Ziel:
Zielsetzung dieser Leitlinie ist die Definition des Zwecks, der Ausrichtung, der Grundlagen und der grundsätzlichen Regeln für die Informationssicherheit und das Informationssicherheits-Management (ISMS) am Krankenhaus.
Patienten, Kooperationspartner, der Medizinische Dienst (MD), der Gesetzgeber und weitere interessierte Parteien erwarten vom Krankenhaus den verantwortungsvollen Umgang mit sensiblen Informationen. Mit dieser Informationssicherheitsleitlinie werden die allgemeinen Ziele und Grundsätze der Sicherheit von Informationen durch die Geschäftsführung am Krankenhaus verbindlich festgelegt.
Ein weiteres Ziel ist es, ein Managementsystem für Informationssicherheit zu etablieren, welches den Reifegrad der Informationssicherheit am Krankenhaus kontinuierlich erhöht.
Die Grundsätze der Informationssicherheit sind auf Anfrage gegenüber externen Parteien zu kommunizieren.

Anwendungsbereich:
Diese Leitlinie gilt verbindlich für die Führungskräfte, alle Mitarbeiter, Geschäftspartner, Dienstleister und Lieferanten des Krankenhauses.

Ansprechpartner:
Ansprechpartner zu allen Themen der Informationssicherheit ist:
der ISMK = Informationssicherheitskoordinator und sein Kernteam, bestehend aus: Mitarbeitern der Bereiche QM, IT-Abteilung, Medizin/Technik, Datenschutz und ext. ISB.

1 - Unternehmensphilosophie

Die COLLM KLINIK OSCHATZ, ein Gemeinschaftsunternehmen des Landkreises Nordsachsen und der Asklepios Kliniken GmbH & Co. KGaA im Freistaat Sachsen, ist ein Haus der Grund- und Regelversorgung sowie der spezialisierten Versorgung in der Orthopädie und Chirurgie.

Unternehmensziel: Wir sind ein etabliertes Gesundheitszentrum der Region mit bestmöglicher Versorgungsqualität bei gleichzeitiger Wirtschaftlichkeit.

Erfolgsfaktoren zur Erreichung des Unternehmenszieles sind:

- Qualitätssicherung mit hoher klinischer Fachkompetenz
- wirtschaftlich optimierte und logistische Patientenversorgung
- Wertschätzung gegenüber jedem sich uns Anvertrauten
- Erwirtschaftung der notwendigen Betriebs- und Investitionsmittel, Zufriedenheit engagierter Mitarbeiter
- Informationssicherheit ist ein strategisches Unternehmensziel zur Sicherstellung der Patientenversorgung.

2 – Stellenwert der Informationssicherheit

Zur Erreichung der Unternehmensziele und zur Sicherstellung der Patientenversorgung unterliegt das Krankenhaus einer Reihe gesetzlicher Regularien zum Umgang mit Patientendaten. In diesem

Zusammenhang müssen hohe Anforderungen an die Informationssicherheit erfüllt und Gesundheitsdaten besonders geschützt werden.
Weiterhin nimmt die Abhängigkeit in den Geschäfts- und Behandlungsprozessen von der Informationstechnologie in allen Bereichen stetig zu. Die medizinische Versorgung ist in einem hohen Maß auf eine funktionierende IT-, Medizintechnik-, Kommunikationstechnik- und Versorgungstechnik-Infrastruktur angewiesen.

Aus diesen Gründen ist die Informationssicherheit ein integraler Bestandteil der strategischen Unternehmensziele und wird somit nicht in erster Linie als Kostenfaktor, sondern als ein wichtiger Erfolgsfaktor für das Krankenhaus angesehen.

Die Verantwortung für eine angemessene Umsetzung der Informationssicherheit liegt bei der Geschäftsführung. Sie räumt der Informationssicherheit eine angemessene Priorität und Stellenwert ein und stellt die notwendigen Ressourcen für die Einrichtung, die Umsetzung, die Aufrechterhaltung sowie die fortlaufende Verbesserung eines Informationssicherheits-Managementsystems (ISMS) zur Verfügung.

Ein wesentlicher Bestandteil für den erfolgreichen Betrieb des ISMS sind die verantwortungsbewussten und qualifizierten Mitarbeiter. (Aus Gründen der Lesbarkeit wurde im Text die männliche Form gewählt, nichtsdestoweniger beziehen sich die Angaben auf Angehörige jeden Geschlechts.)

Die Qualifikation der Mitarbeiter im Bereich der Informationssicherheit sowie Sensibilisierungsmaßnahmen für alle Mitarbeiter am Krankenhaus werden durch regelmäßige Schulungen sichergestellt.

Die Informationssicherheit ist als eine Querschnittsaufgabe zu verstehen und muss in allen Prozessen, die mit der stationären Patientenversorgung in Verbindung stehen, berücksichtigt werden. Hierbei unterstützen alle Führungskräfte und Mitarbeiter die ISMS-Verantwortlichen.

Das Krankenhaus hat beschlossen, ein an dem internationalen Standard DIN ISO/IEC 27001 ausgerichtetes ISMS als Managementsystem für Informationssicherheit zu etablieren, um somit zukünftig auf eine mögliche Zertifizierung durch eine akkreditierte Prüfstelle vorzubereitet zu sein. Zusätzlich werden die spezifischen Sicherheitsstandards des Gesundheitssektors gemäß dem branchenspezifischen Standard „B3S Gesundheitswesen“ berücksichtigt.

3 – Grundwerte der Informationssicherheit

Die Informationssicherheit umfasst angemessene organisatorische, technische und personelle Maßnahmen sowie zugehörige Prozesse, um Unternehmensinformationen zu schützen. Die Schutzziele sollen die Informationssicherheit in den Geschäftsprozessen gewährleisten und somit die Auswirkungen von Informationssicherheitsvorfällen auf den Krankenhausbetrieb minimieren bzw. diesen vorbeugen.

Im Rahmen des B3S werden die Schutzziele wie folgt definiert:

- VERFÜGBARKEIT von Dienstleistungen, Funktionen eines Informationssystems, IT-Systems, IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwendern stets wie vorgesehen genutzt werden können.

- INTEGRITÄT bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Daten und der korrekten Funktionsweise von Systemen.

- AUTHENTIZITÄT der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle erstellt wurden.

- VERTRAULICHKEIT stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

- PATIENTENSICHERHEIT als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

- BEHANDLUNGSEFFEKTIVITÄT stellt die wirksame Behandlung des Patienten unter Benutzung von Informationen und wirksamen Therapiemaßnahmen, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

4 – Ziele der Informationssicherheit

Ergänzend zu den allgemeinen strategischen Zielen des Krankenhauses plant die Geschäftsführung (GF) folgende Ziele in der Informationssicherheit zu erreichen.

- Die GF sieht Informationssicherheit als ein strategisches Unternehmensziel zur Sicherstellung der Patientenversorgung.
- Informationssicherheit soll zu einem wesentlichen Faktor für eine positive Außenwirkung für Patienten, Mitarbeiter und Vertragspartner werden.
- Die Patienten, Mitarbeiter und andere interessierte Parteien erwarten den rechtlichen und ethischen Schutz ihrer Daten, insbesondere der personenbezogenen Daten und Gesundheitsdaten.
- Es wird ein kontinuierlicher Prozess zur Überprüfung von angemessenen organisatorischen und technischen Maßnahmen zur Erreichung der Schutzziele der Informationssicherheit entsprechend dem Stand der Technik etabliert.
- Es wird ein strukturiertes und kontinuierliches Verfahren zum angemessenen Umgang mit Informationssicherheitsrisiken und deren Behandlung eingeführt.
- Die GF erwartet die Einhaltung von Gesetzen, regulatorischen Anforderungen, Vorschriften, Verträgen, Vereinbarungen, technischen Normen und bewährten Methoden.
- Die Wirtschaftlichkeit und Nutzbarkeit wird zukünftig durch lösungsbasierte Ansätze und Impulse aus der Informationssicherheit unterstützt. Die umzusetzenden Maßnahmen sollen im Verhältnis zum wirtschaftlichen Aufwand stehen.

- Über diese grundlegenden Zielsetzungen hinaus legt die GF mindestens jährlich in Absprache mit dem ISMS-Kernteam kurz- und mittelfristig zu erreichende und nach Möglichkeit messbare Informationssicherheitsziele fest und lässt sich regelmäßig über deren Erreichung informieren.
- Die kontinuierliche Verbesserung des Informationssicherheits-Reifegrades für alle Kernprozesse ist geplant.

5 – Erreichung und Umsetzung der Ziele

Die GF hat eine Informationssicherheitsorganisation zum Aufbau, Management und zur kontinuierlichen Verbesserung des ISMS benannt. Diese Organisation umfasst den Informationssicherheitskoordinator (ISMK) und das ISMS-Kernteam.

Der eISB und der ISMK sind im Auftrag der GF für den Aufbau und den operativen Betrieb des ISMS zuständig und werden vom ISMS-Kernteam bei der Aufgabenerfüllung unterstützt.

Neben der Informationssicherheitsleitlinie bedarf es zum Aufbau eines Regelwerkes der Informationssicherheit weiterer ISMS-Richtlinien (z.B. Dienstanweisungen, Verfahrensanweisungen), die erstellt, regelmäßig überarbeitet bzw. aktualisiert und deren Einhaltung überwacht werden muss.

Die von der Informationssicherheitsorganisation erarbeiteten Maßnahmen werden mit der GF abgestimmt und deren Umsetzung durch Bereitstellung geeigneter Ressourcen und Kompetenzen unterstützt. Der Umsetzungsstand wird regelmäßig berichtet.

6 – Kontinuierliche Verbesserung und Weiterentwicklung

Das ISMS wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Alle Maßnahmen und Richtlinien zur Informationssicherheit werden stetig daraufhin untersucht, ob sie nach dem Stand der Technik umgesetzt und in den Betriebsablauf integriert sind sowie das angestrebte Sicherheitsniveau erfüllen.

7 – Verstöße gegen die Informationssicherheit

Alle Verstöße werden als Handlungen gegen das Regelwerk der Informationssicherheit verstanden. Dazu zählen insbesondere:

- Kompromittieren der Sicherheit von Informationen
- unberechtigter Zugriff auf Informationen
- unberechtigte Änderung, Nutzung und/oder Veröffentlichung von Informationen

Verstöße gegen die Informationssicherheit können nach den geltenden Regelungen und gesetzlichen Bestimmungen strafrechtlich geahndet werden.

8 – ISMS-Anwendungsbereich

Zweck
Die Klinik etabliert ein Informationssicherheits-Managementsystem (ISMS) nach den Vorgaben der gültigen Fassung des DIN EN ISO/IEC 27001. Das vorliegende Dokument definiert den Anwendungsbereich (Scope) des ISMS und gibt Aufschluss über die Inhalte sowie die Grenzen und Ausschlüsse des Anwendungsbereiches des ISMS.

Der Aufbau der Organisation sowie die unternehmensinterne Organisation der Klinik ist im ISMS-Managementsystem (Aeneis) dargestellt und wird dort regelmäßig überprüft und aktualisiert.

Kontext
Der interne und externe Kontext ist die Grundlage für die Ziele und Grundsätze der Informationssicherheit in der Klinik.

Zum Kontext gehören sowohl interne Anforderungen an die Informationssicherheit als auch externe Anforderungen bzw. Erwartungen, die sich z.B. durch gesetzliche und regulatorische Rahmenbedingungen sowie vertragliche Verpflichtungen und Schnittstellen zu Partnern und Dienstleistern ergeben.

Der für die Zertifizierung nach DIN ISO/IEC 27001 relevante Kontext des ISMS ist im Folgenden beschrieben.

Anforderungen

interne Anforderungen
Die internen Anforderungen umfassen die internen Gegebenheiten, mit denen die Klinik versucht ihre Unternehmensziele zu erreichen. Das Management der Informationssicherheit muss auf die Kultur, die Prozesse und Strukturen sowie die Strategie der Klinik abgestimmt sein. Der interne Zusammenhang bezieht sich auf alles innerhalb der Organisation, was die Art und Weise beeinflusst, in welcher die Klinik ihre Risiken der Informationssicherheit bewältigen will.

Die internen Anforderungen an die Informationssicherheit ergeben sich aus den organisatorischen Gegebenheiten und der Geschäftstätigkeit der Klinik.

externe Anforderungen
Die externen Anforderungen im Bereich der Informationssicherheit sind u.a. folgende Gesetze bzw. Vorschriften.

Allg. Anforderungen und Vorgaben:
- Sozialgesetzbuch SGB V
- Bundesdatenschutzgesetz
- Sächsisches Krankenhausgesetz
- Sächsisches Datenschutzgesetz
- Datenschutz-Grundverordnung
- Sächsisches Datenschutzdurchführungsgesetz
- Medizinproduktegesetz/Medizinproduktebetreiberverordnung

Spezielle Anforderungen:

- Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz/Sächsisches IT-Schutzgesetz)
- BSI 100-4 / BSI 200-4 Notfallmanagement
- DIN EN ISO/IEC 27001:2017
- DIN EN ISO 22301 Sicherheit und Schutz des Gemeinwesens (BCMS)
- DIN EN ISO 80001 Risikomanagement
- Branchenspezifischer Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus (B3S)

Weiterhin zählen zu den externen Anforderungen die Verträge mit Patienten und Dienstleistern und die Anforderungen von Gesellschaftern.

Interessierte Parteien (extern & intern)

Die interessierten Parteien lassen sich nach intern und extern unterscheiden. Folgende Tabelle gibt eine Übersicht über die interessierten Parteien und deren Anforderungen in Bezug auf die Informationssicherheit.

extern	Anforderung
Gesetzgeber/Aufsichtsbehörden	• Einhaltung von Gesetzen und Verordnungen
Bundesamt für Sicherheit in der Informationstechnik	• Etablierung und Weiterentwicklung ISMS entsprechend Vorgabe IT-Sicherheitsgesetz • Meldung relevanter Störungen bei der Klinik • Zugriff auf Systeme und Daten der Klinik zur Abwehr und Vorbeugung von Sicherheitsrisiken bei öffentlichem Interesse bzw. zum Schutz der nationalen Sicherheit
Gesetzliche Krankenversicherung/ Private Krankenversicherung	• Sicherstellung Gesundheitsversorgung • Medizinisch und wirtschaftlich sinnvolles Arbeiten • elektronischer Datenaustausch bei Anfrage Kostenübernahme und Abrechnung stationärer Aufenthalt
Patienten	• ordnungsgemäße stationäre Behandlung • Schutz der Patientendaten
Angehörige	• ordnungsgemäße stationäre Behandlung • Schutz der Patientendaten

Einweiser/Rettungsdienste/ niedergelassene Ärzte/ andere Krankenhäuser	• reibungsloser Informationsfluss • Übernahme der Patienten • ordnungsgemäße stationäre Behandlung • elektronischer Zugriff auf Patientendaten und Arztbriefe
Pflegeeinrichtungen/Pflegedienste	• reibungslose Weiterversorgung der Patienten im Rahmen des Entlassmanagements • Datenaustausch mit dem Krankenhaus
Externe Dienstleister/Lieferanten	• Einhaltung von vertraglichen Verpflichtungen • Einsatz von Hardware/Software in der Klinik • Zutritt zu Räumlichkeiten bzw. informationsverarbeitende Einrichtungen der Klinik • Zugriff auf schützenswerte Informationen

Interne Parteien	**Anforderung**
Gesellschafter/Aufsichtsrat	• Sicherstellung Gesundheitsversorgung • wirtschaftlich positives Ergebnis der Geschäftstätigkeit • keine negativen Schlagzeilen
Geschäftsführung/Krankenhausleitung	• Verantwortung für die Informationssicherheit • Mitwirkung bei der Initiierung, Überwachung und kontinuierlichen Verbesserung des ISMS • Rechte und Verantwortlichkeiten im Hinblick auf die Einschätzung und Behandlung von Informationssicherheitsrisiken sowie bei der Bereitstellung von Ressourcen (Personal, Finanzen und Sachmittel) • Interesse an der Erlangung und Aufrechterhaltung der DIN EN ISO/IEC 27001-Zertifizierung
Mitarbeiter	• Mitwirkung bei der Umsetzung und beim Betrieb des ISMS • Schutz der Mitarbeiterdaten

Betriebsrat	• Mitwirkungs- und Mitbestimmungsrechte bei der Ausgestaltung des Regelwerks des ISMS in der Klinik sowie bei der Ausgestaltung von Arbeitsabläufen und internen Kontrollen
Datenschutzbeauftragter extern/Datenschutzkoordinator	• Einhaltung datenschutzrechtlicher Vorgaben im ISMS • Mitwirkung bei technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten • Der Datenschutzkoordinator agiert als Schnittstelle zwischen dem eDSB und dem Haus.

Geschäftsprozesse im Anwendungsbereich (kritische Geschäftsprozesse)

Der Anwendungsbereich des ISMS erstreckt sich auf die Kern- und Unterstützungsprozesse der Klinik. Eine Übersicht zu den medizinischen Abteilungen der Klinik ist dem Organigramm zu entnehmen.

Die Kernprozesse (Primärprozesse) des KLINIK umfassen die Aufnahme, Diagnostik, Therapie & Behandlung sowie Entlassung & Verlegung.
Darüber hinaus verfügt die Klinik über Unterstützungsprozesse, die als patientennahe medizinische und nichtmedizinische Sekundärprozesse in der Prozesslandkarte im ISMS-Managementsystem dargestellt sind.
Die Prozesslandkarte aus dem Roxtra wurde in das Aeneis integriert und wird regelmäßig auf Aktualität überprüft.

Durch die Konzentration auf die stationäre medizinische Behandlung wird der Anwendungsbereich in den Kernprozessen wie folgt eingeschränkt:
Dieser umfasst die in den medizinischen Facheinrichtungen, in den Ambulanzen/Sprechstunden und den interdisziplinären Behandlungszentren erbrachte vorstationäre Diagnostik und die Planung des stationären Aufenthalts sowie die stationäre Versorgung. Rein ambulant behandelte Patienten sind nicht im Anwendungsbereich des ISMS.
Die Grenzen des Anwendungsbereichs bei „Entlassung & Verlegung“ werden durch den Abschluss des gesetzlich vorgeschriebenen Entlassmanagements und den administrativen Fallabschluss definiert.
Die nachstationäre ambulante Versorgung außerhalb des stationären Falls liegt nicht im Anwendungsbereich.

Die Prozess-Übersicht ist ebenfalls im roXtra dargestellt.

Organisationseinheiten im Anwendungsbereich

Durch Konzentration auf die stationäre medizinische Versorgung sind vom Anwendungsbereich ausgeschlossen:

- Unternehmenskommunikation (intern/extern); Marketing/PR
- Erlösmanagement
- Controlling

- Qualitäts- und Beschwerdemanagement
- rein ambulante und nachstationäre Versorgung

Mitarbeiter im Anwendungsbereich
Die Mitarbeiter im Anwendungsbereich sind alle Mitarbeiter, deren Tätigkeit einen wesentlichen Einfluss auf die Informationssicherheitsleistung der Klinik hat.

Dienstleister im Anwendungsbereich
- siehe Prozesslandkarte

Zuordnung der Unterstützungsprozesse zu Organisationseinheiten
Folgende Tabelle beinhaltet die Zuordnung von Abteilungen/Dienstleistern zu Unterstützungsprozessen.

Abteilung/Dienstleister	**Unterstützungsprozess intern**
IT-Abteilung	EDV & IT
HBD	Patiententransport
Küche	Küche & Cafeteria
Transfusionsverantwortliche	Transfusion
Hygienefachkraft	Hygienemanagement
Technik	Abfall- und Umweltschutz
Stationen	Medizinisches Notfallmanagement
Stationen	Sicherheit und Notfallpläne
Apotheke, Stationen	Umgang mit Arzneimitteln und BTM/Apotheke
AEMP	Aufbereitung
Ethik-Kommission	Ethik, Werte und Tod
Archiv	Archiv, Dokumentation
Materialwirtschaft	Einkauf & Investition
Arbeitsschutzbeauftragter (AMVZ), Brandschutzbeauftragter	Arbeits- und Brandschutz
Empfang	Rezeption
WISAG	Reinigung

Sitex	Wäscheversorgung
Elblab	Labor
Medizintechnik	Medizintechnik

Irrelevante Prozesse

Folgende Tabelle beinhaltet Organisationseinheiten, die für das ISMS keine relevanten Dienstleistungen sind.

Stabsstelle/ Abteilung	**Prozessbeschreibung**
externe Rechtsanwälte	Rechtliche Beratung
Collmed MVZ	Medizinisches Versorgungszentrum
Kurzzeitpflege	Nachversorgung

9 – ISMS-Organisation

Zweck

- Ein zentraler Baustein für den reibungslosen und effektiven Betrieb eines Informationssicherheits-Managementsystems (ISMS) ist die Informationssicherheits-Organisation (IS-Organisation).
- Die Aufgabe der IS-Organisation ist die Planung, Implementierung, Aufrechterhaltung und Verbesserung des Reifegrades des ISMS. Im Folgenden werden die Struktur und die Aufgabenverteilung im Detail beschrieben

Struktureller Aufbau

- Die Struktur der ISMS-Organisation ist unter der Startseite des Aeneis dargestellt.
- Die ISMS-Organisation ist in der Prozesslandkarte zu finden.
- Die Gesamtverantwortung für die Informationssicherheit liegt bei der Krankenhausleitung. Diese besteht aus der Geschäftsführung, dem Ärztlichen Direktor und der Pflegedienstleitung.
- Die Krankenhausleitung delegiert den operativen Betrieb des ISMS an den Informationssicherheitsmanagementbeauftragten (ISMK) und den externen Informationssicherheitsbeauftragten (eISB).
- ISMK und eISB arbeiten zur Erfüllung der ISMS-Prozesse eng zusammen.
- Der eISB wiederum kann zur Erfüllung seiner Aufgaben auf ein ISMS-Kernteam zurückgreifen. Dieses Team besteht aus Vertretern der für den Geltungsbereich des ISMS relevanten Organisationeinheiten.
- Die Vertreter des ISMS-Kernteams setzen sich zusammen aus dem Bereich Qualitätsmanagement, Mitarbeitern der EDV, der Technik und der digitalen Transformation.
- Schließlich nimmt der Datenschutzbeauftragte (DSB) eine wichtige Rolle im ISMS-Kernteam ein, da der Umgang mit persönlichen Daten im Rahmen der Anforderungen der Europäischen

Datenschutzgrundverordnung (EU-DSGVO) eine Reihe von Schnittstellen zur Informationssicherheit hat.
- Die IS-Organisation wird von der Gesamtheit der Mitarbeiter des Krankenhauses unterstützt, ohne deren angepasstes Verhalten die Umsetzung der notwendigen Informationssicherheit nicht erfolgen kann.

Rollen und Verantwortlichkeiten
Krankenhausleitung (KHL):
- Die KHL trägt die Gesamtverantwortung für Informationssicherheit. Sie definiert die Ziele des ISMS und stellt die erforderlichen Ressourcen für das Erreichen der Ziele zur Verfügung.
- Auf der Basis regelmäßiger Managementbewertungen kontrolliert die KHL die Zielerreichung und die kontinuierliche Verbesserung des ISMS.

interner Informationssicherheitsmanagementkoordinator (ISMK):
Zu den Aufgaben des ISMK gehören u.a.:
- zentraler Ansprechpartner für die Koordination, Verwaltung und Kommunikation der Prozesse zur Informationssicherheit des Krankenhauses und kommuniziert direkt an die Krankenhausleitung;
- regelmäßige und anlassbezogene Information und Beratung der KHL zu Themen der Informationssicherheit (z.B. im Rahmen von Management-bewertungen);

Externer Informationssicherheitsbeauftragter (eISB):
- Der eISB ist zentraler Ansprechpartner für alle IS-Themen für Mitarbeiter und Dienstleister. Gemeinsam mit dem ISMK koordiniert er alle Aufgaben und Schnittstellen zum Betrieb des ISMS.

ISMS-Koordinatoren (ISMS-Kernteam):
Die ISMS-Koordinatoren unterstützen als Vertreter relevanter Fachbereiche den ISMK und den eISB im operativen Betrieb des ISMS.

Zu den Aufgaben der ISMS-Koordinatoren gehören u.a.:
- Umsetzung der IS-Richtlinien in ihrem Verantwortungsbereich durch technische und organisatorische Maßnahmen;
- Einstufen der Schutzbedarfe/Kritikalität der Prozesse/Anwendungen;
- Identifikation und Analyse von Risiken in ihrem Bereich;
- Durchführung von Maßnahmen zur Risikoverminderung;
- Unterstützung des eISB bei Durchführung von Schulungen (Awareness);
- Ermittlung, Umsetzung und Einhaltung von fachspezifischen Anforderungen;
- Meldung von Informationssicherheitsvorfällen an den ISMK;
- Auswertung von Abweichungsberichten in Zusammenarbeit mit ISMK;
- Einleitung von Korrekturmaßnahmen;
- Erstellung und Pflege von fachspezifischen Notfallplänen.

Über die ISMS-Koordinatoren werden die Themen der medizinischen Fachbereiche bzw. der Abteilungen in das ISMS-Kernteam eingebracht.

Datenschutzbeauftragter (DSB):

- Da aufgrund der Ziele der Informationssicherheit zur Gewährleistung von Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität sowie der Patientensicherheit und Behandlungsintensität von Informationen eine Reihe von Schnittstellen zum Datenschutz bestehen, stimmt sich der DSB mit ISMK/eISB bei entsprechenden Themen ab.
- Der DSB stellt die Einhaltung datenschutzrechtlicher Anforderungen im ISMS sicher.

ISMS-Kernteam:

Das ISMS-Kernteam setzt sich aus dem ISMK, dem ISB, dem DSB, den ISMS-Koordinatoren und Vertretern der für den Geltungsbereich des ISMS relevanten Organisationeinheiten (insbesondere EDV, Technik, DT) zusammen. Das ISMS-Kernteam kann bei Bedarf durch Experten ergänzt werden.

Zu den Aufgaben des ISMS-Kernteams gehören u.a.:

- Unterstützung des ISMK/ISB bei deren Aufgaben;
- Steuerung, Koordination und Kontrolle der IS-Prozesse;
- Weiterentwicklung der IS-Richtlinien;
- Prüfung der Umsetzung der IS-Ziele und IS-Richtlinien;
- Erarbeitung von Verbesserungsvorschlägen zur Erreichung der IS-Ziele;
- Ermittlung von technisch und organisatorischen Maßnahmenoptionen bzw. Schulungsbedarf.

Mitarbeiter (MA):

- Informationssicherheit betrifft ohne Ausnahme alle Mitarbeiter.
- Jeder Einzelne kann und sollte durch verantwortungs- und sicherheitsbewusstes Handeln dabei helfen, Schäden durch Informationssicherheitsvorfälle zu vermeiden.
- Voraussetzung dafür ist, dass die zentrale Leitlinie zur Informationssicherheit sowie weitere spezifische Richtlinien zur Informationssicherheit den einzelnen Mitarbeitern bekannt gemacht werden.
- Sensibilisierungsmaßnahmen für Informationssicherheit sowie fachliche Schulungen der Mitarbeiter sind eine weitere Grundvoraussetzung für gelebte Prozesse der Informationssicherheit.
- Mitarbeiter melden Informationssicherheitsvorfälle direkt an zuständigen Kontaktdaten (ISB, ISMS-Kernteam).

Kontaktstelle BSI:

Die Kontaktstelle (§ 8b Abs. 3 BSIG) bildet das Bindeglied zwischen dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und dem Krankenhaus.

Falls das Krankenhaus aufgrund des niedrigen Schwellwertes gegenwärtig nicht zur kritischen Infrastruktur zählt, ist eine Meldung gesetzlich nicht gefordert.

Die Kontaktstelle zum BSI wird durch ein Mitglied der IS-Organisation wahrgenommen.

Aufgabe der Kontaktstelle ist:

- die Entgegennahme der vom BSI erhaltenen Informationen und deren Weiterleitung an die für die weitere Bearbeitung zuständigen Stellen in der Organisation;
- die unverzügliche Information an das BSI bei Informationssicherheitsvorfällen mit erheblichen Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit

10 – Informationssicherheitsbewusstsein, -ausbildung und -schulung

Für alle Beschäftigten werden Schulungen durchgeführt, um ein angemessenes Bewusstsein zur Informationssicherheit zu entwickeln. In den Schulungen wird auch auf Änderungen und Aktualisierungen der Richtlinien und Verfahren eingegangen, die für das jeweilige berufliche Arbeitsgebiet relevant sind.

Die Sensibilisierung für Informationssicherheit steht im Einklang mit Informationssicherheitsrichtlinien und relevanten Verfahren des Krankenhauses, unter Berücksichtigung der zu schützenden Information und der schon bestehenden Maßnahmen.

Das Sensibilisierungsprogramm enthält eine Reihe von Sensibilisierungsmaßnahmen, wie regelmäßige Informationen zum Thema Informationssicherheit im Newsletter des Krankenhauses sowie regelmäßig stattfindende Schulungen.

In Zusammenarbeit mit der Leitung wird ein Schulungsplan zur Sensibilisierung der Mitarbeiter sowie Qualifizierung des ISMS Teams erstellt. Diese Schulungen enthalten Aspekte zur

- Verpflichtung der Leitung zu Informationssicherheit
- Notwendigkeit, geltende Regeln und Verpflichtungen zu beachten, wie sie in Richtlinien, Normen, Gesetzen, Verträgen usw. für das Krankenhaus festgelegt wurden
- persönlichen Verantwortung für eigenes Handeln sowie allg. Verantwortung zur Sicherung und Schutz von Informationen des Krankenhauses und externen Partnern
- Einhaltung grundsätzlicher Verfahren zur Informationssicherheit (Meldung über Informationssicherheitsvorfälle) und grundlegender Sicherheitsmaßnahmen (wie Kennwortsicherheit, Maßnahmen bei Schadsoftware und aufgeräumter Schreibtisch)

Bei der Ausarbeitung eines Sensibilisierungsprogramms wird nicht nur das „Was“ und „Wie“, sondern auch das „Warum“ berücksichtigt. Es ist wichtig, dass die Mitarbeiter das Ziel der Informationssicherheit und die möglichen positiven und negativen Auswirkungen ihres Verhaltens verstehen.

Maßnahmen des Sensibilisierungsprogramms werden zeitlich geplant und regelmäßig durchgeführt, damit auch neue Beschäftigte und Auftragnehmer geschult werden.

Für die Beurteilung des Verständnisses wird ein Wissenstest am Ende des Sensibilisierungs-, Aus- und Weiterbildungskurses durchgeführt.

11 – Gültigkeit

Dieses Dokument ist gültig ab seiner Freigabe. Es wird im Intranet für alle Mitarbeiter bereitgestellt. Diese Leitlinie wird unter Verantwortung des Informationssicherheitskoordinators (ISMK) am Krankenhaus mindestens einmal jährlich geprüft und gegebenenfalls in Abstimmung mit der Geschäftsleitung aktualisiert.

Diese Leitlinie hat die Geschäftsführung des Krankenhauses freigegeben.