Leitlinie zur Informationssicherheit der ViDia Christliche Kliniken Karlsruhe

Inhalt

Leitlinie zur Informationssicherheit

1. Ziel / Zweck

Die Unternehmensführung verabschiedet hiermit folgende Leitlinie zur Informationssicherheit als Bestandteil ihrer Strategie.

Die Informationssicherheitsleitlinie definiert das innerhalb des Geltungsbereiches angestrebte Sicherheitsniveau. Sie legt das vom Unternehmen angestrebten Sicherheitsniveau und die daraus abgeleiteten Sicherheitsziele fest. Ausgehend von der Informationssicherheitsleitlinie werden im Unternehmen entsprechende interne Organisationsstrukturen, Richtlinien, Regeln und Vorgaben dokumentiert, festgelegt und umgesetzt.

2. Geltungsbereich

Diese Leitlinie gilt für alle Mitarbeitenden, Dienstleister und Lieferanten, welche im und für den Anwendungsbereich des ISMS der ViDia Kliniken tätig sind.

3. Zuständigkeiten/Verantwortlichkeiten

Für den Inhalt und die Umsetzung der Leitlinie zur Informationssicherheit trägt der Vorstand die volle Verantwortung.

4. Informationssicherheitspolitik

Die Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung innerhalb des Unternehmens. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss vermieden oder kurzfristig kompensiert werden können. Die Patientenversorgung muss sichergestellt sein, selbst wenn die Informationssicherheit bzw. die Informationssicherheitsziele der ViDia Kliniken in Teilbereichen bedroht ist.

Um die Kernprozesse des Unternehmens vor Schäden zu bewahren, ist der Schutz der Informationen vor unberechtigtem Zugriff, vor unerlaubter Änderung und vor Zerstörung von existenzieller Bedeutung.

Unsere Kernaufgabe ist die Sicherstellung einer dauerhaft qualitativ hochwertigen und sicheren Gesundheitsversorgung. Diese Aufgabe erfordert einen sensiblen Umgang mit Informationen aus den Bereichen Patient, Mitarbeiter und Unternehmen. Es ist daher unser Ziel, Informationen als wichtige Werte in angemessener Weise hinsichtlich der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität zu schützen.

Für eine sichere und zuverlässige Versorgung werden wir durch angemessene Maßnahmen die Aufgaben und Prozesse sowie die hierfür benötigten Informationssysteme permanent weiterentwickeln.

Dieses Ziel wird nachhaltig über das Informationssicherheits-Managementsystem (ISMS) gemäß den Anforderungen des internationalen Standard ISO/IEC 27001:2022 und dem B3S Medizinische Versorgung unterstützt. Um die Effektivität des ISMS zu wahren, wird dieses kontinuierlich bewertet, überwacht und bei Bedarf verbessert. Hierdurch entwickeln wir uns von einem heute hohen individuellen sicherheitsbewussten Verhalten zu einer zukünftig umfassenden gemeinsamen Sicherheitsstrategie.

Informationssicherheit ist eine Angelegenheit aller Mitarbeiter und Bereiche. Der Vorstand trägt die Verantwortung für die Informationssicherheit und somit auch für das ISMS. Er verpflichtet sich, für den Aufbau und den Betrieb des ISMS genügend Ressourcen zur Verfügung zu stellen und den fortwährenden Betrieb des ISMS zu unterstützen.

Jeder Mitarbeiter im Anwendungsbereich ist verpflichtet, sich an die Regeln der Informationssicherheit zu halten und ist aufgefordert, durch Hinweise auf Verbesserungspotentiale der Informationssicherheit zu deren Weiterentwicklung beizutragen.

5. Informationssicherheitsziele

Vertraulichkeit:

Für die vom Unternehmen verarbeiteten Informationen und Daten ist eine angemessene Vertraulichkeit zu gewährleisten, so dass die vertraglichen, gesetzlich vorgeschriebenen und sonstigen Anforderungen eingehalten werden können. Nur berechtigte Personen dürfen auf vertrauliche Daten und Informationen zugreifen.

Integrität:

Fehlerhafte Daten und Informationen sind zu korrigieren bzw. deren Korrektur ist zu veranlassen. Fehlfunktionen und Unregelmäßigkeiten bezüglich Prozessen, Informationen, Daten, IT-Systemen und medizinischen Geräten sind auszuschließen und nur in Ausnahmefällen akzeptabel. Es sind angemessene Schutzmaßnahmen zu treffen, sodass deren Integrität sowie die Integrität der Prozesse, Daten und Informationen nicht kompromittiert werden können. Nur berechtigte Personen dürfen Daten und Informationen verändern.

Verfügbarkeit:

Die Prozesse, Informationen, datenverarbeitenden IT-Systeme und medizinischen Geräte der Informations-, Kommunikations-, Versorgungs- und Medizintechnik sind so zu sichern/schützen, dass deren Verfügbarkeit derart sichergestellt ist, dass im Falle von Unterbrechungen, Störungen oder sonstigen Beeinträchtigungen die daraus resultierenden Ausfallzeiten nicht bestandsgefährdend für das Unternehmen und die Patientenversorgung werden können.

Authentizität

Die Informationen, welche für die Patientenversorgung relevant sind, müssen vertraulich behandelt werden, integer und verfügbar sein. Es muss sichergestellt werden, dass der Ursprung der Information sicher nachgewiesen werden kann, unabhängig davon, ob es sich hierbei um eine Person oder ein System handelt.

Um die Einhaltung der Informationssicherheitsziele sicherzustellen, wurde ein Informationssicherheitsmanagementsystem (ISMS) etabliert. Seitens der Unternehmensführung wurde ein Informationssicherheitsbeauftragter (ISB) benannt. Der ISB berichtet in seiner Funktion direkt an die Unternehmensführung.

Alle Mitarbeiter sind angewiesen, den ISB in seiner Arbeit zu unterstützen und frühzeitig in alle Projekte einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte zu

berücksichtigen. Die Mitarbeiter des Unternehmens haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des ISB zu halten.

Neben der Einhaltung der vier Schutzziele dient das ISMS auch der Erreichung der folgenden, aktuell im Fokus stehenden Ziele des Vorstandes:

- Erfüllung der Anforderungen, welche sich nach BSI-Gesetz § 8a ergeben.
- Informationen und Systeme werden bezüglich ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Ausfallzeiten im klinischen Umfeld toleriert werden können. Ausfallzeiten, die zu größeren Arbeitsverzögerungen führen können, sollen durch entsprechende Maßnahmen vermieden werden.
- Die Anforderungen an Integrität und Vertraulichkeit orientieren sich an der Gesetzeskonformität. Die Anforderungen des Datenschutzes sind bei der Bearbeitung personenbezogener Daten uneingeschränkt zu erfüllen.
- Der Zugriff auf Informationen wird durch ein angemessenes Berechtigungskonzept, in Anlehnung an die Orientierungshilfe Krankenhausinformationssysteme, begrenzt. Neben dem Schutz der IT-Infrastruktur – Netze, Server, Computer, Software – sind auch Gebäude und Räumlichkeiten angemessen zu schützen.
- ISMS-Maßnahmen zur Sicherstellung der Patientenversorgung müssen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen stehen. Schadensfälle mit hohen finanziellen oder immateriellen Auswirkungen müssen verhindert werden.

6. Sicherheitsmaßnahmen

Damit die Informationssicherheit angemessen sichergestellt werden kann, sind für alle Verfahren, Prozesse, Informationen, IT-Anwendungen, IT-Systeme und sonstige für das Unternehmen wichtigen Werte verantwortliche Personen zu benennen, die den jeweiligen Schutzbedarf bestimmen und für den Zugang und Zugriff die entsprechenden Berechtigungen vergeben.

Für alle verantwortlichen Funktionen innerhalb des Unternehmens werden Vertretungen eingerichtet, soweit es die Personalsituation des Unternehmens ermöglicht. Durch Unterweisungen, Schulungen und ausreichende Dokumentationen wird sichergestellt, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der logische Zugang zu IT-Systemen, medizinischen Geräten oder sonstigen, für das Unternehmen wichtigen Werten ist durch angemessene Zugangskontrollen abgesichert und der Zugriff auf Daten und Informationen durch ein restriktives Berechtigungskonzept geschützt.

Die im Einsatz befindlichen IT-Systeme und die darauf gespeicherten und verarbeiteten Daten werden gegen Zerstörung, Manipulation und Spionage geschützt.

Die Übergänge vom unternehmenseigenen Datennetzwerk in das Internet sind durch geeignete Systeme (z. B. Firewalls, IDS, IPS) und Netzstrukturen (DMZ) abgesichert. Die Kommunikationsnetze innerhalb des Unternehmens sind so zu gestalten, dass eine ungewünsch-

te Beeinflussung ausgeschlossen bzw. minimiert wird. Getroffene Schutzmaßnahmen, egal ob technischer, physikalischer oder organisatorischer Natur sind einzuhalten und so zu betreiben, dass sie einen effektiven Schutz darstellen und Manipulationen verhindern.

Die Mitarbeiter des Unternehmens sind angehalten, sich sicherheitsbewusst zu verhalten und durch ihre Arbeitsweise die Informationssicherheitsbemühungen des Unternehmens zu unterstützen. Bei Auffälligkeiten sind die im Unternehmen für die Informationssicherheit zuständigen und festgelegten Stellen umgehend zu informieren. Dies gilt auch für Dienstleister und Lieferanten.

Trotz aller Bemühungen können Datenverluste oder Beeinträchtigungen in der Verfügbarkeit von Daten und Informationen nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher sichergestellt, dass der IT-Betrieb im Rahmen der identifizierten Verfügbarkeit wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.

Informationen 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. Dazu werden entsprechende Verfahren und Maßnahmen für den Notfall in einem separaten Notfallkonzept zusammengestellt.

Das Ziel des Unternehmens ist es, auch bei einem Systemausfall kritische Versorgungsprozesse aufrechterhalten zu können und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

Um die Informationssicherheitsanforderungen auch im Falle von ausgelagerten (IT-) Dienstleistungen einhalten zu können, werden in Verträgen mit externen Dienstleistern konkrete Sicherheitsanforderungen vorgegeben.

Mitarbeiter nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT, der Einhaltung und Umsetzung der Informationssicherheit und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Unternehmensführung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

7. Verbesserung der Informationssicherheit

Das ISMS wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Dies geschieht u. a. durch regelmäßige interne Kontrollen (interne Audits) und Management-Reviews sowie durch die regelmäßigen Prüfungen zur Erfüllung des §8a des BSIG.

Die Unternehmensführung unterstützt die ständige Verbesserung des Sicherheitsniveaus. Darüber hinaus sind Mitarbeiter angehalten, mögliche Verbesserungen oder Schwachstellen an die entsprechenden Stellen weiterzugeben.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Informationssicherheitsniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation risikoorientiert zu verbessern und ständig auf einem möglichst aktuellen Stand der Informationssicherheit zu halten. Etwaige Änderungen müssen von der Unternehmensführung genehmigt werden.

8. Verbindlichkeitserklärung der Unternehmensführung

Mittels dieser Erklärung verpflichtet sich die Unternehmensführung, das Informationssicherheitsmanagement nachhaltig und angemessen zu unterstützen und in Zusammenarbeit mit dem ISB des Unternehmens umzusetzen.

Der ISB und die Unternehmensführung sind jeweils verantwortlich für die Planung, Überwachung, den Betrieb und die Korrektur des ISMS.

Die vom ISB erstellten und von der Unternehmensführung freizugebenden Richtlinien, Prozesse und Konzepte sind für alle Mitarbeiter und Abteilungen im Geltungsbereich verbindlich.

Durch die Unterschrift der Unternehmensführung unter diese Informationssicherheitsleitlinie kommt die Unternehmensführung ihrer Verantwortung nach, das Thema Informationssicherheit angemessen und nachvollziehbar zu unterstützen.

Diese Informationssicherheitsleitlinie wurde vom Vorstand als Bestandteil seiner Strategie für das Unternehmen verabschiedet.

9. Inkrafttreten und Veröffentlichung

Durch die Freigabe dieser Informationssicherheitsleitlinie für alle Mitarbeitenden, Dienstleister und Lieferanten durch die Geschäftsführung der ViDia Christliche Kliniken Karlsruhe, ist diese ab sofort gültig und in allen enthaltenden Punkten ausnahmslos anzuwenden.

Karlsruhe, 26.06.2025

gez.

Richard Wentges (Vorsitzender)	Caroline Schubert