für die Informationssicherheit und des Datenschutzes in allen Bereichen
- Bekenntnis zur kontinuierlichen Verbesserung der Geschäftsprozesse
- Pflege eines wirksamen Risikomanagementsystems
- Schaffung von Transparenz und Vertrauen gegenüber Patienten, Kooperationspartnern, Mitarbeitern und sonstigen Dritten bei der Verarbeitung personengebundener Daten
- Anerkennung des Persönlichkeitsrechts und der digitalen Selbstbestimmung aller Betroffenen bei der Verarbeitung personenbezogener Daten
- Einbindung interessierter Parteien [11]

8 Organisationsstruktur für Informationssicherheit

Beide Vorstände der UMMD verantworteten die Informationssicherheit des Universitätsklinikums. Sie werden dabei von einem ISMS-Team unterstützt, das von der Informationssicherheitsbeauftragten (ISB) geleitet wird [2].

Die Informationssicherheitsbeauftragte ist dem Vorstandsbereich „Informationssicherheit“ (V2) und damit unmittelbar beiden Vorständen zugeordnet. Die ISB steuert den Informationssicherheitsprozess und überwacht, dass die in dieser Leitlinie beschriebenen übergeordneten Ziele geeignet und wirtschaftlich innerhalb der UMMD umgesetzt werden. In diesem Prozess arbeitet die ISB eng mit der Datenschutzbeauftragten zusammen.

Beim Projektmanagement muss die Informationssicherheit unabhängig von der Projektart bei Projektbeginn durch Einbindung der ISB berücksichtigt werden. Kriterien für die Einbindung der ISB sind im Projektmanagementhandbuch & UMMD-Prozess-Wiki ersichtlich.

Mechanismen zur Umsetzung der Informationssicherheit an der UMMD werden regelmäßig in einem ISMS-Tool nach dem PDCA-Zyklus (Plan-Do-Check-Act) geplant, umgesetzt, kontrolliert und behandelt.

9 Verantwortlichkeiten im ISMS

Im Folgenden werden die Verantwortlichkeiten im Informationssicherheitsmanagementsystem (ISMS) an der UMMD beschrieben [1]. Dabei werden bestimmte Rollen mit verschiedenen Aufgaben unterschieden.

9.1 Vorstände

Verantwortlich für die Informationssicherheit an der UMMD sind beide Vorstände, der Klinikumsvorstand (KliVo) und der Fakultätsvorstand (FaVo).

9.2 Informationssicherheitsbeauftragte (ISB)

Beide Vorstände übertragen diese Aufgabe an die Informationssicherheitsbeauftragte (ISB), die im Namen beider Vorstände die Umsetzung der Informationssicherheit in der UMMD steuert, weiterentwickelt und überprüft *(detaillierte Aufzählung der Aufgaben/Befugnisse – siehe Kapitel 10)*.

9.3 IT-Sicherheitsmanager (ITSM)

Ein IT-Sicherheitsmanager (ITSM) ist im Geschäftsbereich ITMT etabliert worden. Fokus des ITSM ist die IT-Sicherheit in der Gesamtheit ihrer technischen Aspekte und über alle Abteilungs- und Verantwortungsgrenzen innerhalb des Bereichs IT und Medizintechnik hinweg und damit der gesicherte Betrieb der IT-Systeme und der Schutz der darin enthaltenen digitalen Daten des UKMD. Der ITSM arbeitet eng mit der ISB zusammen und stimmt sich mit ihr hinsichtlich IT-Sicherheit ab *(detaillierte Aufzählung der Aufgaben/Befugnisse – siehe Kapitel 10)*.

9.4 Team der Informationssicherheit (ISMS-Team)

(1) Neben der ISB und den Mitarbeitern des Vorstandsbereichs 2 gibt es ein Team der Informationssicherheit (ISMS-Team) an der UMMD, das von der ISB geleitet wird. Das ISMS-Team unterstützt die ISB bei ihrer Tätigkeit *(detaillierte Aufzählung der Aufgaben/Befugnisse – siehe Kapitel 11)*. Das Team gibt sich eine Geschäftsordnung [2].

(2) Insbesondere soll über folgende Angelegenheiten beraten werden:

- Allgemeine Themen der Informationssicherheit,
- Beobachtungen, die Störungen im Betriebsablauf oder Sicherheitsrisiken verursachen [3],
- Änderungen bzw. Neuerungen die Auswirkungen auf die Ziele der Informationssicherheit der UMMD haben (z.B. durch Einführung, Erweiterung und Änderungen von IT- und medizintechnischen Systemen) [4],
- Einsatz von Investitionen für die Umsetzung der Informationssicherheit an der UMMD,
- Anfragen von Mitarbeitern, die Themen des ISMS-Teams berühren.

(3) Die Mitglieder des ISMS-Teams sind berechtigt, jederzeit die erforderlichen Auskünfte einzuholen. Alle Mitarbeiter und entsprechenden Struktureinheiten der UMMD sind verpflichtet, diese zu erteilen *(siehe Kapitel 2.2)*.

(4) Das ISMS-Team an der UMMD setzt sich aus den folgend genannten Mitgliedern zusammen.

- Die **Informationssicherheitsbeauftragte (ISB)** ist für alle Fragen zur Informationssicherheit in der UMMD zuständig. Die ISB ist als Leiterin des Vorstandsbereichs Informationssicherheit organisatorisch unabhängig und den Vorständen gegenüber unmittelbares Vortragsrecht.

- Weiterhin gehört dem Team der Leiter des Geschäftsbereichs IT und Medizintechnik (ITMT) und stellvertretend der ITSM an.

- Die **Datenschutzbeauftragte (DSB)** ist im ISMS-Team für alle Fragen rund um den Schutz personenbezogener Daten zuständig.

(5) Die **Vertreter beider Personalräte** der UMMD sind dauerhaft als Gäste geladen. Die gesetzlichen Regelungen des Landespersonalvertretungsgesetz Sachsen-Anhalt und insbesondere ihr Mitbestimmungsrecht in Technologieangelegenheiten entsprechend §69 Landespersonalvertretungsgesetz Sachsen-Anhalt bleiben gewahrt.

9.4.1 Vorsitz und Stellvertreter

(1) Die Vorsitzende des ISMS-Teams wird durch beide Vorstände der UMMD, dem KliVo und dem FaVo, benannt. Derzeit leitet die ISB das ISMS-Team.

(2) Stellvertreter ist ein von der Vorsitzenden benannter Mitarbeiter aus dem Vorstandsbereich „Informationssicherheit“. Der Benennung haben die Vorstände zuzustimmen.

(3) Die Vorstände können aus begründetem Anlass die Benennung des Vorsitzenden sowie seine Zustimmung zur Person des Stellvertretenden widerrufen und ein neues ISMS-Team benennen.

Auch soweit es in der Geschäftsordnung [2] nicht ausdrücklich bestimmt ist, darf der Stellvertreter in jeglichem Verhinderungsfall der Vorsitzenden des ISMS-Teams deren Pflichten und Rechte vollumfänglich stellvertretend wahrnehmen bzw. ausüben.

9.5 Leiter der Struktureinheiten

Jeder Leiter hat die Aufgabe, die Mitarbeiter seiner Struktureinheiten für die Einhaltung der Informationssicherheit entsprechend der Richtlinien zu sensibilisieren. Weiterhin sollen Leiter so früh wie möglich die ISB und DSB in Projekte einbinden, damit Sicherheitsmaßnahmen des Datenschutzes und der Informationssicherheit rechtzeitig bewertet und umgesetzt werden können.

9.6 Datenschutzkoordinatoren

Die Datenschutzkoordinatoren an der UMMD haben neben ihren im Datenschutzkonzept [11] genannten Aufgaben zum Schutz von personenbezogenen Daten, auch den Schutz von Betriebsgeheimnissen zu beachten und Vorfälle hinsichtlich der Informationssicherheit der ISB zu melden.

10 Aufgaben und Befugnisse der Informationssicherheitsbeauftragten

Im Folgenden werden die Aufgaben und die Befugnisse der ISB und der Mitglieder des ISMS-Teams beschrieben.

10.1 Aufgaben der Informationssicherheitsbeauftragten

(1) Die ISB ist für alle Fragen zur Informationssicherheit in der UMMD zuständig. Die ISB ist als Leiterin des Vorstandsbereichs Informationssicherheit fachlich unabhängig und hat den Vorständen gegenüber unmittelbares Vortragsrecht.

(2) Ihre Hauptaufgaben sind:

- Aufbau, Betreuung und Weiterentwicklung eines Informationssicherheitsmanagementsystems (ISMS) gemäß ISO/IEC 27001 sowie entsprechend der zusätzlichen Anforderungen, die sich aus dem IT-Sicherheitsgesetz ergeben
- Erstellung, Koordination und Genehmigung bereichsübergreifender Regelungen zum ISMS sowie Vorgaben für den Betrieb des ISMS
- Überwachung von Maßnahmen und relevanten Prozessen; Entscheidung bei Fragen der Informationssicherheit
- Überprüfung der Erreichung der Informationssicherheitsziele
- Bewertung von Sicherheitsaspekten in Projekten
- Verteilung und Aktualisierung des Managementhandbuchs Informationssicherheit
- Durchführung interner und Koordinierung externer Audits zur Überprüfung der Wirksamkeit des ISMS
- Koordinierung der Durchführung sowie Auswertung der Risikoanalyse; Erstellen von Risikobehandlungsplänen
- Unterstützung bei der Auswertung und Verfolgung von Sicherheitsvorfällen im Rahmen der Eskalation und Wahrnehmung von Meldepflichten gegenüber Behörden (BSI)
- Verbesserung des Sicherheitsbewusstseins mittels Durchführung von (internen) Schulungen und Sicherheitsaudits und Beratung aller Abteilungen in Fragen der Informationssicherheit
- Beantwortung von Fragen zum ISMS, die seitens interessierter Dritter gestellt werden

- Erarbeitung von Vorschlägen zur Risikominimierung an die Vorstände
- Jährliche Berichterstattung an die Vorstände (Managementreview)
- Berichtsprozess gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gemäß den Vorgaben des IT-Sicherheitsgesetzes
- Zusammenarbeit mit der DSB
- Leitung des ISMS-Teams

10.2 Befugnisse der Informationssicherheitsbeauftragten

(1) Die ISB ist in allen für die Informationssicherheit relevanten Themen zu informieren (sowohl auf Nachfrage als auch unaufgefordert, soweit eine Relevanz für die Informationssicherheit besteht).

(2) Vorhaben und Änderungen, die die Informationssicherheit berühren können, müssen frühzeitig mit der ISB abgestimmt werden. Beispiele sind neue IT-Projekte, Änderungen der IT-Infrastruktur und Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit.

(3) Die ISB hat ein Mitspracherecht bei allen Entscheidungen die ihren Verantwortungsbereich betreffen (z. B. bei der Initiierung von IT-Projekten, Beschaffung von informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern).

(4) Die ISB hat direktes Vortragsrecht gegenüber beiden Vorständen.

(5) Die ISB hat Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängende Daten verarbeitet werden, und zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden.

(6) Die ISB hat im Rahmen ihrer Tätigkeit ein zeitlich, auf die Dauer der wahrzunehmenden Aufgabe, begrenztes Zugriffsrecht auf alle betroffenen IT-Systeme und damit verarbeitete Daten. Je nach Art der Daten muss sie sich hierzu vorab mit der DSB und den Personalräten (PR) abstimmen.

(7) Die ISB führt Revisionen/Audits im Themenbereich der Informationssicherheit durch bzw. veranlasst Revisionen/Audits durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in ihrem Aufgabenbereich.

(8) Die ISB vertritt die UMMD im Bereich des ISMS und ist gegenüber beiden Vorständen berichtspflichtig.

10.3 Aufgaben und Befugnisse des IT-Sicherheitsmanagers

(1) Der ITSM hat die IT-Sicherheit in der Gesamtheit ihrer technischen Aspekte und über alle Abteilungs- und Verantwortungsgrenzen innerhalb des Bereichs IT und Medizintechnik im Blick.
(2) Der ITSM berät alle Bereiche der UMMD zu Themen der IT-Sicherheit.
(3) Der ITSM unterstützt insbesondere die ISB bei ihrer Arbeit im Hinblick auf IT-Sicherheit.

(4) Der ITSM koordiniert die Durchführung von IT-Schwachstellenscans und unterstützt bei externen Penetrationstests.

11 Aufgaben und Befugnisse der Mitglieder des ISMS-Teams

Die Mitglieder des ISMS-Teams unterstützen die ISB bei ihrer Tätigkeit, zum Beispiel:

- durch regelmäßige Teilnahme an den Beratungen des ISMS-Teams
- Planung und Organisation der Informationssicherheit
- Unterstützung bei der Planung und Durchführung der Risikoanalyse
- Erstellung, Koordination und Genehmigung bereichsübergreifender Regelungen zum Informationssicherheitsmanagementsystem sowie von Vorgaben für den Betrieb des ISMS
- Bewertung von Sicherheitsaspekten in Projekten
- Erarbeitung von Vorschlägen zur Risikominimierung für die Vorstände der UMMD

Hierfür sind den Mitgliedern des ISMS-Teams sämtliche benötigten Zugriffe und Zugänge zu relevanten – für die Stelle und Aufgaben notwendigen – IT-Systemen/Software zur Verfügung zu stellen.

12 Fort- und Weiterbildung

(1) Zur fortwährenden Erfüllung der Aufgaben der ISB und ihrer Mitarbeiter ist eine ständige Fort- und Weiterbildung für den Vorstandsbereich V2 zu gewährleisten [4].
(2) Fort- und Weiterbildungen sind durch den Bereich eigenständig zu planen und die Beantragung der finanziellen Mittel in die Finanzplanung aufzunehmen.
(3) Zu Fort- und Weiterbildungsmaßnahmen zählt ebenfalls der aktive Austausch mit Informationssicherheitsbeauftragten und die Teilnahme an Kongressen bzw. Seminaren zu Themen, wie beispielsweise der Informationssicherheit und zum aktuellen Stand der Technik.

13 Mittelbereitstellung

(1) Dem Vorstandsbereich V2 sind für die Wahrnehmung und Erfüllung der übertragenen Aufgaben entsprechende finanzielle und personelle Mittel zur Verfügung zu stellen.
(2) Die ISB selbst meldet gemäß dem Prozess zur Finanzplanung die Mittel (Investitions- und Personalkosten) entsprechend an [5].
(3) Die ISB überwacht den Einsatz von finanziellen Mitteln als Investitionen zur Verbesserung der Informationssicherheit an der UMMD und stimmt sich dazu innerhalb des ISMS-Teams ab (*s. Abschnitt 9.3*).

14 Verbindlichkeitserklärung und Inkrafttreten

Beide Vorstände der UMMD genehmigen hiermit die an den neusten Stand angepasste Leitlinie. Beide Vorstände weisen hiermit an, dass dem Informationssicherheitsmanagementsystem von allen Mitarbeitern in allen Ebenen der UMMD zu folgen ist.

Magdeburg, den 13.02.2023

Prof. Dr. Daniela C. Dieterich

Dekanin

Prof. Dr. med. Hans-Jochen Heinze

Ärztlicher Direktor

Prof. Dr. med. Maciej Pech

Prodekan für Struktur

Marco Bohn

Kaufmännischer Direktor

Prof. Dr. med. Florian Junne

Prodekan für Forschung

Christine Michelfeit-Schaper

Pflegedirektorin

Prof. Dr. med. Roland Croner

Prodekan für Klinische Angelegenheiten

Prof. Dr. med. Christoph H. Lohmann

Studiendekan