LL ISMS IT-Sicherheitsleitlinie

Inhaltsverzeichnis

Die Geschäftsführung verabschiedet folgende IT-Sicherheitsleitlinie als Bestandteil ihrer Strategie. Auf eine geschlechtsspezifische Unterscheidung wird aus Gründen der Lesbarkeit in diesem Dokument verzichtet.

1 Anwendungsbereich / Scope

Die Leitlinie gilt für das gesamte Ortenau Klinikum.

2 Stellenwert der Informationssicherheit

Die IT-Systeme am Ortenau Klinikum müssen in einem 24-Stunden-Betrieb das ganze Jahr über zuverlässig funktionieren, um eine effektive Arbeit zu gewährleisten. Die Leistungsfähigkeit und Behandlungsqualität des Ortenau Klinikum wird maßgeblich von der Verfügbarkeit der IT-Systeme und der Qualität der darin enthaltenen Daten beeinflusst. Die Verarbeitung von Informationen stellt eine Schlüsselrolle im Krankenhausbetrieb dar. Zahlreiche strategische und operative Prozesse werden durch informationstechnische Systeme unterstützt oder komplett ausgeführt. Ein unsachgemäßer Umgang mit den IT-Systemen, Verletzungen von Datenschutzbestimmungen, Missbrauch von IT-Systemen oder die Verseuchung der IT-Systeme durch Viren können schwerwiegende Konsequenzen für das Ortenau Klinikum haben. Daher ist es von existenzieller Bedeutung die Verfügbarkeit, Integrität und Vertraulichkeit der vorhandenen Systeme und Daten zu schützen. Ein Ausfall von IT-Systemen muss insgesamt kurzfristig kompensiert werden können.

Das Ortenau Klinikum verarbeitet personenbezogene Daten in einer über das übliche Maß hinausgehende Menge. Diese Daten dürfen unter keinen Umständen unbefugten Personen zugänglich gemacht werden.

3 Sicherheitsziele und Strategie zur Erreichung

Das Ortenau Klinikum legt folgende Sicherheitsziele fest:

- Die Verfügbarkeit, Integrität und Vertraulichkeit der IT-Systeme ist stets zum Schutz des Patienten sowie zum Schutz einer effektiven Behandlung zu gewährleisten.
- Dieser Schutz der sensiblen, personenbezogenen Daten hat eine hohe Priorität.
- Die Mindestanforderung an alle eingesetzten Systeme ist die Einhaltung von gesetzlichen, vertraglichen und aufsichtsrechtlichen Verpflichtungen.
- Die eingesetzten IT-Systeme werden so überwacht, dass ein Sicherheitsvorfall nachverfolgt werden kann.

Um diese Ziele zu erreichen orientiert sich das Ortenau Klinikum am branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S) in seiner aktuellen Fassung.

Die Strategie zum Betrieb von IT-Systemen und zum Zugriff auf Daten des Ortenau Klinikum richtet sich darauf aus, eine bestmögliche Verfügbarkeit zu gewährleisten.
Hierzu ist es notwendig jene Werte zu identifizieren, welche von elementarer Bedeutung für den Geschäftsbetrieb sind. Fehlfunktionen und Unregelmäßigkeiten, dieser als kritisch geltenden Werte, werden nur in geringem Umfang und nur in Ausnahmefällen toleriert.
Um die Vertraulichkeit zu schützen, halten wir uns an geltendes Recht und orientieren uns an vorhandenen Gesetzen.
Informationssicherheitsmaßnahmen sollten stets in einem wirtschaftlich vertretbaren Verhältnis zu der Kritikalität der schützenswerten Daten und Systemen stehen. Die Mitarbeiter der IT-Abteilung sind verpflichtet die festgelegten Regelungen anzuwenden und Verstöße zu vermeiden. Sie unterstützen die IT-Sicherheitsleitlinie und sind sich über die Wichtigkeit der IT bewusst.

Unsere Strategie zum sicheren Betrieb der IT-Systeme basiert auf folgenden Prinzipien:

- Hochkritische Systeme werden redundant und hoch verfügbar betrieben.
- Wir führen regelmäßige Datensicherungen nach einem definierten Datensicherungskonzept durch.
- Mit sicherheitsrelevanten Vorfällen gehen wir kontrolliert um.
- Für alle IT-Verfahren, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person inklusive Vertretung benannt.
- Durch ausreichende Unterweisung und Dokumentation wird gewährleistet, dass Vertreter ihre Aufgaben erfüllen können.
- IT-Räumlichkeiten werden ausreichend vor unbefugten Zutritten geschützt.
- Es existiert ein Virenschutzkonzept für alle IT-Systeme.
- Ein Zugriff von außen wird durch geeignete Systeme gesichert.
- Potenziell gefährliche Websites und Anhänge werden blockiert.
- Es existiert ein Notfallkonzept, um schnell auf Vorfälle reagieren zu können und Systeme nach einer tolerierbaren Zeit wiederherzustellen.
- Der Zugriff auf personenbezogene Daten erfolgt nur über persönliche und passwortgeschützte Zugänge.
- Zugriffe werden nach dem Minimalprinzip gewährt.
- Personenbezogene Daten, die das Unternehmen verlassen, werden über sichere Wege übermittelt.
- Die Einhaltung des Sicherheitskonzeptes wird regelmäßig kontrolliert und auditiert. Mitarbeiter werden regelmäßig sensibilisiert und geschult.
- Unsere Mitarbeiter kennen und befolgen die Dienstanweisung über die Nutzung der IT-Systeme im Ortenau Klinikum.

4 Organisation und Management

Zur Umsetzung der IT-Sicherheitsleitlinie ist ein Informationssicherheitsmanagementteam (ISMT) eingerichtet. Dieses Team besteht aus

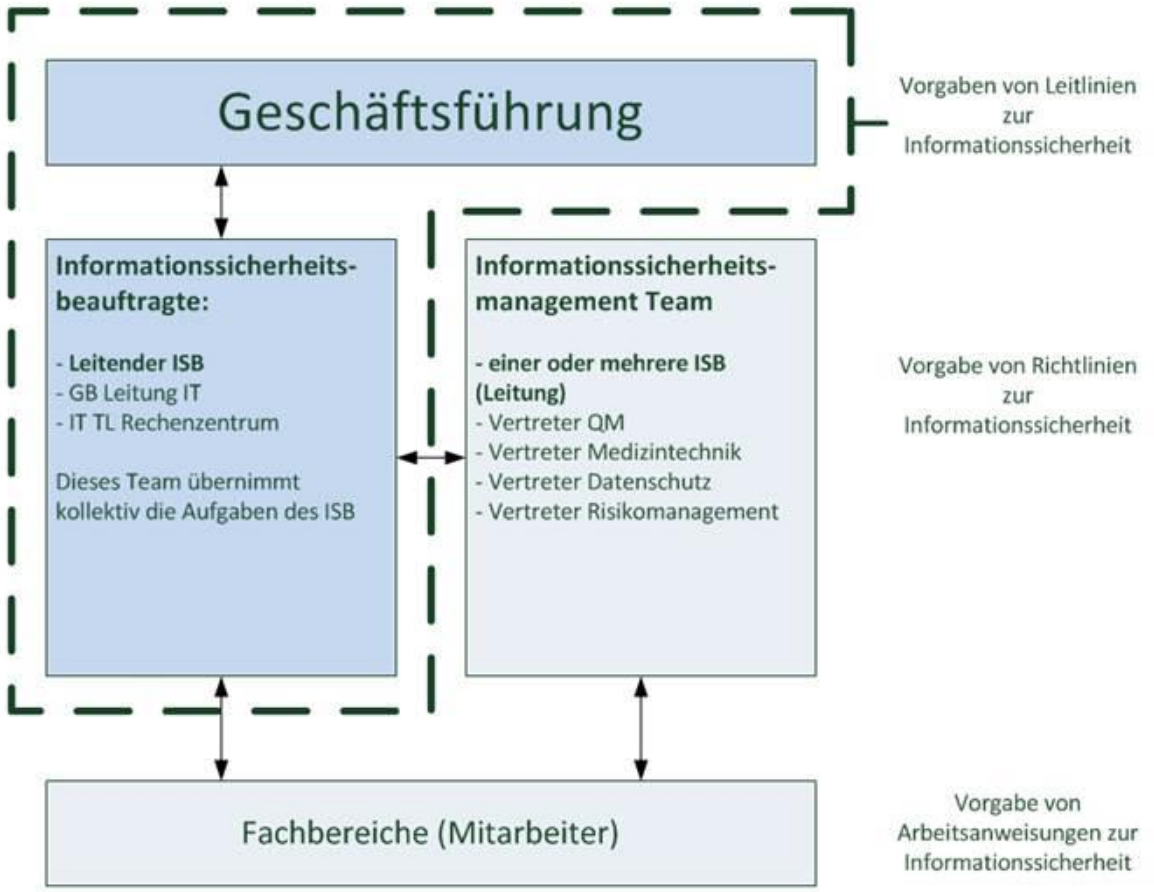
- einem oder mehreren Informationssicherheitsbeauftragten (ISB) als Leiter des ISMT
- einem Vertreter aus dem Bereich Medizintechnik
- einem Vertreter aus dem Bereich Qualitätsmanagement
- einem Vertreter aus dem Bereich Datenschutz
- einem Vertreter aus dem Bereich Risikomanagement

Zur Zielerreichung werden dem ISMT ausreichend finanzielle, zeitliche und personelle Ressourcen zur Verfügung gestellt. Dies beinhaltet auch die regelmäßige Weiterbildung.

Das Team der ISB besteht aus:

- Einem leitenden ISB
- dem Geschäftsbereichsleiter IT
- dem IT-Teamleiter Rechenzentrum

Diese Mitarbeiter nehmen kollektiv die Aufgaben eines Informationssicherheitsbeauftragten (ISB) wahr. Diese umfassen die Steuerung, Koordination, Weiterentwicklung und Kontrolle des Informationssicherheitsmanagementprozesses.
Ein ISB ist frühzeitig in alle relevanten Projekte und Prozesse einzubinden, um schon in der Planungsphase sicherheitsrelevante Aspekte berücksichtigen zu können. Dies gilt insbesondere bei der Einführung neuer Technologien. Sicherheitsrelevante Vorgaben eines ISB sind für alle Mitarbeiter verbindlich einzuhalten. Ein ISB berichtet direkt dem Geschäftsführer.



5 Kontinuierliche Verbesserung der IT-Sicherheit

Das Informationssicherheitsmanagementsystem (ISMS) wird regelmäßig auf Aktualität und Wirksamkeit geprüft. Zudem wird geprüft, ob die festgelegten Maßnahmen bei den Mitarbeitern bekannt sind und umgesetzt werden. Abweichungen werden als Chance erkannt, das Sicherheitsniveau zu verbessern und auf einem aktuellen technischen Stand zu halten. Damit wird das Sicherheits- und Datenschutzniveau stetig verbessert.

Diese kontinuierliche Verbesserung wird von der Geschäftsführung unterstützt und gelebt. Mitarbeiter sind dazu angehalten, mögliche Schwachstellen und Verbesserungen an einen ISB zu melden.

6 Erklärung der Geschäftsführung

Die Geschäftsführung identifiziert sich in vollem Umfang mit dieser IT-Sicherheitsleitlinie und den darin festgehaltenen Zielen. Sie sichert deren Durchsetzung zu.

Offenburg, 01.05.2019

gez. Christian Keller, Geschäftsführer