

1 Krankenhausführung / 1.09 Informationssicherheit

Leitlinie für Informationssicherheit und Datenschutz

Version	Änderungen gegenüber der letzten Fassung:
15	Neu: MediGate (vorher Stabstelle Forschungsdatenschutz), Ergänzung vom 06.06.2025: neue Anlage 05 Organisation des Informationssicherheitsprozesses
14	Neue Anlage 04 Auditplan Informationssicherheit
13	Initiale Neufassung nach neuer Struktur des ISMS (ehem. QMH 5.10.01 v12) und Ergänzung der Anlagen 01 - 03

1 Ziel und Zweck

Diese Leitlinie für Informationssicherheit und Datenschutz gewährleistet die strategische Ausrichtung in Bezug auf sämtliche Aspekte der Informationssicherheit und des Datenschutzes und gibt den Rahmen für die Ziele der Informationssicherheit und des Datenschutzes vor. Die operativen Ziele der Informationssicherheit leiten sich daraus ab und sind in Anlage 03 festgelegt.

2 Geltungsbereich

Das vorliegende Dokument gilt für das Universitätsklinikum Hamburg-Eppendorf KdöR (UKE) sowie deren Tochtergesellschaften, die gemeinsam den *UKE-Konzern* bilden, sofern diese dem Geltungsbereich der Leitlinie beigetreten sind.

Die Geschäftsführungen der Tochtergesellschaften prüfen in eigener Verantwortung, ob ein entsprechender Bedarf besteht und setzen diesen gegebenenfalls um.

Diese Leitlinie gilt verbindlich für Dienstleister und Lieferanten, die für Konzerngesellschaften im Geltungsbereich

- IT-Systeme konfigurieren, installieren, anpassen, in Betrieb nehmen, warten, in Stand setzen oder administrativ betreuen (*IT-Dienstleister*) oder
- auf IT-/MT-/OT-Systemen des UKE-Konzerns Informationen zur Leistungserbringung verarbeiten (*Sonstige Dienstleister / Dritte*) sowie
- unabhängig von den vorgenannten Kriterien als *Auftragsverarbeiter* gem. Art. 28 DS-GVO tätig sind.

Dienstleister und Dritte, die durch vertragliche Vereinbarung im Rahmen der Bestellung über die Inhalte der Leitlinie Informationssicherheit und Datenschutz informiert und auf die Informationssicherheit verpflichtet sind, unterliegen ebenfalls dem Geltungsbereich.

Haben Dienstleister / Dritte ein eigenes ISMS implementiert wird im Rahmen von Kontrollhandlungen überprüft, ob die Anforderungen dieser Richtlinie erfüllt werden.

Diese Leitlinie gilt gegenüber allen Mitarbeitenden der Unternehmen und sonstigen Vertragsparteien im Geltungsbereich.

3 Prozessablauf

3.1 Informationsklassifizierung

Diese Leitlinie ist gem. Traffic Light Protocol (TLP 2.0) mit **TLP: CLEAR** eingestuft.

Informationen aus dem Prozessablauf dürfen ohne Einschränkungen frei weitergegeben werden.

Die Anlagen sind gem. Traffic Light Protocol (TLP 2.0) mit **TLP: AMBER** eingestuft.

Die Weitergabe der Dokumente oder einzelner Informationen aus diesen Dokumenten ist auf die Organisationen sowie externen Vertragspartner im Geltungsbereich sowie gesetzlich legitimierte Empfänger außerhalb der Organisationen (z.B. Auditoren, Behörden) beschränkt. Es gilt das Prinzip „Kenntnis nur, wenn nötig“.

3.2 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. Erhöhte Bedrohungen durch die aktuelle globale Sicherheitslage sowie technische Schwachstellen in Informations- und Netzwerktechnik (IT- / NT-Systeme) erfordern angemessene und wirksame Maßnahmen, um ein ausreichendes Schutzniveau zu etablieren.

Das UKE, das auf Grundlage der BSI-Kritis-Verordnung (BSI-KritisV) die kritische Dienstleistung der vollstationären Versorgung erbringt (KRITIS), aber auch alle anderen medizinischen Tochtergesellschaften, die Krankenhausbehandlungen im Sinne des § 39 SGB V anbieten und den Anforderungen des § 39 I SGB V unterliegen, sind in besonderem Maße an die Ziele der Informationssicherheit im Kontext des Gesundheitswesens gebunden.

Konzernweit sollen die Anforderungen des branchenspezifischen Sicherheitsstandards „Medizinische Versorgung“ (B3S) als Standard für die Informationssicherheit bei medizinischen Dienstleistungen gelten, unabhängig davon, ob dies eine kritische Dienstleistung gem. BSI-KritisV darstellt.

Im Übrigen gelten mindestens die international anerkannten Standards zur Informationssicherheit, die sich aus der ISO 27001ff. oder alternativen Normen ergeben (z.B. BSI-Grundschutz, NIST).

3.3 Schutzziele der Informationssicherheit

Neben den allgemeinen Schutzzielen der Informationssicherheit sind im Kontext der medizinischen Versorgung besonders die Patientensicherheit und die Behandlungseffektivität zu berücksichtigen.

Vertraulichkeit

Es ist sicherzustellen, dass nur befugte Personen Daten und Informationen zur Kenntnis nehmen können.

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.

Patientensicherheit

Es ist sicherzustellen, dass die Freiheit von unvermeidbaren 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.

3.4 Stellenwert des Datenschutzes

Der Schutz personenbezogener Daten im Rahmen der medizinischen Versorgung ist schon aus dem ärztlichen Berufsbild heraus von besonderer Bedeutung. Ohne Einschränkung ist dieser Schutz aber auch für die personenbezogenen Daten von Mitarbeitenden, Studierenden und Teilnehmenden der Forschung sowie anderer Personen zu

gewährleisten. Ein vertrauenswürdiger Umgang mit den personenbezogenen Daten und den Risiken für die Betroffenen stärkt gerade in Vertrauensbeziehungen, wie im Behandlungs- oder Beschäftigungsverhältnis, das Miteinander und auch die positive Wahrnehmung in der Öffentlichkeit. Daher ist es nicht nur, aber insbesondere für den Umgang mit Patientendaten als auch Beschäftigtendaten essentiell, die datenschutzrechtlichen Anforderungen zu gewährleisten.

3.5 Schutzziele des Datenschutzes

Zum Schutz personenbezogener Daten und zur Gewährleistung der Einhaltung datenschutzrechtlicher Anforderungen werden technische und organisatorische Maßnahmen ergriffen, welche die Zwecke, Art, Umfang und Umstände der Verarbeitungen ebenso wie die Risiken für die Betroffenen angemessen berücksichtigen. Diese Maßnahmen dienen auch dem internen und ggf. externen Nachweis der Rechtskonformität. Bei der Planung und Spezifizierung von Verarbeitungstätigkeiten sowie konkreter Maßnahmen sind insbesondere die Auswirkungen auf den Behandlungsprozess und Gesundheitsschutz der Betroffenen zu beachten.

Dabei werden sowohl den Schutzzielen der Datensicherheit (Vertraulichkeit, Verfügbarkeit, Integrität) als auch der Gewährleistungsziele des Standard-Datenschutzmodells (Datenminimierung, Nichtverkettung, Transparenz, Interventionsbarkeit) Rechnung getragen.

Bei der Planung und Umsetzung der Geschäftsprozesse wird die Verfügbarkeit, Integrität und Vertraulichkeit der personenbezogenen Daten sichergestellt und hierbei auf die Informationssicherheit zurückgegriffen. Darüber hinaus wird der Umfang der Datenverarbeitung stets unter dem Gesichtspunkt der Notwendigkeit und bestehender gesetzlicher Anforderungen geleitet (Datenminimierung). Betroffene sind über die Verarbeitung seiner personenbezogenen Daten stets transparent und nachvollziehbar zu informieren und Ihnen hierdurch die Kenntnis zu verschaffen, welche Daten zu welchen Zwecken in welcher Form verarbeitet werden und wer die rechtliche Verantwortung hierfür trägt (Transparenz).

Die technischen und organisatorischen Maßnahmen haben auch sicherzustellen, dass Betroffenen die Wahrnehmung ihrer Rechte, namentlich der Rechte aus den Art. 15 ff. DSGVO (Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit), unkompliziert ermöglicht wird, soweit hiervon nicht gesetzlich legitimiert abzu-sehen ist. Die Verkettung (das Zusammenführen) zu unterschiedlichen Zwecken erhobener Daten ist technisch und organisatorisch unter Beachtung der vorstehenden Faktoren insoweit zu unterbinden, als sie rechtlich unzulässig ist oder daraus Risiken für Betroffene resultieren (Nicht-Verkettung).

3.6 Übergreifende Unternehmensziele

Der Vorstand sowie die jeweiligen Geschäftsführungen bekennen sich ausdrücklich zur Einhaltung der rechtlichen und ethischen Verantwortlichkeiten zum Schutz sensibler Informationen, zu dieser Leitlinie und zu ihrer Durchsetzung.

Über die vorgenannten Schutzziele hinaus verbindet der UKE-Konzern 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, BSI, 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

Das UKE ist ein Krankenhaus der Maximalversorgung und strebt den Ausbau der Spitzenmedizin an. Das UKE wird die Verzahnung von Forschung, Krankenversorgung und Lehre sowie das interdisziplinäre Zusammenwirken vorantreiben. Es konzentriert sich in der Spitzenmedizin auf die klinischen Schwerpunkte Herz-Kreislauf-Erkrankungen, neurologische Erkrankungen, entzündliche und Infektions-Erkrankungen, Tumorerkrankungen, psychische Erkrankungen und Transplantationsmedizin. Einen mindestens ebenso hohen Stellenwert haben Kindermedizin und Perinatal Medizin. Neue Schwerpunkte entwickelt das UKE in den Bereichen Seltene Erkrankungen, Lebensphasenmedizin (Transfusionsmedizin) sowie Präventiv- und Sportmedizin.

Das UKE strebt eine Spitzenstellung in der universitären medizinischen Forschung an, die auf der engen Verzahnung von Forschung, Krankenversorgung und Lehre beruht. Das wissenschaftliche Profil, das sich derzeit in fünf Forschungsschwerpunkten und zwei Potenzialbereichen zeigt, muss weiter geschärft und die Forschungsnetzwerke müssen entsprechend ausgebaut werden. Die Vernetzung mit den Versorgungsschwerpunkten wird vertieft.

Das UKE strebt eine national wie international sichtbare Spitzenstellung in der Ausbildung von Medizinerinnen und Zahnmedizinerinnen sowie in der Lehrforschung an. Das UKE wird darüber hinaus den Wissenschaftsstandort Hamburg stärken, indem fächerübergreifende Curricula mit Hamburger Universitäten und Hochschulen ausgebaut werden.

Das UKE ist als „Familienfreundliches Unternehmen“ zertifiziert und hat die „Charta der Vielfalt“ unterzeichnet. Das UKE will attraktivster Arbeitgeber im Gesundheitswesen werden.

Das UKE ist zentrales Element des Gesundheitsmarktes der Metropolregion Hamburg und will die Wachstumschancen der Metropolregion nutzen. Wirtschaftliches Wachstum, das das UKE nach Kräften anstrebt, ist dabei nicht Selbstzweck, sondern stellt das Fundament für den weiteren erfolgreichen Weg mit einem hohen Maß an Eigenständigkeit dar. Die Netzwerkstrategie ist ein wichtiger Baustein, unternehmerische Eigenverantwortung eine wichtige Voraussetzung.

3.7 Risikomanagement

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

Die Beteiligung der Informationssicherheit kann auch durch Vorstellung von neuen Systemen beim CGB oder durch das Datenschutzmanagement im GB SI erfolgen.

Die Risikobewertung soll bereits im Rahmen der Beschaffung unabhängig vom Vergabeverfahren, spätestens jedoch vor der Implementierung neuer Systeme durchgeführt werden. Besteht eine vom Vorstand oder der jeweiligen Geschäftsführung oder konzernweit verabschiedete Projektbeauftragung ist dieser Bewertungsschritt von der verantwortlichen Projektleitung zwingend einzuleiten und das Team Informationssicherheit zu involvieren.

Sofern sich aus der Risikobewertung die Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung gem. Art. 35 Datenschutz-Grundverordnung (DSGVO) ergibt, ist diese unter Einbindung des Team Datenschutz 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.

Darüber hinaus erhalten der Vorstand des UKE sowie die Geschäftsführungen der Konzerngesellschaften vom ISB mindestens jährlich einen Risikobericht. Die Überwachung der daraus resultierenden Risikobehandlung obliegt dem Team Informationssicherheit.

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

3.8 Weiterentwicklung der Informationssicherheit und des Datenschutzes

Systemverantwortliche erarbeiten angemessene, allgemeingültige Schutzkonzepte zur Absicherung der technikunterstützten Informationsverarbeitung in enger Abstimmung mit dem Team Informationssicherheit unter Berücksichtigung des Stands der Technik.

Spezifische Maßnahmen und Vorgaben werden in den gelenkten Dokumenten des Rahmenwerks zur Informationssicherheit sowie in den jeweiligen Konzepten, Betriebs- und Dienstvereinbarungen sowie Handlungsanweisungen ausformuliert. Diese Dokumente unterliegen einer ständigen Weiterentwicklung, basierend u.a. auf den Erkenntnissen des Teams Informationssicherheit und den Feststellungen von internen und externen Audits.

Der Vorstand und die jeweiligen Geschäftsführungen unterstützen die ständige Verbesserung des Informationssicherheitsniveaus sowie des Datenschutzniveaus. Alle Mitarbeitenden sind angehalten, Verbesserungsvorschläge oder mögliche Schwachstellen an den ISB / DSB bzw. das Team Informationssicherheit / Team Datenschutz zu melden.

Der ISB überprüft und entwickelt die Informationssicherheitsstrategie und die Wirksamkeit der bisherigen Organisationsform, Maßnahmen und Prozesse für Informationssicherheit kontinuierlich weiter.

Der ISB berichtet regelmäßig zum Stand der Informationssicherheit gegenüber dem Vorstand und den jeweiligen Geschäftsführungen. Diese entscheiden dabei in dokumentierter Form über die empfohlenen Maßnahmen zur Verbesserung und zum Ausbau der Informationssicherheit.

Dem Vorstand, in Form der höchsten Managementebene, obliegt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz, sowohl im Hinblick auf die Umsetzung des Sicherheits- und Datenschutzmanagements als auch auf dessen kontinuierlich Verbesserung. Hierzu sind die notwendigen Ressourcen für den Betrieb und die Weiterentwicklung der Managementsysteme aus den Bereichen Informationssicherheit und Datenschutz bereitzustellen.

4 Prozesssteuerung

4.1 Prozessverantwortliche

Verantwortliche/r für die Prozesssteuerung: ISB

Prozessverantwortliche	Beschreibung
Vorstand / Geschäftsführungen	Verantwortung für die Informationssicherheit und den Datenschutz. Dies umfasst alle jeweils betriebenen informationstechnischen Systeme und Verarbeitungsprozesse mit personenbezogenen Daten. Die Umsetzung und Einhaltung dieser Leitlinie wird vom Vorstand und den jeweiligen Geschäftsführungen als letzte Kontrollinstanz verantwortet.
ISB	Fördert die Informationssicherheit im UKE-Konzern, koordiniert und steuert Sicherheitsprozesse der Informationssicherheit und ist Verantwortlicher für die Durchführung und Dokumentation der Prozesse.
DSB	Fördert den Datenschutz im UKE durch Unterrichtung und Beratung der Leitungsebene und der Mitarbeitenden, Überwachung der Einhaltung datenschutzrechtlicher Anforderungen, Durchführung von Schulungen und Führung des Verzeichnisses der Verarbeitungstätigkeiten.

4.2 Prozessbeteiligte und -schnittstellen

Prozessbeteiligte	Beschreibung
Externe Vertragsparteien	Gewährleistung der Mitwirkung zur Einhaltung der Ziele sowie die Einhaltung der entsprechenden Anforderungen der Leitlinie sowie weiterer Regelungen und Maßnahmen zur Informationssicherheit und zum Datenschutz.
Mitarbeitende	Verantwortung im Rahmen der Tätigkeiten die Risiken für die Informationssicherheit zu minimieren und die Fortführung der Behandlungs- und Geschäftsprozesse im Notfall sicherzustellen sowie die gesetzlichen Datenschutzanforderungen einzuhalten. Dies gilt im Besonderen für die Führungskräfte.
Führungskräfte	Unter Beachtung ihrer maßgebenden Vorbildfunktion tragen sie in ihrem jeweiligen Verantwortungsbereich insbesondere auch dafür, dass die für den UKE-Konzern bestehenden Regelungen zur Informationssicherheit und zum Datenschutz beachtet und eingehalten werden.
Systemverantwortliche	Sicherstellung der Einhaltung der Leitlinie sowie ergänzender Regelungen der Informationssicherheit und des Datenschutzes auf den von ihnen betriebenen Systemen und Nachweis im Rahmen des ISMS/DSMS.
Prozessverantwortliche	Überwachung der Durchführung konkreter Prozesse im jeweiligen Zuständigkeitsbereich. Einstufung der Schutzbedarfe des jeweiligen Prozesses und somit für die unterstützende Anwendung.
GB Einkauf / Verantwortliche für Externe Vertragsparteien	Verpflichtung der Dienstleister / Lieferanten und sonstigen externen Vertragsparteien zur Informationssicherheit.
Datenschutzkoordinatoren	Erste Ansprechpartner für Datenschutzfragen. Sie beraten und unterstützen die Leitung und die Beschäftigten ihrer Organisationseinheiten im Rahmen ihrer Zuständigkeit bei der Umsetzung gesetzlicher und vor allem innerbetrieblicher Anforderungen des Datenschutzes.
MediGate GmbH	Die Datenschutzjuristen der MediGate GmbH erarbeiten vertieft Lösungen konkreter datenschutzrechtlicher Fragen und Klauseln im Bereich des Vertragsmanagements Drittmittel. Zudem übernehmen sie innerhalb der MediGate GmbH die Bearbeitung von DTAs und Registerstudien im Bereich der Forschung. Sie bilden die Schnittstelle zum DSB und unterstützen diesen.
Team Informationssicherheit	Unterstützt den ISB bei der Erfüllung seiner Aufgaben zur Steuerung des Informationssicherheitsprozesses sowie des ISMS.
Datenschutzmanagement (GB SI)	Stellt die Umsetzung der datenschutzrechtlichen Anforderungen und des DSMS sicher.
GB Recht	Berät (u.a.) in datenschutzrechtlichen Angelegenheiten und vertritt das UKE gegenüber Datenschutzaufsichtsbehörden. Darüber hinaus ist er operativ für den Umfang und die Meldung von Verletzungen der Sicherheit personenbezogener Daten zuständig.

Schnittstellen	Beschreibung
Compliance und Governance Board (CGB)	Zentrales Steuerungsgremium im Konzern für alle Belange der Informationssicherheit und des Datenschutzes.
Personalvertretung	Mitbestimmung im Rahmen des Personalvertretungsrechts zur Festlegung der Modalitäten und Rahmenbedingungen hinsichtlich der Maßnahmen der Informationssicherheit und des Datenschutzes.
Stabstelle Business Continuity Management (BCM)	Steuert alle Aktivitäten rund um die Notfallvorsorge und die Geschäftsführung.

4.3 Prozessdokumentation

Der Beitritt von Konzerngesellschaften in den Geltungsbereich dieser Leitlinie wird in Anlage 01 dokumentiert. Die Verpflichtung von externen Vertragsparteien zur Informationssicherheit wird auf Grundlage des Formblatts in Anlage 02 dokumentiert. Dies gilt auch für die Beitrittserklärung von Konzerngesellschaften in den Geltungsbereich dieser Leitlinie sowie des ISMS Rahmenwerks.

4.4 Prozessrisiken

Der Prozess ist für die Erfüllung gesetzlicher und normierter Anforderungen an ein ISMS sowie ein DSMS erforderlich und legt die strategische Ausrichtung sowie die Ziele der Informationssicherheit und des Datenschutzes fest.

4.5 Prozesskennzahlen

Beschreibung Prozesskennzahlen
Anzahl der Unternehmen des UKE-Konzern im Geltungsbereich der Leitlinie
Anzahl der externen Vertragsparteien im Geltungsbereich der Leitlinie

4.6 Prozesskontrollen

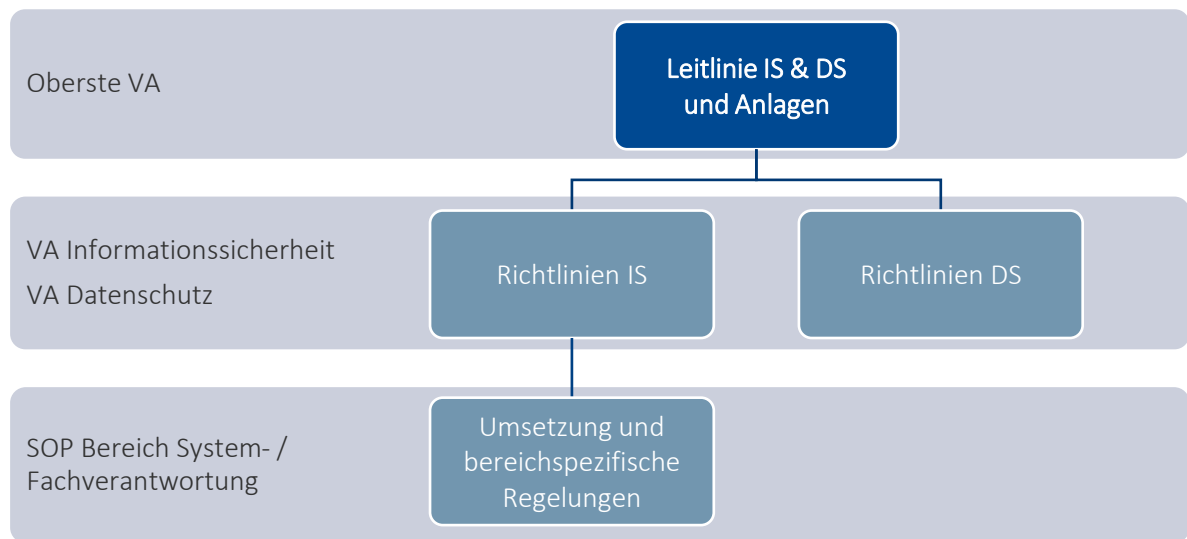
- Sicherstellung der (normativen) Konformität
 - Kontrollen durch den ISB oder DSB
- Regelmäßige Kontrolle der Prozesskennzahlen
- Berichterstattung durch den ISB

5 Mitgeltende Unterlagen

Diese Leitlinie bildet die oberste Ebene des ISMS Rahmenwerks sowie des DSMS Rahmenwerks.

Nachrangig gelten alle Richtlinien, Handlungsanweisungen, Sicherheitskonzepte und sonstige Vorgaben der Informationssicherheit und des Datenschutzes, die im QMH gelenkt sind.

Soweit auf das Rahmenwerk der Informationssicherheit verwiesen wird, umfasst dies die Richtlinien der Informationssicherheit sowie die bereichsspezifischen SOP betrachtet.



5.1 Literatur, Rechtsvorschriften und Normen

- BSI-Gesetz / BSI-Kritis-Verordnung
- B3S medizinische Versorgung
- BSI IT-Grundschutz-Kompendium
- ISO 27001 (Anforderungen an ein ISMS)
- ISO 27002 (Sicherheitsmaßnahmen für die Informationssicherheit)
- ISO 27004 (Messung der Wirksamkeit des ISMS)
- ISO 27005 (Risikomanagement in der Informationssicherheit)
- ISO 22301 (Business Continuity Management)
- IEC 80001 (Risikomanagement vernetzte Medizintechnik)
- DS-GVO, BDSG
- SGB V
- GBA Beschlüsse
- Hamburgisches Datenschutzgesetz
- Hamburgisches Krankenhausgesetz
- Verordnung 536 aus 2014

6 Begriffe und Abkürzungen

6.1 Begriffe

Entfällt

6.2 Abkürzungsverzeichnis

Entfällt

7 Hinweise und Anmerkungen

Keine

8 Anlagen

Anlage	Titel der Anlage
Anlage 01	Geltungsbereich ISMS UKE-Konzern
Anlage 02	Verpflichtungserklärung zur Informationssicherheit
Anlage 03	Operative Ziele und Kennzahlen des ISMS
Anlage 04	Auditplan Informationssicherheit
Anlage 05	Organisation des Informationssicherheitsprozesses

Freigabevermerk: Diese Verfahrensanweisung (VA) wurde durch Beschluss des Vorstands des UKE in Kraft gesetzt und durch die Leitung des Geschäftsbereichs Qualitätsmanagement und Patientensicherheit im QM-Handbuch des UKE freigegeben. Zurückgezogene Versionen dieser VA werden entsprechend der geltenden Regelungen archiviert.

Autor:in:

Timo Ehlers, GB SI (ISB)