1 INHALTSVERZEICHNIS

2 GENERELLE INFORMATIONEN

2.1 Ziel und Zweck des Dokumentes

Durch das Voranschreiten der Digitalisierung und der hohen Abhängigkeit von der Informationstechnologie, ist Informationssicherheit mehr und mehr Schlüssel zum Erfolg und Voraussetzung für robuste Prozesse geworden. Ziel dieses Dokumentes ist die Festlegung klarer Regeln für den Umgang mit Informationswerten des Klinikums Aschaffenburg-Alzenau.
Dieses Dokument ist sowohl für alle Mitarbeiter des Klinikums als auch für externe Dienstleister sowie weitere Dritte mit Zugriff auf Informationswerte bestimmt.

Die im Text gewählte männliche Form bezieht immer gleichermaßen Personen aller Geschlechter mit ein. Auf eine Mehrfachbezeichnung wurde aufgrund einfacherer Lesbarkeit verzichtet.

2.2 Freigabe

Das vorliegende Dokument tritt nach Zustimmung des Betriebsrats mit seiner Freigabe durch die Krankenhausführung in Kraft.

2.3 Revision

Dieses Dokument sowie die daraus sich ergebenden Sicherheitsmaßnahmen und Ziele unterliegen der Dokumentenlenkung [1]. Eine regelmäßige Revision erfolgt gemäß den dort spezifizierten Vorgaben.

2.4 Mitgeltende Unterlagen

[1] Richtlinie Dokumentenlenkung

[2] Handbuch Risikomanagement

[3] Geschäftsordnung

3 EINLEITUNG

3.1 Rahmenbedingungen

Ein Informationssicherheitsmanagementsystem (ISMS) wahrt die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.
Die entsprechenden Forderungen bestehen aufgrund verschiedener Regelungen:

- Sorgfaltspflicht – Sorgfältige Führung des Unternehmens;
- Überwachungspflicht – Verhinderung zukünftiger Rechtsverstöße im Unternehmen;
- Gesetzliche Verpflichtung zum Schutz personenbezogener Daten auf der Basis der EU DSGVO;
- Dem IT-Sicherheitsgesetz (IT-SIG) zur Informationssicherheit von kritischen Infrastrukturen (KRITIS),
- Dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI Gesetz – BSIG)

Zu berücksichtigen ist auch, dass die Folgen einer unangemessenen Informationssicherheit nicht auf das Klinikum begrenzt bleiben, sondern sich auf Mitarbeiter, Patienten und Dritte auswirken können.

3.2 Risiken für Patientendaten

Zum Schutz der sensiblen Patientendaten werden dem Risiko entsprechende Sicherheitsmechanismen eingesetzt. Ein unbefugter Zugriff auf diese Daten hätte neben den rechtlichen Konsequenzen einen erheblichen Image- und Vertrauensverlust zur Folge. Dennoch ist es zweckgebunden erforderlich, diese Daten nach Maßgabe entsprechender Regularien anderen zugänglich zu machen oder zu übertragen.

3.3 Risiken für Unternehmensdaten

In gleichem Maße wie die Patientendaten müssen auch Unternehmensdaten einschließlich Mitarbeiterdaten vor unbefugten Zugriffen oder ungewollten Übertragungen geschützt werden. Die stetig wachsende Vernetzung mit externen Stellen (z.B. Finanzamt, Banken, Krankenversicherungen, Lieferanten, etc.) erhöht die Risiken auch für Unternehmensdaten.
Daher gelten auch für Unternehmensdaten dieselben Grundregeln zur Absicherung wie für die Absicherung von Patientendaten.

4 Leitlinie des Klinikums Aschaffenburg-Alzenau zur Informationssicherheit und zum Datenschutz

Der Einsatz von moderner IT, sowie Medizin- und Kommunikationstechnik ist wesentlich für die Aufgabenerfüllung des Klinikums Aschaffenburg-Alzenau. Als Klinikum der Schwerpunktversorgung II werden die Prozesse in allen patientenabhängigen und kaufmännischen Bereichen maßgeblich durch die IT getragen. Teile der Infrastruktur des Klinikums werden für die Aufrechterhaltung der Patientenversorgung als kritisch eingestuft. Ein Ausfall von kritischen Systemen bzw. kritischer Infrastruktur gefährdet den Geschäftsbetrieb und die Patientenversorgung. Die Sicherheit der Informationsverarbeitung spielt daher eine Schlüsselrolle für unsere Aufgabenerfüllung.
Für die Patientenversorgung müssen schutzbedürftige Gesundheitsdaten der Patienten verarbeitet werden. Auch im Rahmen der übrigen Geschäftsprozesse ist die Verarbeitung von vertraulichen Daten, wie zum Beispiel Personaldaten oder Geschäftsgeheimnissen erforderlich.
Die Vertraulichkeit von schutzbedürftigen Daten und die Aufrechterhaltung der Patientenversorgung und wichtiger Geschäftsprozesse werden durch wirksame und angemessene technische und organisatorische Maßnahmen sichergestellt.
Um dies zu gewährleisten wird vom Klinikum Aschaffenburg-Alzenau ein Informationssicherheits- und Datenschutzmanagementsystem aufgebaut, betrieben und kontinuierlich weiterentwickelt. Das Informationssicherheitsmanagementsystem (ISMS) trägt dazu bei, die gesetzlichen Anforderungen des Datenschutzes umzusetzen.
Die vorliegende Leitlinie definiert die Ziele der Organisation im Bereich der Informationssicherheit unter Berücksichtigung der gesetzlichen Anforderungen.
Die zur Gewährleistung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen im Bereich des Datenschutzes erforderlichen Aufgaben und Pflichten gegenüber unseren Patienten, Kunden, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten werden in dieser Leitlinie festgelegt. Diese Aufgaben und Pflichten sind in Betriebsvereinbarungen, Richtlinien und Arbeitsanweisungen weiter konkretisiert.
Ferner werden die Sicherheitsstrategie, die Sicherheitsorganisation und die Sicherheitsziele des Klinikums Aschaffenburg-Alzenau definiert.
Mit dieser Sicherheitsleitlinie bekennt sich die Krankenhausführung zu ihrer Verantwortung für die Informationssicherheit und für den Datenschutz.
Alle Mitarbeiterinnen und Mitarbeiter des Klinikums Aschaffenburg-Alzenau sind aufgefordert, im Rahmen ihrer beruflichen Tätigkeit auf die Einhaltung der in dieser Leitlinie definierten Ziele hinzuwirken. Dies gilt insbesondere für Führungskräfte, die dafür verantwortlich sind, sowohl durch ihr Vorbild als auch durch ihre Anleitung ihre Mitarbeiter bei der Umsetzung der Regelungen zur Einhaltung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen des Datenschutzes zu unterstützen.
Die Gesamtverantwortung für die Informationssicherheit und den Datenschutz obliegt der Geschäftsführung des Klinikums und der Krankenhausleitung, die dabei vom Informationssicherheits- und Datenschutzbeauftragten (ISB/DSB) unterstützt und beraten wird.

5 Berücksichtigung des Datenschutzes

Die Anforderungen des Datenschutzes basierend auf der DSGVO decken sich teilweise mit den Anforderungen der Informationssicherheit im Sinne der einschlägigen Normen, wie der ISO/IEC 27001. Maßnahmen, die die Schutzziele der DSGVO gemäß Art. 32 Abs. 1 sicherstellen, entsprechen Maßnahmen, die auch von der Norm ISO/IEC 27001 gefordert werden. Dementsprechend können durch die Integration von Datenschutz und Informationssicherheit sowohl auf der Ebene des Managementsystems als auch auf der Ebene der Umsetzung von konkreten Maßnahmen Synergien genutzt werden. Die normative Grundlage für die Informationssicherheit bildet die ISO/IEC 27001, die über die Compliance-Anforderungen in A.18, insbesondere A.18.1.4 auch die DSGVO mit einschließt.

6 Berücksichtigung des BSI-Gesetzes und der Kritis-Verordnung

Das Klinikum Aschaffenburg-Alzenau zählt gemäß dem BSI-Gesetz (BSIG) und der Kritis-Verordnung im Bereich der stationären Versorgung zu den Betreibern „Kritischer Infrastruktur". Gemäß § 8a Abs. 1 BSIG sind Betreiber Kritischer Infrastrukturen verpflichtet, spätestens zwei Jahre nach Inkrafttreten der Rechtsverordnung nach § 10 Abs. 1 BSIG angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit der von ihnen betriebenen Kritischen Infrastrukturen maßgeblich sind. § 8a Abs. 2 BSIG fordert den Nachweis der Umsetzung durch Sicherheitsaudits, Prüfungen oder Zertifizierungen. Der Nachweis ist alle 2 Jahre neu zu erbringen.

7 Normative Grundlage und Schutzziele

Unter Berücksichtigung der Anforderungen der DSGVO gemäß Art. 32 Abs. 1 lit. b), des BSIG sowie des B3S für die Gesundheitsversorgung im Krankenhaus (22.10.2019) ergeben sich folgende Schutzziele:

- Gewährleistung der **Vertraulichkeit** von schutzbedürftigen Daten
- Gewährleistung der **Integrität** aller relevanten Daten
- Gewährleistung der **Verfügbarkeit** von relevanten Prozessen und kritischer Infrastruktur
- Gewährleistung der **Authentizität** von relevanten Daten
- Gewährleistung der **Belastbarkeit** (Resilienz) kritischer Systeme und Infrastruktur

Bei der Bewertung der Risiken werden für jedes Schutzziel die Faktoren Patientensicherheit und Behandlungseffektivität berücksichtigt.

8 Geltungsbereich

Entsprechend den Anforderungen des BSIG ergibt sich folgender Geltungsbereich für das Informationssicherheitsmanagementsystem
Prozesse, interne und externe IT-basierte Dienste und der Betrieb von dazu genutzten IT-Systemen einschließlich der Medizin- und Kommunikationstechnik und kritischen Infrastrukturkomponenten für die beiden Standorte des Klinikums Aschaffenburg-Alzenau, die für die stationäre Versorgung von Patienten erforderlich sind in den Bereichen

- Stationäre Versorgung
- Technik (Versorgungs-, Gebäudesicherheit)
- Apotheke
- Einkauf (alle beschaffenden Stellen)
- Labor

9 VERPFLICHTUNG VON GESCHÄFTSFÜHRUNG UND FÜHRUNGSKRÄFTEN

Mit dieser Leitlinie legt die Krankenhausführung die Informationssicherheitspolitik und die Informationssicherheitsziele fest. Die Krankenhausführung stellt sicher, dass die in dieser Leitlinie festgelegten Ziele und die Umsetzung des Informationssicherheitsmanagementsystems mit der strategischen Ausrichtung der Organisation vereinbar ist. Sie bestimmt die erforderlichen Ressourcen für den Aufbau, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung des Informationssicherheitsmanagementsystems und stellt diese bereit.
Mit Unterstützung aller Führungskräfte stellt die Krankenhausführung sicher, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der Organisation integriert werden. Die Geschäftsführung und alle Führungskräfte sind dafür verantwortlich, die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der gesetzlichen und normativen Anforderungen zur Informationssicherheit und zum Datenschutz zu vermitteln. Mit Unterstützung des Informationssicherheits- und Datenschutzbeauftragten (ISB/DSB) sowie aller Führungskräfte stellt die Krankenhausführung sicher, dass das Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt und der Datenschutz innerhalb der Organisation sichergestellt wird. Die Führungskräfte sind dafür verantwortlich, ihre Mitarbeiter und gegebenenfalls auch die Mitarbeiter von involvierten Dienstleistern anzuleiten und dabei zu unterstützen, zur Wirksamkeit des Informationssicherheitsmanagementsystems beizutragen und sicherzustellen, dass die gesetzlichen Anforderungen zum Datenschutz umgesetzt werden. Die Unternehmensführung unterstützt die Fortbildung der Führungskräfte zum Thema Informationssicherheit und Datenschutz. Unternehmensführung und Führungskräfte fördern die fortlaufende Verbesserung der Informationssicherheit und des Datenschutzes.

10 SICHERHEITSSTRATEGIE

Die Gewährleistung der Vertraulichkeit von personenbezogenen Daten und insbesondere von Gesundheitsdaten (bzw. personenbezogenen Daten der besonderen Kategorien im Sinne von Art. 9 Abs. 1 DSGVO) hat einen hohen Stellenwert für das Klinikum Aschaffenburg-Alzenau.
Bei der Planung und Umsetzung von Geschäftsprozessen werden die Vertraulichkeit, die Integrität, und die Authentizität der Daten sowie die Verfügbarkeit der Geschäftsprozesse und der dazu erforderlichen Systeme und Infrastruktur sowie die Resilienz der Systeme sichergestellt. Dabei muss gewährleistet werden, dass die getroffenen Maßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf stehen.
Durch das Risikomanagement wird sichergestellt, dass Risiken identifiziert und mit angemessenem Aufwand durch geeignete und wirksame Maßnahmen reduziert werden. Dabei werden insbesondere folgende Kategorien von Gefährdungen berücksichtigt:

- Höhere Gewalt
- Organisatorische Mängel
- Menschliche Fehlhandlungen
- Technisches Versagen
- Vorsätzliche Handlungen

11 SICHERHEITSZIELE

- Die Patientenversorgung, kritische Geschäftsprozesse sowie alle dazu erforderlichen IT-Systeme und Infrastruktur sind hinsichtlich ihrer Verfügbarkeit so weit abgesichert, dass gegebenenfalls zu erwartende Ausfallzeiten toleriert werden können und diese keine wesentlichen Auswirkungen auf den Geschäftsbetrieb haben.
- Fehlfunktionen in IT-Systemen, die gegebenenfalls zum Verlust der Integrität der auf ihnen verarbeiteten Daten führen, sind nur in Ausnahmefällen akzeptabel. Fehlfunktionen in Systemen der Medizintechnik, die das Patientenwohl gefährden können, sind inakzeptabel.
- Die Vertraulichkeit von Patientendaten wird sichergestellt. Die gesetzlichen Anforderungen zum Datenschutz und die ärztliche Schweigepflicht werden durchgängig gewährleistet.

- Für die personenbezogenen Daten der Mitarbeiter und die IT-Anwendungen der Personalabteilung wird ein hoher Vertraulichkeitsschutz gewährleistet. Gleiches gilt für die Daten unserer Geschäftspartner.
- Das Risiko materieller und immaterieller Folgen für das Unternehmen, die Patienten sowie für die Mitarbeiter durch Verstöße gegen die Datenschutz Vorschriften wird (z.B. durch interne Audits und Risikoanalysen) bestimmt und durch geeignete technische und organisatorische Maßnahmen systematisch reduziert.
- Verspätete oder fehlerhafte Managemententscheidungen können weitreichende Folgen nach sich ziehen. Daher ist für das Management bei wichtigen Entscheidungen der Zugriff auf aktuelle Steuerungsdaten wichtig. Für diese Informationen ist ein hohes Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität sicher zu stellen.
- Die Nutzung des Internets zur Informationsbeschaffung und zur Kommunikation ist für uns selbstverständlich. E-Mail ist ein essentielles Medium in der Bürokommunikation. Durch entsprechende Maßnahmen (z.B. Schulungen, verschlüsselte Kommunikation) wird sichergestellt, dass die Risiken der Internet- und E-Mail-Nutzung auf ein akzeptables Maß reduziert werden.
- Medizinische Daten, die für die Forschung genutzt werden, werden nur pseudonymisiert bzw. anonymisiert und mit Einwilligung der Patienten dem jeweiligen Forschungsinstitut zur Verfügung gestellt. Forschung mit Patientendaten darf nur im Rahmen der gesetzlichen Vorgaben des Bayerischen Krankenhausgesetzes mittels der vom Klinikum etablierten Verfahren durchgeführt werden.
- Mitarbeiter, Führungskräfte und die Unternehmensführung sind sich ihrer Verantwortung im Umgang mit der IT bewusst und unterstützen die Sicherheitsstrategie. Sie kennen die einschlägigen Gesetze und Verordnungen (z. B. Strafgesetzbuch, Betriebsverfassungsgesetz, Handelsgesetzbuch, Sozialgesetz-buch, Gesetze und Regelungen zum Datenschutz, usw.) und die vertraglichen Regelungen und halten diese ein.
- Auch zeitweilig beschäftigtes Personal oder Freiwillige bzw. unterstützendes Personal wie Studenten, kirchliches Personal oder Personal von Wohltätigkeitsorganisationen folgen den vom Klinikum bereitgestellten Vereinbarungen, in denen die Grenzen der Befugnisse z. B. für den Zugriff auf persönliche Gesundheitsinformationen definiert sind.

12 SICHERHEITSMAßNAHMEN

- Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist der jeweilige Schutzbedarf bestimmt und sind Zugriffsberechtigungen je nach Aufgabenstellung vergeben.
- Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein Rollen- und Berechtigungskonzept geschützt.
- Computer-Schadsoftware-Schutzprogramme werden sofern möglich auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch einen geeigneten Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Systeme werden in regelmäßigen Abständen auf Ihre Aktualität und Sicherheitsrelevanz überprüft und Updates durchgeführt. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.
- Durch eine umfassende Datensicherung wird gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind. Informationen physischer Natur werden einheitlich gekennzeichnet und so aufbewahrt, dass sie schnell auffindbar sind.
- Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.
- IT-Benutzer nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Schulungen werden vom internen Dienstleister unter Einbindung des ISB organisiert. Die Fachbereiche legen unter Einbindung des Betriebsrates fest, welche Schulungen als Pflichtschulung angesetzt werden. Der Vorstand bzw. die Personalabteilung unterstützen dabei die bedarfsgerechte Fort- und Weiterbildung.

13 KONTROLLE

Informationssicherheit erfordert permanente Anstrengungen (Sicherheitsstrategie) und ist folglich keine einmalige Aktivität, sondern ein Prozess.

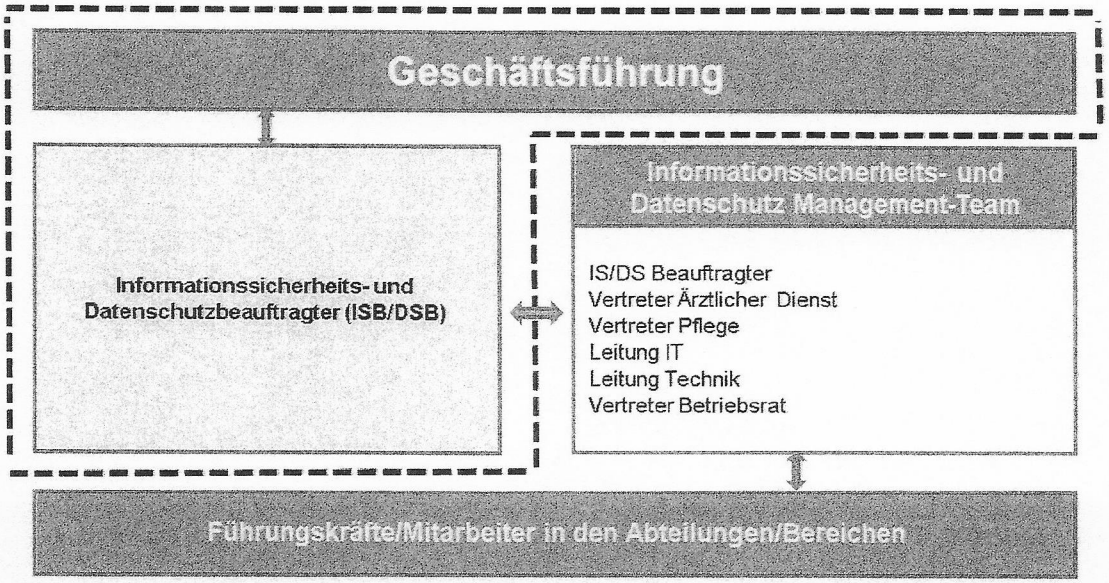
Das Management der Fachbereiche ist dafür verantwortlich implementierte Maßnahmen regelmäßig (z.B. jährlich) auf Ihre Wirksamkeit zu prüfen. Diese Prüfungen und Ergebnisse werden dokumentiert und evaluiert. Festgestellte Mängel werden dem Risiko entsprechend zeitnah behoben. Der ISB/DSB stellt das Rahmenwerk und die Werkzeuge für diese regulären Prüfungen zur Verfügung.

Durch zusätzliche Prüfungen unter der Verantwortung des ISB/DSB stellt dieser fest, ob eine effektive Kontrolle der Wirksamkeit der Maßnahmen gegeben ist. Die Prüfungen und Ergebnisse werden dokumentiert. Festgestellte Mängel werden dem Risiko entsprechend zeitnah behoben.

Die gewählten Maßnahmen werden regelmäßig evaluiert um festzustellen, ob diese noch ausreichen oder an welcher Stelle Anpassungen erforderlich sind.

14 ORGANISATION DES INFORMATIONSSICHERHEITS- & DATENSCHUTZMANAGEMENTS

Zur Erreichung der Informationssicherheitsziele hat das Klinikum Aschaffenburg-Alzenau eine Sicherheitsorganisation implementiert.



Informationssicherheits- und Datenschutzbeauftragter (DSB/ISB):
Aufgrund der Synergien im Informationssicherheits- und Datenschutzmanagement ist im Klinikum Aschaffenburg-Alzenau ein Informationssicherheits- und Datenschutzbeauftragter (ISB/DSB) in einer Person bestellt. Der Beauftragte ist in Form einer Stabsstelle unmittelbar der Geschäftsführung unterstellt. Er arbeitet weisungsfrei und berichtet direkt an die Geschäftsführung. Rollen und Aufgaben beider Funktionen sind in einer Geschäftsordnung beschrieben. Diese beinhaltet auch das Vorgehen bei möglichen Interessenskonflikten beider Funktionen.
Der Informationssicherheits- und Datenschutzbeauftragte wird von allen Führungskräften bei der Erfüllung seiner Aufgaben unterstützt. Ihm werden die zur Erfüllung seiner Aufgaben erforderlichen Ressourcen zur Verfügung gestellt. Dazu gehört die regelmäßige Teilnahme an Fortbildungsmaßnahmen, angemessene Unterstützung bei der Durchführung von internen Auditierungen sowie die Unterstützung bei der Ausübung seines Weisungsrechts im Kontext der Informationssicherheit bzw. des Datenschutzes.

Der ISB/DSB unterstützt alle Führungskräfte und Mitarbeiter und gegebenenfalls auch Mitarbeiter von Dienstleistern bei der Umsetzung der Regelungen zur Einhaltung der Informationssicherheit und der gesetzlichen Anforderungen zum Datenschutz im Klinikum Aschaffenburg-Alzenau.

Risikomanagement und Datenschutz
Das Risikomanagement stellt sowohl für den Datenschutz im Sinne der DSGVO als auch für das Informationssicherheitsmanagement ein wichtiges Hilfsmittel dar. Die methodische Verantwortung für das Risikomanagement hat der Risikomanagementbeauftragte. Das Risikomanagement des Klinikums kommt soweit möglich für alle Bereiche des Klinikums zur Anwendung. Dabei wird den besonderen Anforderungen des Datenschutzes und der Informationssicherheit Rechnung getragen.
Das Qualitätsmanagement unterstützt im Rahmen seiner Aufgaben sowohl den Datenschutz als auch die Informationssicherheit und stellt insbesondere eine unternehmensweit einheitliche Dokumentenlenkung sicher.

Informationssicherheits- und Datenschutz-Management-Team
Um die Integration von Managementsystemen innerhalb der Organisation zu fördern, wird ein IS/DS-Management-Team eingerichtet.
Das IS/DS-Management-Team unterstützt den ISB/DSB, indem es übergreifende Maßnahmen in der Gesamtorganisation koordiniert, Informationen zusammenträgt und Kontrollaufgaben durchführt.
Das Team setzt sich aus Vertretern der folgenden Bereiche zusammen:

- Informationssicherheit- und Datenschutz
- Medizinischer Bereich (Ärztlicher Dienst und Pflege)
- IT
- Technik
- Betriebsrat

Die regelmäßigen Teilnehmer (Kernteam) sind:

- Informationssicherheits- und Datenschutzbeauftragter
- Vertreter des Ärztlichen Dienstes
- Vertreter des Pflegedienstes
- Leiter IT
- Leiter Technik
- Vertreter Betriebsrat

Anlassbezogen können weitere Teilnehmer hinzugezogen werden.

Das IS/DS-Management-Team berichtet an die Geschäftsführung. Relevante Entscheidungen hinsichtlich des Informationssicherheits- und Datenschutzmanagement werden im interdisziplinär besetzten Gremium der Fachgruppenkonferenz des Klinikums verabschiedet.
Weitere Einzelheiten zur Organisation und zur Arbeitsweise des Informationssicherheits- und Datenschutz-Management-Teams werden in einer Geschäftsordnung beschrieben.

15 Einbindung von Informationssicherheit & Datenschutz innerhalb der Organisation

Der Informationssicherheits- und Datenschutzbeauftragte muss frühzeitig in alle relevanten Projekte eingebunden werden, damit schon in der Planungsphase sicherheitsrelevante Aspekte berücksichtigt werden können. Gleiches gilt für die Verarbeitung von personenbezogenen Daten.
Alle IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des Informationssicherheits- und Datenschutzbeauftragten zu halten.
Alle Mitarbeiter des Klinikums-Aschaffenburg-Alzenau sind aufgefordert, tatsächliche und gegebenenfalls auch vermutete Abweichungen von den Vorgaben dieser Leitlinie oder anderer Regelungen die Informationssicherheit oder den Datenschutz betreffen an den Informationssicherheits- und Datenschutzbeauftragten zu melden. Meldungen zum Datenschutz werden vertraulich behandelt. Meldungen hinsichtlich der Informationssicherheit können auf Wunsch des Meldenden und soweit dies im Rahmen der Ziele dieser Informationssicherheitsleitlinie möglich ist, gegebenenfalls vertraulich behandelt werden.

16 KONTINUIERLICHE VERBESSERUNG DER INFORMATIONSSICHERHEIT UND DES DATENSCHUTZES

Das Informationssicherheits- und Datenschutzmanagementsystem wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar und integriert sind.
Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und diese ständig auf dem aktuellen Stand der Technik und konform zu den jeweiligen gesetzlichen Regelungen und normativen Vorgaben zu halten.

Gezeichnet:

Geschäftsführung
Ärztlicher Direktor
Zentrale Pflegedienstleitung
Kaufmännischer Leiter (Prokurist)
Technischer Leiter (Prokurist)
Betriebsrat
ISB/DSB

17 DOKUMENTENINFORMATIONEN

Revisionshistorie				
Datum	**Revisionsstand**	**Revision/Prüfung/Stillegung**	**Änderung**	**Ausführender**
12.02.19	Entwurf	Erstellung		D. Sauer
12.02.20	Entwurf	Überarbeitung	Anpassung an neue Führungsstruktur	P. Schneider
30.03.20	Rev01	Freigabe		KH Leitung