1. Vorbemerkung

Ziel und Zweck des Dokuments

In der Leitlinie zur Informationssicherheit werden die grundlegenden Ziele, Anforderungen und die Strategie der Informationssicherheit der Kreiskrankenhaus Greiz-Ronneburg GmbH sowie deren Organisationsstruktur festgelegt. Die Leitlinie zur Informationssicherheit:

- beschreibt den Stellenwert der Informationssicherheit
- formuliert die allgemeinen Sicherheitsziele
- legt die Informationssicherheitsstrategie fest
- legt die Verantwortung der Informationssicherheit fest
- definiert die Sicherheitsorganisation
- verpflichtet zur Weiterentwicklung der Informationssicherheit

Geltungsbereich

Der Geltungsbereich dieser Leitlinie zur Informationssicherheit erstreckt sich über alle Einheiten und Prozesse der Kreiskrankenhaus Greiz-Ronneburg GmbH, die mit der Erfassung, Verarbeitung, Speicherung und Übertragung von Informationen befasst sind. Dies beinhaltet sowohl interne als auch externe Komponenten und Akteure. Die interne Richtlinie zum Geltungsbereich konkretisiert diesen Sachverhalt.

Zielgruppe

Die Zielgruppe dieser Leitlinie zur Informationssicherheit umfasst alle Personen und Gruppen, die in irgendeiner Weise mit den Informationssystemen und -daten des Krankenhauses in Berührung kommen. Eine klare Definition der Zielgruppe ist essenziell, um sicherzustellen, dass alle relevanten Akteure die Leitlinie kennen, verstehen und anwenden. Im Einzelnen umfasst die Zielgruppe folgende Gruppen:

Feste und temporäre Mitarbeiter: Dies schließt alle fest angestellten und temporären Mitarbeiter des Krankenhauses ein, unabhängig von ihrer Position oder Funktion. Dazu gehören Ärzte, Pflegepersonal, Verwaltungskräfte, IT-Mitarbeiter, Reinigungspersonal sowie Aushilfskräfte und saisonale Mitarbeiter. Jeder Mitarbeiter trägt zur Sicherheit der Informationen bei und muss daher die Leitlinie vollständig verstehen und befolgen.

Führungskräfte und Management: Führungskräfte und das Management des Krankenhauses sind dafür verantwortlich, die Leitlinie zur Informationssicherheit in ihren jeweiligen Abteilungen umzusetzen und zu überwachen. Sie müssen sicherstellen, dass alle Mitarbeiter die Leitlinie kennen und gemäß den festgelegten Richtlinien handeln. Darüber hinaus sind sie dafür verantwortlich, sicherheitsrelevante Entscheidungen zu treffen und Ressourcen für die Informationssicherheit bereitzustellen.

Externe Dienstleister und Partner: Alle externen Dienstleister und Partner, die im Auftrag des Krankenhauses tätig sind oder Zugang zu den Informationssystemen und -daten des Krankenhauses haben, müssen die Richtlinien zur Informationssicherheit befolgen. Dazu

gehören IT-Dienstleister, Wartungsfirmen, Beratungsunternehmen, Lieferanten und andere externe Partner. Verträge mit externen Dienstleistern müssen klare Sicherheitsanforderungen und Vertraulichkeitsvereinbarungen enthalten.

Praktikanten, Auszubildende und Freiwillige: Praktikanten, Auszubildende und freiwillige Helfer, die im Krankenhaus tätig sind, müssen ebenfalls in die Leitlinie zur Informationssicherheit einbezogen werden. Sie müssen eine angemessene Einführung und Schulung erhalten, um die Bedeutung der Informationssicherheit zu verstehen und die Richtlinien korrekt anzuwenden.

Patienten und Besucher: Obwohl Patienten und Besucher nicht direkt zur Zielgruppe der Leitlinie gehören, ist es wichtig, dass sie über Grundprinzipien der Informationssicherheit informiert werden, insbesondere wenn sie Zugang zu bestimmten Bereichen oder Systemen des Krankenhauses haben. Informationsmaterialien und Hinweise sollen sicherstellen, dass Patienten und Besucher die Sicherheitsmaßnahmen respektieren.

2. Stellenwert der Informationssicherheit

Informationssicherheit hat im Krankenhaus einen herausragenden Stellenwert, da sie die Grundlage für den Schutz sensibler Informationen und die Aufrechterhaltung eines sicheren und effizienten Krankenhausbetriebs bildet. Die Informationssicherheit dient nicht nur dem Schutz von Patientendaten, sondern auch der Sicherstellung der Verfügbarkeit und Integrität der gesamten IT-Infrastruktur. Schutzziele und weitere Aspekte wie Patientensicherheit und Behandlungseffektivität sind von zentraler Bedeutung.

3. Schutzziele:

Verfügbarkeit: Die kontinuierliche Verfügbarkeit von IT-Systemen und Daten ist essenziell für den reibungslosen Krankenhausbetrieb. Ausfälle oder Unterbrechungen können schwerwiegende Auswirkungen auf die Patientenversorgung und die betrieblichen Abläufe haben. Maßnahmen zur Sicherstellung der Verfügbarkeit umfassen redundante Systeme, regelmäßige Datensicherungen und Notfallpläne.

Integrität: Die Integrität der Daten muss gewährleistet sein, um sicherzustellen, dass Informationen vollständig, korrekt und unverändert sind. Datenintegrität ist entscheidend für die Diagnose, Behandlung und Verwaltung von Patienten. Maßnahmen zur Gewährleistung der Integrität umfassen Zugangskontrollen, Verschlüsselung und regelmäßige Überprüfungen.

Vertraulichkeit: Der Schutz der Vertraulichkeit sensibler Informationen ist besonders wichtig, um die Privatsphäre der Patienten zu wahren und gesetzliche Vorgaben wie die Datenschutz-Grundverordnung (DSGVO) zu erfüllen. Maßnahmen zur Sicherstellung der Vertraulichkeit beinhalten Zugriffskontrollen, Schulungen und Sensibilisierungsmaßnahmen für das Personal sowie Verschlüsselungstechnologien.

Patientensicherheit: Die Informationssicherheit trägt direkt zur Patientensicherheit bei. Sichere IT-Systeme verhindern unbefugten Zugriff und Manipulationen, die zu falschen Diagnosen oder Behandlungen führen könnten. Ein hohes Maß an Informationssicherheit stellt sicher, dass die richtigen Informationen zur richtigen Zeit am richtigen Ort verfügbar sind.

Behandlungseffektivität: Effektive Behandlung erfordert genaue und aktuelle Informationen. Durch den Schutz der Informationssicherheit wird sichergestellt, dass medizinische Fachkräfte auf zuverlässige Daten zugreifen können, um fundierte Entscheidungen zu treffen. Dies verbessert die Qualität der Patientenversorgung und minimiert das Risiko von Fehlern.

Weitere Aspekte der Informationssicherheit:

Wirtschaftlichkeit: Informationssicherheit trägt zur Wirtschaftlichkeit des Krankenhauses bei, indem sie finanzielle Verluste durch Datenverluste, Systemausfälle oder Cyberangriffe verhindert. Investitionen in Informationssicherheitstechnologien und -prozesse sind langfristig kosteneffektiv und schützen das Krankenhaus vor finanziellen Schäden und Reputationsverlusten.

Compliance und rechtliche Anforderungen: Krankenhäuser unterliegen strengen rechtlichen und regulatorischen Anforderungen hinsichtlich des Schutzes von Patientendaten. Die Einhaltung dieser Vorschriften ist nicht nur gesetzlich vorgeschrieben, sondern auch notwendig, um das Vertrauen der Patienten und der Öffentlichkeit zu erhalten. Informationssicherheit gewährleistet die Einhaltung von Vorschriften wie der DSGVO, dem Bundesdatenschutzgesetz (BDSG) und spezifischen Gesundheitsrichtlinien.

Vertrauen und Reputation: Ein hohes Maß an Informationssicherheit stärkt das Vertrauen der Patienten, Mitarbeiter und Partner in das Krankenhaus. Es zeigt, dass das Krankenhaus verantwortungsvoll mit sensiblen Informationen umgeht und sich aktiv um deren Schutz bemüht. Dies trägt zur positiven Wahrnehmung und Reputation des Krankenhauses bei.

4. Festlegung von weiteren Sicherheitszielen

Neben den grundlegenden Schutzzielen Verfügbarkeit, Integrität und Vertraulichkeit, die bereits im Kontext der Schutzziele definiert wurden, legt die Kreiskrankenhaus Greiz-Ronneburg GmbH weitere spezifische Sicherheitsziele fest, um die Informationssicherheit auf höchstem Niveau zu gewährleisten und kontinuierlich zu verbessern. Diese zusätzlichen Sicherheitsziele sind darauf ausgerichtet, den sich ständig ändernden Bedrohungslandschaften und technologischen Entwicklungen gerecht zu werden. Im Folgenden werden die wesentlichen Sicherheitsziele beschrieben:

Kontinuierliche Risikobewertung und -management:

Ein zentrales Sicherheitsziel ist die kontinuierliche Bewertung und das Management von Risiken. Dies umfasst die regelmäßige Durchführung von Risikoanalysen, um potenzielle Bedrohungen und Schwachstellen frühzeitig zu erkennen und geeignete Maßnahmen zur

Risikominderung zu entwickeln. Das Ziel ist es, ein dynamisches und proaktives Risikomanagementsystem zu etablieren, das flexibel auf neue Herausforderungen reagiert.

Schulung und Sensibilisierung der Mitarbeiter:

Die Schulung und Sensibilisierung aller Mitarbeiter hinsichtlich Informationssicherheit ist ein weiteres zentrales Ziel. Regelmäßige Schulungen sollen das Bewusstsein für Sicherheitsrisiken schärfen und das Verhalten der Mitarbeiter im Umgang mit Informationen positiv beeinflussen. Das Ziel ist es, eine Sicherheitskultur zu etablieren, in der jeder Mitarbeiter seine Verantwortung für den Schutz von Informationen versteht und wahrnimmt.

Implementierung und Aktualisierung von Sicherheitsrichtlinien:

Die kontinuierliche Überprüfung und Aktualisierung von Sicherheitsrichtlinien und -prozeduren ist entscheidend, um den aktuellen Bedrohungen und technologischen Entwicklungen gerecht zu werden. Das Ziel ist, ein umfassendes Regelwerk zu schaffen, das klare Anweisungen und Verhaltensregeln für den sicheren Umgang mit Informationen und IT-Systemen definiert.

Technologische Erneuerung und Innovation:

Ein weiteres Sicherheitsziel ist die fortlaufende technologische Erneuerung und Innovation. Dies beinhaltet die Implementierung neuer Sicherheitstechnologien und -lösungen, um den Schutz der Informationssysteme und Daten zu verbessern. Beispiele hierfür sind fortschrittliche Verschlüsselungstechnologien, moderne Authentifizierungsmechanismen und innovative Ansätze zur Bedrohungserkennung und -abwehr.

Stärkung der physischen Sicherheitsmaßnahmen:

Die Stärkung der physischen Sicherheitsmaßnahmen ist ebenfalls ein wichtiges Ziel. Dies umfasst den Schutz von IT-Infrastrukturen und sensiblen Bereichen des Krankenhauses vor physischen Bedrohungen wie Einbruch, Diebstahl, Vandalismus oder Naturkatastrophen. Maßnahmen wie Zugangskontrollen, Videoüberwachung und Notfallpläne tragen dazu bei, die physische Sicherheit zu gewährleisten.

Erweiterung der Notfall- und Wiederherstellungsplanung:

Die Erweiterung und regelmäßige Aktualisierung der Notfall- und Wiederherstellungspläne ist ein wesentliches Sicherheitsziel. Dies beinhaltet die Entwicklung und Umsetzung von Strategien zur schnellen Wiederherstellung des Betriebs im Falle eines Sicherheitsvorfalls oder einer Katastrophe. Das Ziel ist es, die Betriebsunterbrechungen zu minimieren und die Kontinuität der Patientenversorgung sicherzustellen.

Erhöhung der Transparenz und Berichterstattung:

Die Erhöhung der Transparenz und die regelmäßige Berichterstattung über Sicherheitsvorfälle und -maßnahmen sind weitere Sicherheitsziele. Dies umfasst die Etablierung eines Systems zur Meldung und Dokumentation von Sicherheitsvorfällen sowie die Erstellung regelmäßiger Berichte für das Management und relevante Aufsichtsbehörden. Ziel ist es, eine transparente und nachvollziehbare Sicherheitskultur zu fördern.

Kooperation und Austausch mit externen Partnern:

Die Kooperation und der Austausch von Informationen und Best Practices mit externen Partnern und Fachgemeinschaften sind ebenfalls wichtige Sicherheitsziele. Durch die Zusammenarbeit mit anderen Gesundheitseinrichtungen, Sicherheitsbehörden und Fachverbänden können Synergien genutzt und das Sicherheitsniveau weiter erhöht werden.

5. Verantwortung der Informationssicherheit

Gesamtverantwortung der Konzerngeschäftsführung

Die Verantwortung der Informationssicherheit im Krankenhaus ist klar strukturiert und verteilt, um sicherzustellen, dass alle Beteiligten ihre Rolle und Verantwortung verstehen und erfüllen. Die Gesamtverantwortung liegt bei der Konzerngeschäftsführung, die die strategischen Rahmenbedingungen setzt und die notwendigen Ressourcen bereitstellt. Es ist ihre Pflicht, eine Kultur der Informationssicherheit zu fördern und sicherzustellen, dass die Informationssicherheitsziele in die Gesamtstrategie des Krankenhauses integriert sind. Die Geschäftsführung ist auch verantwortlich für die Genehmigung und regelmäßige Überprüfung der Informationssicherheitsleitlinie sowie für die Entscheidung über wesentliche Sicherheitsmaßnahmen und -investitionen.

Mitverantwortung aller Beschäftigten und Führungskräfte

Neben der Gesamtverantwortung der Geschäftsführung tragen alle Beschäftigten und Führungskräfte der Kreiskrankenhaus Greiz-Ronneburg GmbH eine Mitverantwortung für die Informationssicherheit. Jeder Mitarbeiter, unabhängig von seiner Position oder Funktion, spielt eine entscheidende Rolle im Schutz sensibler Informationen und der IT-Infrastruktur. Führungskräfte sind insbesondere dafür verantwortlich, die Informationssicherheitsrichtlinien in ihren jeweiligen Abteilungen zu kommunizieren und durchzusetzen. Sie müssen sicherstellen, dass ihre Mitarbeiter regelmäßig geschult und sensibilisiert werden, um mögliche Sicherheitsrisiken zu erkennen und entsprechend zu handeln. Führungskräfte haben auch die Pflicht, sicherheitsrelevante Vorfälle zu melden und aktiv an der kontinuierlichen Verbesserung der Sicherheitsmaßnahmen mitzuwirken.

6. Informationssicherheitsstrategie

Die Informationssicherheitsstrategie der Kreiskrankenhaus Greiz-Ronneburg GmbH ist darauf ausgerichtet, die Vertraulichkeit, Integrität und Verfügbarkeit aller informationsverarbeitenden Systeme und Daten zu gewährleisten. Diese Strategie umfasst eine Reihe von Maßnahmen und Prozessen, die kontinuierlich überprüft und angepasst werden, um den sich ständig ändernden Bedrohungslandschaften und technologischen Entwicklungen gerecht zu werden. Die Informationssicherheitsstrategie ist ein integraler Bestandteil der Gesamtstrategie der Kreiskrankenhaus Greiz-Ronneburg GmbH und wird von der Geschäftsführung aktiv unterstützt und gefördert.

Die strategischen Ziele der Informationssicherheit umfassen den Schutz sensibler Patientendaten, die Sicherstellung des reibungslosen Krankenhausbetriebs und die Einhaltung gesetzlicher und regulatorischer Anforderungen. Diese Ziele werden durch die

Implementierung eines umfassenden Informationssicherheits-Managementsystems (ISMS) erreicht, das auf bewährten Standards und Best Practices basiert.

Durch die konsequente Umsetzung dieser Informationssicherheitsstrategie stellt die Kreiskrankenhaus Greiz-Ronneburg GmbH sicher, dass alle Anforderungen an den Schutz sensibler Informationen und die Aufrechterhaltung eines sicheren Krankenhausbetriebs erfüllt werden. Die Informationssicherheit wird als gemeinschaftliche Aufgabe verstanden, die alle Mitarbeiter und Führungskräfte der Kreiskrankenhaus Greiz-Ronneburg GmbH aktiv unterstützen und fördern.

7. Informationssicherheitsprozess

Der Informationssicherheitsprozess orientiert sich an dem branchenspezifischen Sicherheitsstandard (B3S), sowie den Handlungsempfehlungen und Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und der internationalen Norm ISO/IEC 27001. Diese etablierten Standards und Normen bilden die Grundlage für die Auswahl und Umsetzung geeigneter Informationssicherheitsmaßnahmen.

Um die Informationssicherheit nachhaltig zu gewährleisten, die Sicherheitsziele zu erreichen und die Informationssicherheitsstrategie umzusetzen, ist ein Informationssicherheits-Managementsystem (ISMS) eingeführt worden, das dem internationalen Standard ISO/IEC 27001 entspricht. Das ISMS wird kontinuierlich weiterentwickelt und verbessert und umfasst alle notwendigen Bestandteile wie Regelungen, Rollen und Fähigkeiten, die zur Steuerung und Lenkung der Informationssicherheit erforderlich sind.

Das ISMS wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Diese Überprüfungen erfolgen risikoorientiert oder mindestens stichprobenartig durch den Informationssicherheitsberater (ISB). Darüber hinaus werden regelmäßige interne und externe Audits durchgeführt, um sicherzustellen, dass die Informationssicherheitsmaßnahmen geeignet sind, das erforderliche Sicherheitsniveau aufrechtzuerhalten und zu optimieren, und dass sie den Verantwortlichen bekannt sind, umgesetzt und in den Betriebsablauf integriert werden (siehe Richtlinie zur internen ISMS-Auditierung).

Die Geschäftsführung wird vierteljährlich sowie bei Bedarf über den aktuellen Stand der Informationssicherheit informiert. Diese Berichte berücksichtigen Änderungen der Bedrohungslage sowie relevante Informationssicherheitsvorfälle. Die Geschäftsführung unterstützt die ständige Verbesserung des Informationssicherheitsniveaus aktiv. Alle Beschäftigten sind aufgefordert und motiviert, sich über bestehende Regelungen und aktuelle Gefährdungen auf dem Laufenden zu halten und mögliche Verbesserungen, Schwachstellen sowie Auffälligkeiten zu melden.

Änderungen der Informationssicherheitsanforderungen, der Fach- und Kernaufgaben sowie der Organisation und Struktur der IT- und Kommunikationsarchitektur werden ebenfalls über die Informationssicherheitsorganisation kommuniziert und in den Informationssicherheitsprozess einbezogen.

Durch eine kontinuierliche Revision der Regelungen und deren Umsetzung sowie Einhaltung wird der Informationssicherheitsprozess und das ISMS überprüft. Abweichungen werden analysiert, um das aktuell erforderliche Informationssicherheitsniveau zu erreichen und zu optimieren.

8. Informationssicherheitsorganisation

Das Informationssicherheitsmanagementteam ist dafür verantwortlich, die Umsetzung der Informationssicherheitsmaßnahmen zu überwachen und bei Vorfällen im Bereich der Informationssicherheit geeignete Schritte einzuleiten. Neben dem Informationssicherheitsbeauftragten, der das Team leitet, spielt auch der IT-Teamleiter eine entscheidende Rolle. In Absprache mit der Geschäftsführung treffen diese beiden Schlüsselpersonen bei Bedarf kurzfristige Entscheidungen, um die Sicherheit der IT-Systeme und der Informationen sicherzustellen.

Die Hauptaufgaben des Teams bestehen in der Bearbeitung von Vorfällen im Bereich der Informationssicherheit. Es koordiniert die Organisation, dem Aufbau sowie die Durchführung und Überwachung der notwendigen Maßnahmen. Zudem ist es an der Entwicklung von Vorgaben beteiligt und stellt sicher, dass eine themenbezogene Schnittstelle zwischen den verschiedenen Abteilungen des Krankenhauses besteht. Bei Bedarf können jederzeit weitere Bereiche und Personen hinzugezogen werden, um die Informationssicherheit umfassend zu gewährleisten.

Komplexe Fragestellungen und technisch-organisatorische Maßnahmen zum Datenschutz werden von einem externen Datenschutzbeauftragen behandelt. Dieser arbeitet eng mit dem Informationssicherheitsmanagementteam zusammen und kommuniziert bei Bedarf zeitnah, um sicherzustellen, dass datenschutzrelevante Themen angemessen berücksichtigt werden.

Durch diese strukturierte und umfassende Informationssicherheitsorganisation wird sichergestellt, dass alle notwendigen Maßnahmen zur Erhaltung der Informationssicherheit effektiv koordiniert und umgesetzt werden.

9. Risikomanagement

Das Risikomanagement der Kreiskrankenhaus Greiz-Ronneburg GmbH ist ein zentraler Bestandteil der Informationssicherheitsstrategie und zielt darauf ab, potenzielle Bedrohungen frühzeitig zu erkennen und zu minimieren. Regelmäßige Risikoanalysen werden durchgeführt, um Schwachstellen in den informationsverarbeitenden Systemen und Prozessen zu identifizieren. Basierend auf den Ergebnissen dieser Analysen werden geeignete Maßnahmen entwickelt und implementiert, um die identifizierten Risiken zu mindern. Dieser Prozess wird kontinuierlich überwacht und angepasst, um sicherzustellen, dass er den aktuellen Bedrohungen und technologischen Entwicklungen gerecht wird.

Sämtliche Fachabteilungen der Kreiskrankenhaus Greiz-Ronneburg GmbH unterstützen auf Anforderung den Informationssicherheitsbeauftragten bei der Erstellung der Risikobewertung.

Ein System kann erst in das bestehende IT-Netzwerk oder in Betrieb genommen werden, wenn die Risikobewertung durchgeführt und vom Informationssicherheitsbeauftragten freigegen wird. Besteht hier eine potenzielle Gefahr so ist die Geschäftsführung vor der Inbetriebnahme zu informieren.

Durch diesen strukturierten Ansatz trägt das Risikomanagement wesentlich dazu bei, die Informationssicherheit und den reibungslosen Betrieb des Krankenhauses zu gewährleisten.

10. Weiterentwicklung der Informationssicherheit

Die Weiterentwicklung der Informationssicherheit ist ein kontinuierlicher Prozess, der darauf abzielt, das Sicherheitsniveau stetig zu verbessern und an neue Bedrohungen und technologische Veränderungen anzupassen.

Dies umfasst regelmäßige Schulungen und Sensibilisierungsmaßnahmen für alle Mitarbeiter, um das Bewusstsein für Informationssicherheit zu schärfen. Zudem werden neue Technologien und Verfahren eingeführt, die den Schutz sensibler Daten und Systeme weiter erhöhen. Durch regelmäßige Überprüfungen und Anpassungen der Sicherheitsrichtlinien und -maßnahmen wird sichergestellt, dass die Informationssicherheit stets den aktuellen Anforderungen entspricht und kontinuierlich optimiert wird.

11. Überprüfung der Leitlinie

Die Leitlinie zur Informationssicherheit wird regelmäßig überprüft und aktualisiert, um sicherzustellen, dass sie den aktuellen gesetzlichen Anforderungen und den sich ändernden Bedrohungslagen entspricht. Diese Überprüfungen erfolgen mindestens einmal jährlich oder bei wesentlichen Veränderungen der IT-Infrastruktur und der Bedrohungssituation. Anpassungen der Leitlinie werden von der Geschäftsführung genehmigt und allen Mitarbeitern kommuniziert, um eine kontinuierliche Verbesserung der Informationssicherheit zu gewährleisten.

12. Freigabe und Inkrafttreten

Diese Leitlinie ist durch die Unterschrift der Geschäftsführung in Kraft getreten. Alle Mitarbeiter sind verpflichtet, sich an die festgelegten Maßnahmen zu halten. Aktualisierung und Änderungen der Leitlinie werden ebenfalls durch die Geschäftsführung freigegeben und kommuniziert.