

# LL ISMS Informationssicherheitsleitlinie

## Inhaltsverzeichnis

<b>1</b>	<b>Anwendungsbereich / Scope.....</b>	<b>3</b>
<b>2</b>	<b>Stellenwert der Informationssicherheit .....</b>	<b>3</b>
<b>3</b>	<b>Sicherheitsziele und Strategie zur Erreichung.....</b>	<b>3</b>
<b>4</b>	<b>Organisation und Management .....</b>	<b>4</b>
<b>5</b>	<b>Kontinuierliche Verbesserung der Informationssicherheit .....</b>	<b>5</b>
<b>6</b>	<b>Erklärung des Vorstands .....</b>	<b>5</b>

## **LL ISMS Informationssicherheitsleitlinie**

---

Der Vorstand verabschiedet folgende Informationssicherheitsleitlinie 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 sowie für Dritte, die Zugriff auf informationstechnische Systeme des Ortenau Klinikum erhalten.

### **2 Stellenwert der Informationssicherheit**

Die informationstechnischen 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 Behandlungseffektivität des Ortenau Klinikum wird maßgeblich von der Verfügbarkeit der informationstechnischen 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 informationstechnischen Systemen, Verletzungen von Datenschutzbestimmungen, Missbrauch von Systemen oder die Verseuchung der Systeme durch Schadsoftware können schwerwiegende Konsequenzen für das Ortenau Klinikum haben. Daher ist es von existenzieller Bedeutung die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der vorhandenen Systeme und Daten zu schützen. Ein Ausfall von informationstechnischen Systemen muss durch Ausfallkonzepte und Ersatzverfahren bestmöglich 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. Die Mitarbeiter sind daher verpflichtet die festgelegten Regelungen anzuwenden und Verstöße zu vermeiden. Sie unterstützen diese Leitlinie und sind sich über die Wichtigkeit der Informationssicherheit bewusst.

### **3 Sicherheitsziele und Strategie zur Erreichung**

Das Ortenau Klinikum legt folgende Sicherheitsziele fest:

- Die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen 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 Systeme werden so überwacht, dass ein Sicherheitsvorfall erkannt, bewältigt und nachverfolgt werden kann.
- Prozesse die maßgeblich zur medizinischen Leistungserbringung beitragen, verfügen über geeignete Ausfallkonzepte und Ersatzverfahren, um einen Ausfall von informationstechnischen Systemen bestmöglich kompensieren zu können.

Um diese Ziele zu erreichen betreibt das Ortenau Klinikum ein Informationssicherheitsmanagementsystem welches sich an dem branchenspezifischen Sicherheitsstandard für die Gesundheitsversorgung im Krankenhaus (B3S) in seiner aktuellen Fassung orientiert. Die Umsetzung des B3S dient ebenso der Erbringung des Nachweises nach §8a BSIG sowie der Erfüllung der Vorgaben aus § 391 SGB V.

## LL ISMS Informationssicherheitsleitlinie

Die Strategie zum Betrieb von informationstechnischen Systemen und zum Zugriff auf Daten des Ortenau Klinikum richtet sich darauf aus, eine bestmögliche Verfügbarkeit der Geschäftsprozesse zu gewährleisten.

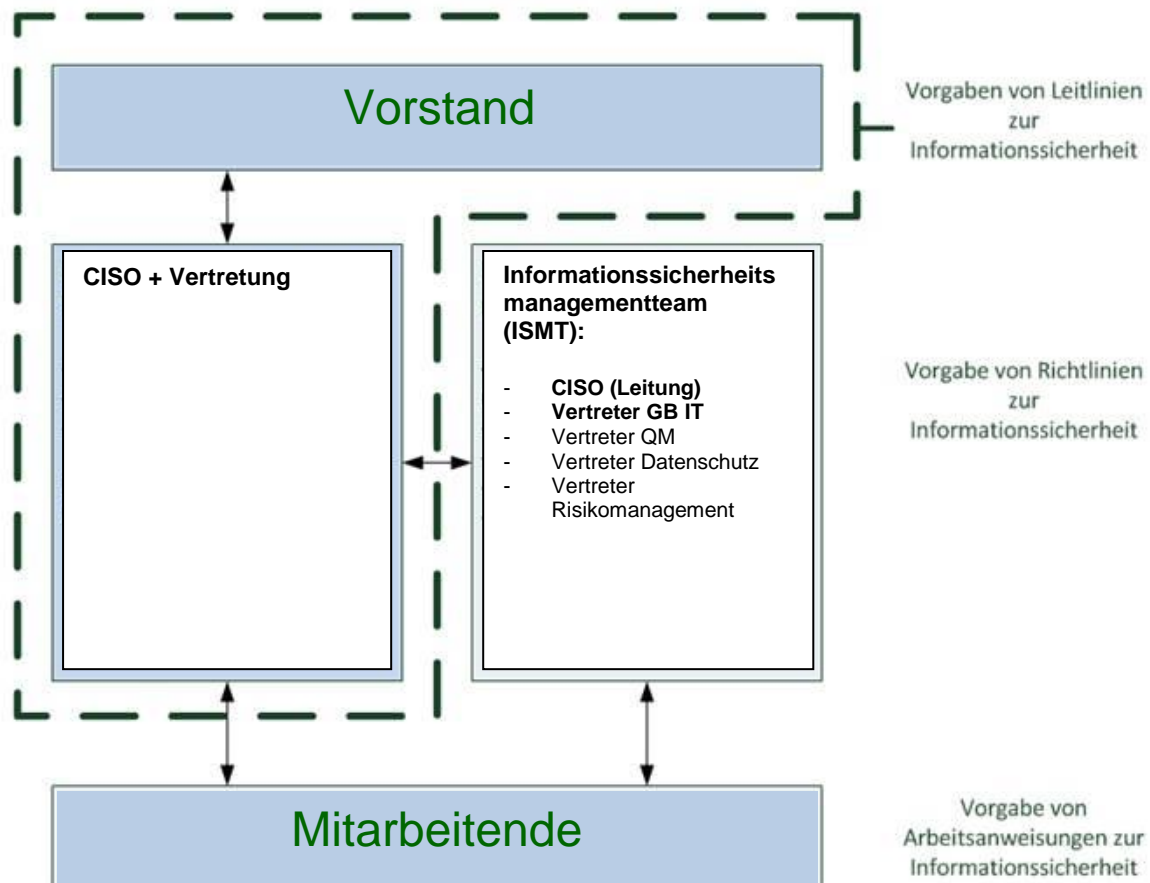
Hierzu ist es notwendig jene Werte zu identifizieren, welche von elementarer Bedeutung für den Geschäftsbetrieb sind. Fehlfunktionen und Unregelmäßigkeiten, dieser als kritisch geltenden Werte, werden nur in geringem Umfang und nur in Ausnahmefällen toleriert. Mit identifizierten Risiken wird kontrolliert umgegangen. 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.

### 4 Organisation und Management

Zur Erreichung der genannten Sicherheitsziele und der Steuerung der damit verbundenen Prozesse und Aufgaben, existiert am Ortenau Klinikum die Rolle des Informationssicherheitsbeauftragten auch Chief Information Security Officer (CISO) genannt und einer benannten Vertretung.

Der CISO besitzt eine unabhängige und organisatorisch herausgehobene Stellung. Diese Rolle wird als Stabstelle innerhalb des Geschäftsbereich IT geführt. Es besteht jedoch ein direktes Vortragsrecht gegenüber dem Vorstand.

Ein CISO 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 CISO sind für alle Mitarbeiter verbindlich einzuhalten. Ein CISO berichtet direkt dem Vorstand. Der Vorstand trägt die Gesamtverantwortung für alle Belange der Informationssicherheit.



## **LL ISMS Informationssicherheitsleitlinie**

---

Zur Unterstützung der Umsetzung dieser Informationssicherheitsleitlinie ist ein Informationssicherheitsmanagementteam (ISMT) eingerichtet. Dieses Team besteht mindestens aus:

- dem Informationssicherheitsbeauftragten (CISO) als Leiter des ISMT
- mehreren Vertretern aus dem Geschäftsbereich IT

Bei Bedarf wird das Team von folgenden Stellen ergänzt:

- 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.

## **5 Kontinuierliche Verbesserung der Informationssicherheit**

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. Dies erfolgt beispielsweise durch Audits. 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 dem Vorstand unterstützt und gelebt. Mitarbeiter sind dazu angehalten, mögliche Schwachstellen und Verbesserungen an den CISO zu melden.

## **6 Erklärung des Vorstands**

Der Vorstand identifiziert sich in vollem Umfang mit dieser Informationssicherheitsleitlinie und den darin festgehaltenen Zielen. Er sichert deren Durchsetzung zu.

Offenburg, 18. Dezember 2024  
gez.

Christian, Keller,  
Vorstandsvorsitzender

Kathleen, Messer  
Pflegerische Vorständin

Dr. Peter, Kraemer  
Medizinischer Vorstand