Informationssicherheitsleitlinie   
für das Klinikum  
[NAME]

[DATUM]

# Zweck

Die Leitung des Klinikums [NAME] äußert mit dieser Leitlinie den hohen Stellenwert der Aufrechterhaltung der Informationssicherheit im Betrieb und darin anfallender und verarbeiteter Daten. Dieses Dokument definiert eine aufgegliederte Zielsetzung im Kontext der Informationssicherheit und legt den Geltungsbereich, eine allgemeine Sicherheitsstrategie mit kontinuierlicher Verbesserungsabsicht sowie den grundlegenden organisatorischen Rahmen fest. Dieses Dokument spiegelt daher die Überzeugungen der Geschäftsführung des Klinikums wider.

# Zielsetzung

[Warum Informationssicherheit im Krankenhaus?

* Gesellschaftlicher Auftrag eines Krankenhauses im Gesundheitssystem
* Kritikalität der Informationen, die in Krankenhäusern generiert und verarbeitet werden
* Stellenwert der IT im Krankenhaus]

[Betonung des Stellenwerts der Informationssicherheit, der Bedeutung von Informationen und Geschäftsprozessen]

Ziele, die im Rahmen einer Gewährleistung von Informationssicherheit im Krankenhaus/Klinikum [NAME] verfolgt werden, sind im Einzelnen:

* Der Schutz der Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität von Informationen und Diensten
* Der Schutz von Patienten und Personal
* Gewährleistung der Einhaltung gesetzlicher Anforderungen
* Gewährleistung einer effektiven Patientenversorgung
* [Weitere Individualanforderungen]

# Geltungsbereich

Die in diesem Dokument festgehaltene Leitlinie der Informationssicherheit gilt für die Betriebsstätten [LISTE BETRIEBSSTÄTTEN] und im besonderen Fokus des medizinischen Betriebs für die Kernprozesse [LISTE KERNPROZESSE, vgl. B3S im Krankenhaus, Kap. 5.2.1 ff]. Jeder (interne als auch externe Dienstleister), der Informationen oder Infrastruktur des Krankenhauses [HAUS] nutzt, unterliegt dieser Informationssicherheitsrichtlinie und ist zu entsprechendem Handeln verpflichtet.

Bewusst und begründet ausgeschlossen aus dem Geltungsbereich sind…

[LISTE AUSGESCHLOSSENER BETRIEBSSTÄTTEN mit jeweiliger kurzer Begründung]

[LISTE AUSGESCHLOSSENER KERNPROZESSE mit jeweiliger Begründung. Eine Liste der wichtigsten Kernprozesse im Krankenhaus findet sich im Branchenspezifischen Standard B3S der DKG]

# Sicherheitsstrategie

* [KURZE/GROBE BESCHREIBUNG GESAMTKONZEPT Hinweis: Die Sicherheitsstrategie kann sinnvoll anhand des Vorgehensmodells der „Orientierungshilfe IT-Sicherheit in Kliniken“ des bayerischen Landesamts für Sicherheit (LSI) in der Informationstechnik festgelegt werden. Dieses Dokument kann vom LSI per E-Mail an [beratung-kritis@lsi.bayern.de](mailto:beratung-kritis@lsi.bayern.de) angefordert werden.
* Hinweis: Verwenden Sie auch unser Reifegradmodell mit Reifegradstufen 1-3 und Zielen zur zeitlichen Erreichung der jeweiligen Reifegradstufe
* **Hinweis: Diese Leitlinie ist allgemein öffentlich einsehbar. Beschreiben Sie hier keine Details zur Ihrer Sicherheitsstrategie, die Externe oder potenzielle Angreifer auf Schwachstellen hinweisen könnten. Eine detaillierte Sicherheitsstrategie müssen Sie in einem internen Dokument beschreiben!]**

# Rollen, Verantwortlichkeiten und Pflichten

**Die Gesamtverantwortung für die Einhaltung und Erfüllung der Sicherheitsstrategie hat die Geschäftsführung**. Des Weiteren sieht das Informationssicherheitsmanagement des Krankenhauses [NAME] weitere im Folgenden aufgelistete Rollen mit entsprechenden Verantwortlichkeiten vor.

|  |  |
| --- | --- |
| Informationssicherheitsbeauftragter (ISB) | Der Informationssicherheitsbeauftragte ist verantwortlich für die organisatorische Umsetzung des Prozesses des Informationssicherheitsmanagements. Er ist diesbezüglich unmittelbar der Geschäftsführung unterstellt. [WEITERE AUFGABEN] |
| Datenschutzbeauftragter (DSB) | Der Datenschutzbeauftragte ist für die Umsetzung und Kontrolle der Einhaltung rechtlicher Bestimmungen zum Datenschutz innerhalb des Krankenhauses verantwortlich. Darüber hinaus ist er für die Organisation und Bewusstseinsmaßnahmen des Datenschutzes im Krankenhaus zuständig. Um seine Aufgaben effektiv ausführen zu können, ist der DSB direkt der Geschäftsführung unterstellt. [WEITERE AUFGABEN] |
| IT-Sicherheitsmanager | Die Aufgaben eines IT-Sicherheitsmanagers dienen in erster Linie der Umsetzung von Informationssicherheit im Krankenhaus. Dazu gehören unter anderem:   * Die Erarbeitung geeigneter Vorgaben und Richtlinien der Nutzung von IT-Systemen * Die Erarbeitung von Vorgaben für sichere Soft- und Hardware * Die Erarbeitung von Lösungen zum Einsatz von Soft- und Hardware zur Absicherung von Systemen und Informationen * Beratung von Anwendern bezüglich Informationssicherheit * [WEITERE] |
| [WEITERE] |  |
|  |  |
|  |  |

# Basiskriterien der Wirksamkeit

Das ISMS wird grundsätzlich auf Basis folgender Kriterien bewertet:

* Die Bekanntheit dieses Dokuments und der Wille zur Verbesserung der Informationssicherheit unter den Mitarbeitern
* Konformität des ISMS zu gesetzlichen Bestimmungen
* Umsetzungsgrad des ISMS
* [WEITERE]

# Meldewege bei Vorfällen

Alle Personen (krankenhausintern als auch extern), die im Geltungsbereich des Dokuments nicht ausdrücklich und begründet ausgeschlossen sind, haben die Pflicht, sicherheitsrelevante Ereignisse, Beobachtungen und erkannte Sicherheitsvorfälle über [MELDEWEG, ROLLE oder MEDIUM] unverzüglich zu melden.

Ein Sicherheitsvorfall ist gegeben, sobald eines der im Abschnitt **Zielsetzung** aufgeführten Ziele erkennbar verletzt wurde. Ein sicherheitsrelevantes Ereignis ist gegeben, sobald eines der aufgeführten Ziele gefährdet erscheint.

# Inkrafttreten, Zusicherung und Durchsetzung

Die vorliegende Informationssicherheitsrichtlinie tritt unmittelbar auf Beschluss der Geschäftsführung in Kraft.

Die Geschäftsführung des Klinikums [NAME] bekennt sich zu den in dieser Richtlinie festgelegten Zielen, dem Geltungsbereich und der beschriebenen Sicherheitsstrategie. Verstöße und Zuwiderhandlungen gegen Überzeugungen und Vorgaben der Informationssicherheitsrichtlinie werden gemäß einem formellen Maßregelprozess behandelt.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  
[NAME GESCHÄFTSFÜHRER]