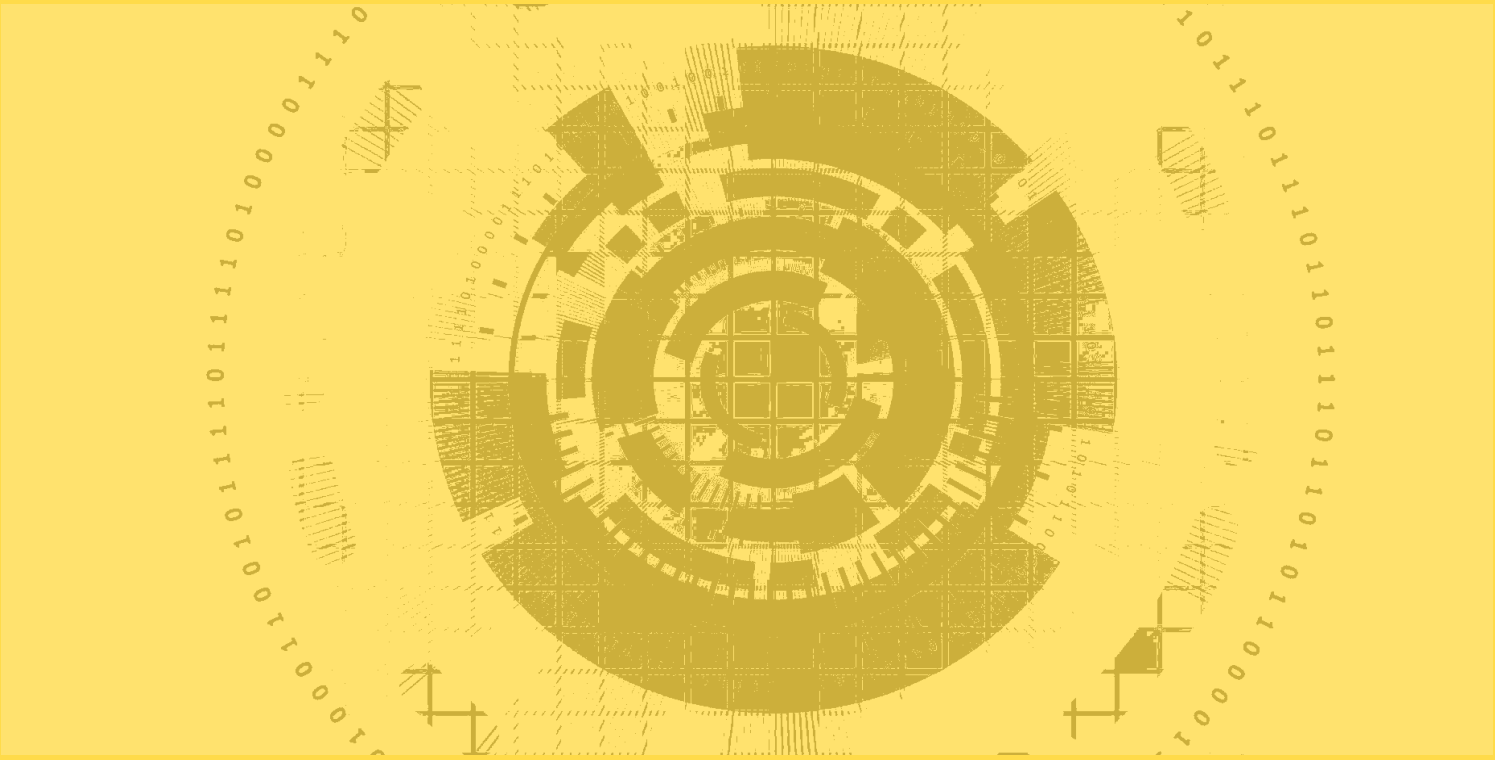
Cyber-Sicherheits Deutschland e.V.

Der Informationssicherheits-beauftragte im Krankenhaus

Organisatorische Einordnung, Aufgaben und Aufwandsübersicht



Information für die Krankenhausleitung und Arbeitshilfe für den Informationssicherheitsbeauftragten

Inhalt

Dokumenteninformation

Klassifizierung

Schutzklasse	Öffentlich
Freigaben	Ablage: keine Vorgaben, beliebige Ablage
	Übermittlung: keine Vorgaben, beliebige Übermittlung
	Ausdruck: keine Vorgaben, jeglicher Ausdruck ist zulässig
	Entsorgung (löschen, vernichten): keine Vorgaben, beliebige Entsorgung

Haftungsausschluss

Dieses Dokument sowie dazugehörige Arbeitshilfen wurden mit größter Sorgfalt erstellt und geprüft, erheben jedoch keinen Anspruch auf Vollständigkeit. Sie geben ausschließlich den Stand zum Zeitpunkt ihrer Erstellung wieder und ersetzen keine individuelle Prüfung. Insofern übernimmt der Cybersicherheitsrat Deutschland e.V. keine Haftung für die Anwendung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen.

Autoren

Bei der Erstellung des vorliegenden Dokuments haben die nachfolgend genannten Beteiligten ihre Expertise eingebracht. Die Beteiligten werden in alphabetischer Reihenfolge aufgeführt.

Name	Unternehmen
Arfwedson, Jan	AuraSec GmbH Leiter eHealth Hub im CSRD e.V.
Benda, Dr. Heidrun	Landesamt für Sicherheit in der Informationstechnik, Bayern
Ferenczy, Florian	AuraSec GmbH
Giese, Karin	Sana Kliniken AG
Leonard, Dr. Thomas	AuraSec GmbH

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

1 Ausgangssituation

Krankenhäuser und viele andere Einrichtungen des Gesundheitswesens tragen in mehrfacher Hinsicht eine besondere Verantwortung für die Resilienz ihrer IT-Infrastrukturen. Die Versorgung von Patientinnen und Patienten mit Unterstützung modernster IT-Systeme muss ebenso zuverlässig gewährleistet sein wie der Schutz sensibler Patientendaten.

Öffentlich bekannt gewordene IT-Sicherheitsvorfälle in Kliniken und Krankenhäusern zeigen, dass medizinische Einrichtungen zunehmend gezielt, aber auch ungezielt Opfer eines Cyber-Angriffs werden können. Auch die veränderte weltpolitische Lage muss zukünftig ggf. stärker bei der Konzeption von Sicherheitsmaßnahmen zum Schutz von kritischen Infrastrukturen berücksichtigt werden.

Nicht zuletzt aufgrund der zunehmenden Digitalisierung im Bereich der medizinischen Versorgung stehen vor allem Krankenhäuser vermehrt vor großen Herausforderungen im Hinblick auf die Absicherung und die Resilienz ihrer IT-Systeme, -Prozesse und -Komponenten, die für die medizinische Versorgung relevant sind.

2 IT-Sicherheitsanforderungen an Kliniken/Krankenhäuser

Diesen Handlungsbedarf hat der Gesetzgeber erkannt und bereits mit dem IT-Sicherheitsgesetz in 2015 bzw. der BSI-KRITIS-Verordnung in 2017 adressiert und Universitätskliniken sowie Großkrankenhäuser dazu verpflichtet, entsprechende Sicherheitsmaßnahmen zu implementieren und die effektive Umsetzung gegenüber dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nachzuweisen. Auch für Krankenhäuser unterhalb des Schwellenwertes aus der BSI-Kritis Verordnung, der aktuell bei 30.000 stationären Behandlungsfällen pro Jahr liegt, rückt IT- und Informationssicherheit immer stärker in den Fokus.
Mit Wirkung vom 01.01.2022 sind aufgrund des § 75c SGB V nicht nur die KRITIS-Kliniken, sondern nun alle rund 1.900 bundesdeutschen Kliniken gefordert, den Prozess ihrer kritischen Dienstleistung zu analysieren, um diesen durch die Umsetzung von technischen und organisatorischen IT-Sicherheitsmaßnahmen bestmöglich schützen zu können.

Patientendatenschutzgesetz (PDSG) bzw. Ergänzung des § 75 SGB V Maßnahmen für mehr IT-Sicherheit ab 2022 verpflichtend für alle Kliniken

Im Oktober 2020 wurde das Patientendaten-Schutz-Gesetz (PDSG) beschlossen; ein Artikelgesetz, welches viele andere Gesetze verändert bzw. ergänzt, darunter auch den neuen § 75c SGB V.

(1) Ab dem 1. Januar 2022 sind Krankenhäuser verpflichtet, nach dem Stand der Technik angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit sowie der weiteren Sicherheitsziele ihrer informationstechnischen Systeme, Komponenten oder Prozesse zu treffen, die für die Funktionsfähigkeit des jeweiligen Krankenhauses und die Sicherheit der verarbeiteten Patienteninformationen maßgeblich sind.

(2) Die Krankenhäuser können die Verpflichtungen nach Absatz 1 insbesondere erfüllen, indem sie einen branchenspezifischen Sicherheitsstandard für die informationstechnische Sicherheit der Gesundheitsversorgung im Krankenhaus in der jeweils gültigen Fassung anwenden, dessen Eignung vom Bundesamt für Sicherheit in der Informationstechnik nach § 8a Absatz 2 des BSI-Gesetzes festgestellt wurde.

Unter „angemessenen organisatorischen und technischen Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit" wird ein sogenanntes Informationssicherheitsmanagementsystem (ISMS) verstanden.
Solch ein ISMS beschreibt auch der Branchenspezifische Sicherheitsstandard (B3S) für die medizinische Versorgung, welcher 168 Maßnahmen aufführt, die nötig sind, um eine resiliente Informationstechnik zu gewährleisten und die medizinische Versorgung, die Patientensicherheit und die Behandlungseffektivität sicherzustellen.

Siehe hierzu auch das Dokument Information für KH-Geschäftsführer §75c SGB V, welches die Deutsche Krankenhausgesellschaft e.V. veröffentlicht hat.

3 Organisation der Informationssicherheit

3.1 Aufgaben der Krankenhaus-Leitung und Einordnung/Abgrenzung zum Informationssicherheitsbeauftragten

Die Krankenhausleitung hat die notwendigen Voraussetzungen für die sachgerechte und angemessene Umsetzung von Sicherheitsmaßnahmen entsprechend dem BS3 med. Versorgung oder alternativer normativer Grundlagen, wie der Norm ISO 27001 oder dem BSI-Grundschutz, zu schaffen. Dazu gehört insbesondere die Bereitstellung von angemessenen Ressourcen und das Zuweisen von entsprechenden Verantwortlichkeiten innerhalb der Organisation.

Die Krankenhaus-Leitung trägt die Gesamtverantwortung für die Umsetzung und kontinuierlichen Verbesserung der erforderlichen technischen und organisatorischen Maßnahmen. Sie muss sicherstellen, dass ein wirksames Informationssicherheitsmanagementsystem (ISMS) aufgebaut und betrieben wird. Dies umfasst, entsprechende Ziele der Informationssicherheit in Form von Leit- und Richtlinien bekanntzugeben und durchzusetzen, Rollen und Verantwortlichkeiten zuzuweisen, notwendige Ressourcen bereitzustellen und sowohl im Innen- als auch Außenverhältnis die Bedeutung des Informationssicherheitsmanagements glaubhaft und nachhaltig zu vermitteln.

Eine zentrale Rolle in dem kontinuierlichen Verbesserungsprozess der Informationssicherheit kommt dem Informationssicherheitsbeauftragten (ISB) zu. Dieser ist zuständig für alle Belange der Informationssicherheit innerhalb des Krankenhauses. Er unterstützt die Leitungsebene bei deren Aufgaben bezüglich der Informationssicherheit.

Abb.: Organisation der Informationssicherheit im Krankenhaus

Der Informationssicherheitsbeauftragte muss sowohl bei der Organisation des Aufbaus als auch bei der Durchführung und Überwachung der für die Informationssicherheit notwendigen Maßnahmen unterstützt werden. Hierfür muss ein Informationssicherheitsmanagement-Team (ISM-Team) gebildet werden, dessen Arbeit der ISB koordiniert (siehe Grafik).

Für weitere Informationen zu den Verantwortlichkeiten der Krankenhausleitung im Informationssicherheitsmanagement siehe Branchenspezifischer Sicherheitsstandard, Kap. 7.2.1 ff.

3.2 Der Informationssicherheitsbeauftragte (ISB)

Der Informationssicherheitsbeauftragte (im Folgenden „ISB") erfüllt eine zentrale Rolle bei Aufbau, Betrieb, Überwachung und Verbesserung des Informationssicherheitsmanagements im Krankenhaus.

3.2.1 Abgrenzung IT-Sicherheitsbeauftragter vs. Informationssicherheitsbeauftragter

In den Dokumenten und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik wurde in der Vergangenheit die Bezeichnung „IT-Sicherheitsbeauftragter (IT-SiBe)" verwendet, da dieser Begriff in Unternehmen und Behörden lange Zeit üblich war.

Mit dem Titel „Sicherheitsbeauftragter" werden dagegen häufig diejenigen Personen bezeichnet, die für Arbeitsschutz, Betriebssicherheit oder Werkschutz zuständig sind. Aus diesen Titeln folgt aber auch häufig ein anderes Rollenverständnis.

Mit dem neuen IT-Grundschutz (200-x) wurde die Namensgebung des Verantwortlichen für Informationssicherheit auf den Begriff „Informationssicherheitsbeauftragter (ISB)" vereinheitlicht. So macht der Titel „Informationssicherheitsbeauftragter" anstelle „IT-Sicherheitsbeauftragter" deutlich, dass diese Person sich um die Absicherung aller Arten von Informationen kümmert und nicht nur um die IT-bezogenen Aspekte.

3.2.2 Unabhängigkeit und organisatorische Zuordnung des ISB

Der ISB muss das direkte und jederzeitige Vorspracherecht bei der Krankenhausleitung haben, um diese über Sicherheitsvorfälle, -risiken und -maßnahmen informieren zu können. Darüber hinaus muss er aber auch über das Geschehen im Krankenhaus, bspw. geplante Projekte, Beschaffungsvorhaben, soweit es einen Bezug zu seiner Tätigkeit hat, umfassend und frühzeitig unterrichtet und eingebunden werden.

Eine häufige Frage ist, ob die Position des ISB gleichzeitig vom Datenschutzbeauftragten (DSB) wahrgenommen werden kann. Der DSB an sich hat die Aufgabe, alle Aspekte des Datenschutzes (betrifft die Erfassung, Verarbeitung, Aufbewahrung, Übermittlung und Löschung persönlicher und personenbezogener Daten) zu bearbeiten und sorgt für angemessene Umsetzung und Kontrolle. In einem Krankenhaus bzw. bei der Verarbeitung von Gesundheitsdaten ist die Bestellung eines DSB gesetzlich vorgeschrieben.
Die beiden Rollen schließen sich nicht grundsätzlich aus, es sind allerdings einige Aspekte im Vorfeld zu klären:

- Die Schnittstellen zwischen den beiden Rollen sollten klar definiert und dokumentiert werden. So ist jeweils eine Bestellungs-/Benennungsurkunde zu erstellen, in welcher die Aufgaben und Befugnisse dokumentiert sind. Ferner sollte festgelegt werden, wie Interessenskonflikte vermieden werden bzw. wie in Interessenskonflikten verfahren wird.
- Es muss sichergestellt sein, dass der ISB als auch der DSB über ausreichend freie Ressourcen für die Wahrnehmung beider Rollen verfügt.

3.2.3 Aufgaben und Zuständigkeiten

Zu den Aufgabenschwerpunkten des ISB im Krankenhaus zählen:

- Beratung der Klinikleitung in allen Belangen der Informationssicherheit
- Aufbau eines Berichtswesens zur Informationssicherheit
- Entwicklung und Fortschreibung des Informationssicherheitsmanagementsystems (ISMS)
- Untersuchung und Meldung informationssicherheitsrelevanter Ereignisse
- Steuerung und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen
- Identifikation, Analyse und Bewertung von Risiken für die Informationssicherheit
- Unterstützung des Risikomanagements für IT-Netzwerke, die Medizinprodukte beinhalten
- Unterstützung aller Projekte des Klinikums hinsichtlich Fragen der Informationssicherheit
- Initiierung, Vorbereitung und Begleitung von Audits, Begehungen, Penetrationstests und Zertifizierungen
- Unterstützung bei der Umsetzung datenschutzrelevanter IT-Prozesse auf Basis der EU-DSGVO
- Erstellung und Überarbeitung von Vorgaben zur Steigerung des Sicherheitsniveaus der Informationstechnik
- Leitung des Informationssicherheitsmanagementteams
- Fortschrittskontrolle der Realisierung von Informationssicherheitsmaßnahmen
- Koordination der Informationssicherheitsziele mit den Unternehmenszielen

Die einzelnen Aufgaben und Zuständigkeiten des ISB finden sich im Branchenspezifischen Sicherheitsstandard (B3S) für die Gesundheitsversorgung im Krankenhaus in Kapitel 7.2.2.

3.2.4 Befugnisse und Kompetenzen

Der Informationssicherheitsbeauftragte

- ist in allen für die Informationssicherheit relevanten Themen zu informieren (sowohl auf Nachfrage als auch unaufgefordert, soweit eine Relevanz für die Informationssicherheit besteht).
- ist in Vorhaben und Änderungen, die die Informationssicherheit berühren können (z.B. neue IT-Projekte, Änderungen der IT-Infrastruktur, Änderungen von Rahmenbedingungen mit Auswirkungen auf die Informationssicherheit) frühzeitig mit einzubinden.
- hat ein Mitsprache- und Vetorecht bei allen Entscheidungen, die seinen Verantwortungsbereich betreffen (z.B. bei der Initiierung von IT-Projekten, Beschaffung von informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern).
- hat ein direktes Vortragsrecht bei der Geschäftsführung.

- hat ein Vorschlagsrecht bei der Geschäftsführung zu Maßnahmen zur Verbesserung der Informationssicherheit
- hat Zutrittsrecht zu allen Bereichen, in denen Informationstechnik eingesetzt wird und damit zusammenhängend Daten verarbeitet werden, sowie zu allen Bereichen, in denen relevante Geschäftsprozesse und Informationen bearbeitet werden.
- hat im Rahmen seiner 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 müssen hierzu Abstimmungen mit dem Datenschutzbeauftragten, Betriebsrat/Personalrat oder Geheimschutzbeauftragten erfolgen.
- führt regelmäßig Revisionen im Themenbereich der Informationssicherheit durch bzw. veranlasst Revisionen durch unabhängige Dritte und überprüft so das aktuelle Informationssicherheitsniveau in seinem Aufgabenbereich.
- führt regelmäßig Risikoanalysen für den Bereich Informationssicherheit durch.
- vertritt das Unternehmen im Bereich des Informationssicherheitsmanagements.

3.2.5 Auswahl des Informationssicherheitsbeauftragten

Der ISB sollte sowohl Wissen als auch Erfahrung in den Gebieten Informationssicherheit und Informationstechnik besitzen.
Weiterhin sollte er über die folgenden Qualifikationen und Eigenschaften verfügen:

- Identifikation mit den Zielsetzungen der Informationssicherheit
- Grundlegende Kenntnisse über die gängigen IT-Systeme und Prozesse innerhalb des Krankenhauses und, soweit erforderlich, Grundkenntnisse in den Bereichen OT*/Medizintechnik und ICS**/Transportsysteme sowie Gebäudeleittechnik
- Erfahrungen im Risikomanagement, idealerweise im Bereich der Systemanalyse und Kenntnisse über Methoden zur Risikoanalyse
- Kooperations- und Teamfähigkeit (wenige andere Aufgaben erfordern so viel Fähigkeit und Geschick im Umgang mit anderen Personen)
- Fähigkeit zum selbstständigen Arbeiten mit dem Ziel der kontinuierlichen Verbesserung des ISMS bzw. der Erhöhung des Sicherheitsniveaus
- Kommunikations- und Präsentationsfähigkeiten
- Durchsetzungsvermögen aber auch Empathie, die Ziele der Informationssicherheit und die Notwendigkeit von technischen und organisatorischen Maßnahmen effektiv vermitteln/durchsetzen zu können
- Bereitschaft, sich in neue Gebiete einzuarbeiten und Entwicklungen in der IT zu verfolgen (Der ISB sollte sich so aus- und fortbilden, dass er die erforderlichen Fachkenntnisse für die Erledigung seiner Aufgaben besitzt.)

3.2.6 Zusammenarbeit mit der Krankenhausleitung

Ein ISB allein kann nicht für angemessene Sicherheit in allen Bereichen eines Krankenhauses sorgen. Der ISB muss sowohl durch die Krankenhausleitung sowie durch die Mitarbeiter ausreichend unterstützt werden.

Dazu gehört, dass der ISB so früh wie möglich in alle relevanten Prozesse und Projekte eingebunden wird, damit bereits in der Planungsphase sicherheitsrelevante Aspekte berücksichtigt werden.

Die Zusammenarbeit mit den Mitarbeitern und der Ärzteschaft ebenso wie mit Externen verlangt viel Geschick, da diese von der Notwendigkeit der (für sie manchmal nicht unmittelbar ersichtlichen) Informationssicherheitsmaßnahmen überzeugt (Überzeugungsfähigkeit) werden müssen.

In Zweifelsfällen sollte die Krankenhausleitung ihrem ISB den Rücken stärken. Häufig entstehen in der Praxis Situationen, in denen Mitglieder der Führungsebene mit notwendigen Maßnahmen, die vom ISB angeregt und vertreten werden, unzufrieden sind.

* OT: Abkürzung für „Operational Technology"
** ICS: Abkürzung für „Industrial Control Systems"

Die Krankenhausleitung muss in einer solchen Situation einen Balanceakt ausführen: Keinesfalls sollte sie ohne zwingenden Grund eine vom ISB vertretenen Maßnahme „kassieren".

Dies könnte unter Umständen die Konformität gegenüber der normativen Grundlage und - mindestens genauso ungünstig - die Rolle des ISB als „verlängerten Arm der Krankenhausleitung im Kontext der Informationssicherheit" nachhaltig beschädigen. Damit es nicht zu einer solchen Situation kommt, ist ein regelmäßiger Austausch, zum Beispiel im Rahmen eines Jour Fixe, zwischen der Krankenhausleitung und dem ISB ausdrücklich angeraten.

3.2.7 Bestellung eines internen Informationssicherheitsbeauftragten

Die Aufgaben und Zuständigkeiten sowie die Befugnisse und Kompetenzen eines ISB sollten dokumentiert werden. Hierfür empfiehlt es sich, eine schriftliche Bestellung vorzunehmen.

Als Vorlage kann hier das Dokument Vorlage ISB Bestellung Intern dienen, welches die Deutsche Krankenhausgesellschaft e.V. mit dem sog. Starter-Paket veröffentlicht hat.

3.2.8 Bestellung eines externen Informationssicherheitsbeauftragten

Insbesondere in kleineren Krankenhäusern kann es unter Umständen zweckmäßig sein, die Rolle des ISB nicht durch einen eigenen Mitarbeiter zu besetzen, sondern auf die Dienstleistungen eines externen ISB zurückzugreifen.
Hierzu muss zunächst ein geeigneter, qualifizierter Experte für Informationssicherheit ausgewählt werden (siehe Kap. 4.2.5 zu den notwendigen Qualifikationen)

Bevor ein externer ISB bestellt wird, ist zwischen dem Dienstleister und dem Krankenhaus ein Vertrag zu schließen, in dem die Aufgaben des externen ISB sowie die gegenseitigen Rechte und Pflichten möglichst präzise geregelt werden müssen.

Folgende Aspekte sollten in dem Vertrag mindestens geregelt werden:

- Anforderungen an die Qualifikation des externen IT-Sicherheitsbeauftragten
- Vertretungsregelungen und Mindest-Ressourcen
- Aufgaben des externen ISB
- Melde-, Berichts- und Eskalationswege, Ansprechpartner (Rollen)
- Einbindung in Kommunikationskanäle der beauftragenden Institution
- Arbeitsorte, Räumlichkeiten und Anwesenheits- bzw. Erreichbarkeitszeiten
- Zutritts-, Zugangs- und Zugriffsrechte
- Vortragsrechte und Berichtspflichten gegenüber der Leitungsebene der beauftragenden Institution
- Mitwirkungspflichten des Auftraggebers
- Vertraulichkeitsvereinbarung
- Hinweis, dass keine Interessenskonflikte bestehen dürfen
- Folgen bei Vertragsverstößen
- Regelungen zur Beendigung des Vertragsverhältnisses, z. B. Übergabe von Aufgaben und Unterlagen
- Kosten

Als Vorlage kann hier das Dokument Vorlage ISB Bestellung Extern dienen, welches die Deutsche Krankenhausgesellschaft e.V. mit dem sog. Starter-Paket veröffentlicht hat.

4 Zusammenfassung
Checkliste für die Krankenhausleitung

- **Ein Informationssicherheitsbeauftragter (ISB) muss bestellt werden.**
- **Der ISB muss unabhängig sein und es dürfen keine Interessenkonflikte bestehen.**
  → die Funktion sollte als Stabsstelle eingerichtet werden
- **Der ISB muss jederzeitiges Vorspracherecht bei der Krankenhausleitung haben.**
- **Der ISB muss über die erforderliche Kompetenz verfügen**
  (siehe Kap. 4.2.5).
- **Der ISB muss über ausreichende Kapazitäten und Ressourcen verfügen, um seine Aufgaben effektiv wahrzunehmen.**
- **Der ISB muss durch die Krankenhausleitung und die Führungskräfte unterstützt werden.**
- **Grundsätzlich kann ein interner oder ein externer ISB benannt werden.**
- **Der Umfang der Stelle des ISB richtet sich nach der Größe des Krankenhauses**
  (siehe hierzu Excel-Kalkulationsschema).

5 Anlage 1: Checklisten für den ISB

Die Aufgaben und Aktivitäten des ISB sollten geplant, dokumentiert und die Dokumentation gelenkt sein (siehe Kap. 7.5 ff. ISO/IEC 27001). Dies kann beispielsweise in Form von Checklisten für den ISB oder über eine/n Maßnahmenplan/-liste erfolgen.

Nachstehend finden Sie Checklisten für die strukturierte und nachvollziehbare Planung der täglichen Arbeit des ISB sowie für die regel-/turnusmäßigen, quartalsweisen und jährlichen Aktivitäten des ISB.

5.1 Tägliche Aktivitäten

Nachstehende Tätigkeiten gehören zum Tagesgeschäft eines ISB:

Themenfeld	Beschreibung	Check-box
CERT***-Meldungen	▪ Durchsicht von CERT-Meldungen (CERT-Bund, BSI, Heise) hinsichtlich Warnungen/technischen Schwachstellen ▪ Ableitung von Handlungsempfehlungen und Abstimmung mit den fachlichen Ansprechpartnern in der Krankenhaus-IT/Medizintechnik	☐
Bearbeitung Maßnahmenplan	▪ Bearbeitung von Maßnahmen aus dem Maßnahmenplan/Risikobehandlungsplan - Statusprüfung: sind geplante Maßnahmen überfällig? - Anpassung Status bzw. Ergänzung etwaiger neuer Maßnahmen - Abstimmung der Informationssicherheitsmaßnahmen mit dem Datenschutzbeauftragten	☐
Begehungen	▪ Begehungen und Kontrolle der Umsetzung von Informationssicherheitsmaßnahmen ▪ Ableitung und Dokumentation erforderlicher Maßnahmen im Maßnahmenplan/Risikobehandlungsplan	☐
Risikoanalyse	▪ Anlassbezogene Risikoanalysen/-bewertungen, z.B. bei Sicherheitsereignissen und -vorfällen	☐

	▪ Ableitung und Dokumentation erforderlicher Maßnahmen im Maßnahmenplan/Risikobehandlungsplan	
Schulungs- und Sensibilisierungsmaßnahmen	▪ Initiierung/Durchführung anlassbezogener Schulungs- und Sensibilisierungsmaßnahmen, z.B. bei Sicherheitsereignissen und -vorfällen	☐

*** CERT: Abkürzung für Computer Emergency Response Team. Ein Warn- und Informationsdienst bzgl. bekanntwerdender technischer Schwachstellen.

Sicherheitsereignisse und -vorfälle	▪ Reaktion auf Informationssicherheitsereignisse und -vorfälle: - Untersuchung - Durchführung und Dokumentation einer Risikobewertung - Meldungen, Ableitung und Dokumentation erforderlicher präventiver oder reaktiver Maßnahmen im Maßnahmenplan/Risikobehandlungsplan - Initiierung von Verbesserungen - Meldung an Aufsichten (BSI, Landesamt für Datenschutzaufsicht), sofern erforderlich	☐
Informationssicherheit in Projekten/Beschaffungsvorhaben	▪ Identifikation von Informationssicherheitsrisiken im Rahmen von Projekten oder Beschaffungsvorhaben, um notwendige technische und organisatorische Maßnahmen abzuleiten bzw. Vorgaben zur Informationssicherheit zu machen ▪ Gegebenenfalls Begleitung sicherheitsrelevanter Projekte	☐
Unterstützung	▪ Unterstützung von Führungskräften, z.B. bei der Konzeption von Prozessen und der Implementierung von Maßnahmen in den Fachbereichen und Abteilungen mit dem Fokus Informationssicherheit ▪ Unterstützung/Beratung der Administratoren und Mitarbeiter hinsichtlich Fragen zur Informationssicherheit	☐

5.2 Regel-/Turnusmäßige Aktivitäten

Themenfeld	Beschreibung	Check-box
Sitzung ISM-Team	▪ Planung/Durchführung regelmäßiger Sitzungen des ISM-Teams, u.a. - Festlegung der Sicherheitsziele und Strategien sowie Erstellung bzw. Aktualisierung der Leitlinie zur Informationssicherheit. - Überprüfung der Umsetzung der Sicherheitsleitlinie; Initiierung, Steuerung und Kontrolle des Informationssicherheitsprozesses - Mitwirkung bei der Entwicklung sicherheitsrelevanter Prozesse /Prozessvorgaben - Überprüfung, ob die im Informationssicherheitsprozess geplanten Sicherheitsmaßnahmen geeignet und wirksam sind und wie beabsichtigt funktionieren - Konzeption von Schulungs- und Sensibilisierungsprogrammen für Informationssicherheit - Beratung der Leitungsebene, der Fachverantwortlichen, der IT/Medizintechnik, Apotheke und des Labors	☐
Änderungen am ISMS	▪ Änderungen am ISMS (sofern vorhanden) - Geschäftsanforderungen - Sicherheitsanforderungen - Gesetzliche, regulative Vorgaben - Vertragliche Verpflichtungen - Risikoklassen - Wirksamkeitsabschätzung	☐

Review Risikoanalyse	▪ Turnusmäßiges Review der Risikoanalyse/-bewertung ▪ Ableitung und Dokumentation erforderlicher Maßnahmen im Maßnahmenplan/Risikobehandlungsplan	☐
Sicherheitsereignisse und -vorfälle	▪ Sicherheitsvorfälle seit letztem ISB-Review (erkannte Schwachstellen/Bedrohungen) - Prüfung ergriffene Maßnahmen: warum haben diese den Vorfall nicht verhindert? - Prüfung KPI* auf Wirksamkeit der ergriffenen Maßnahmen	☐

*KPI: Abkürzung für „Key Performance Indicators".

Schulung- und Sensibilisierungsmaßnahmen	▪ Planung, Initiierung und Durchführung von Schulungs- und Sensibilisierungsmaßnahmen, ▪ Überprüfung Schulungsstand	☐
Technische Sicherheitsanalysen/Penetrationstests	▪ Initiierung von technischen Sicherheitsanalysen und Penetrationstests - turnusmäßig, mindestens 1x im Jahr über die gesamte Infrastruktur (von extern und intern) - bei Major Updates von Applikationen - bei einem umfangreichen Umbau der Netzwerk-Infrastruktur - Um die Wirksamkeit von Patches zu testen bzw. zu bestätigen - im Falle des Bekanntwerdens von kritischen Schwachstellen, um eine erfolgte Kompromittierung auszuschließen (z.B. Shitrix-, Log4Shell-Schwachstelle)	☐
Bearbeitung Maßnahmenplan	▪ Stand der Maßnahmenumsetzung (insb. fristgemäße Umsetzung)	☐
Kontinuierliche Verbesserung	▪ Vorschläge zur Verbesserung des ISMS - von Mitarbeitern	

	- von Dienstleistern - selbst erkannte Verbesserungsmöglichkeiten (z.B. aufgrund von Erkenntnissen aus Sicherheitsvorfällen, aus Fortbildungen, Best Practice von Kollegen, etc.) - Ableitung von reaktiven und proaktiven Maßnahmen zur Verbesserung	☐
KPI	▪ Abschätzung der Wirksamkeit des ISMS/Kennzahlenüberwachung/ -aktualisierung - Auswertung bestehender KPI und Kennzahlen - Definition neuer/weiterer und besser an den Fortschritt auf Angreiferseite und der technologischen Entwicklung angepasster KPI	☐
Lieferantenmanagement	▪ Review des Lieferantenmanagements	☐
ISMS-Dokumentation/Dokumentenreview	▪ Review der ISMS-Dokumentation	☐
Management-Review	▪ Durchführung und Dokumentation eines Management-Reviews	☐
Jour-Fix Krankenhausleitung	▪ Information der Krankenhaus-Leitung (Jour Fixe) zum Stand der Informationssicherheit, der Bedrohungslage und zu treffenden Maßnahmen → Dokumentation der Beschlüsse der Klinikleitung zu den vereinbarten und auch zu den evtl. abgelehnten Maßnahmen	☐
Schnittstellen zum ISMS	▪ Unterstützung des Fachbereichs Qualitätsmanagement und – sofern vorhanden – des Risikomanagementverantwortlichen oder des Geschäftsfortführungsbeauftragten, um angemessene Schnittstellen zum ISMS sicherzustellen	☐

Geschäftsfortführung / Notfallmanagement (sofern kein Geschäftsfortführungsbeauftragter vorhanden ist)	▪ Unterstützung anderer Fachbereiche - bei der Konzeption, Prüfung und Pflege von Notfallplänen - durch Begleitung von Notfallübungen und -tests - bei der Aktualisierung der Geschäftsfortführungsanalyse	☐

5.3 Jährliche Aktivitäten

Themenfeld	Beschreibung	Check-box
Änderungen an ISMS/Leitlinie	▪ Prüfung, ob Änderungen an Leitlinie und ISMS notwendig geworden sind aufgrund von veränderten - Geschäftsanforderungen - Sicherheitsanforderungen - gesetzliche, regulative Vorgaben - vertragliche Verpflichtungen - Risikoklassen - Wirksamkeitsprüfungen	☐
Review Risikoanalyse	▪ Review der Risikoeinschätzung/Maßnahmendefinition	☐
Bearbeitung Maßnahmenplan	▪ Stand der Maßnahmenumsetzung (insb. fristgemäße Umsetzung)	☐
Status Schulungs- und Sensibilisierungsmaßnahmen	▪ Überprüfung Schulungsstand und etwaige Nachschulung fehlender Teilnehmer	☐
Interne und externe Audits	▪ Planung und Durchführung mind. eines internen Audits p.a. zum Informationssicherheitsmanagement ▪ Teilnahme an und Koordination von etwaigen externen Audits (z.B. im Rahmen der Jahresabschlussprüfung oder anderer Management-Systeme) ▪ Planung und Durchführung von Lieferantenaudits in Zusammenarbeit mit anderen Fachbereichen	☐
Geschäftsfortführung/ Notfallmanagement (sofern kein Geschäftsfortführungsbeauftragter vorhanden ist)	▪ Unterstützung bei der Aktualisierung und Pflege der Prozesse zur Geschäftsfortführung bzw. des Notfallmanagements ▪ Abstimmen des Notfallmanagements mit ext. Partnern	☐
KPI	▪ Abschätzung der Wirksamkeit des ISMS/Kennzahlenüberwachung/-aktualisierung	☐

Lieferantenmanagement	▪ Review des gesamten Lieferanten-managements	☐
ISMS-Dokumentation/Dokumen-tenreview	▪ Review der gesamten ISMS-Doku-mentation	☐
Management-Review	▪ Planung, Durchführung und Doku-mentation des jährlichen Gesamt-Management-Reviews	☐