1 Einleitung

In dieser Informationssicherheitsleitlinie werden die für DIAKO Ev. Diakoniekrankhaus gemeinnützige GmbH (im Folgenden DIAKO) geltenden, grundlegenden Ziele der Informationssicherheit festgelegt.

Die Informationssicherheitsleitlinie des DIAKO

- beschreibt den Stellenwert der Informationssicherheit,
- legt den Geltungsbereich der Informationssicherheitsleitlinie fest,
- enthält das Bekenntnis der Geschäftsführung zu ihrer Verantwortung für die Informationssicherheit,
- legt die Sicherheitsstrategie fest,
- formuliert allgemeine Sicherheitsziele,
- definiert die Sicherheitsorganisation,
- verpflichtet zur kontinuierlichen Fortschreibung des Regelwerks zur Informationssicherheit,
- legt den Rahmen zur Veröffentlichung fest.

2 Stellenwert der Informationssicherheit

In unserem Krankenhaus werden schützenswerte Informationen verarbeitet, die nicht nur, aber weit überwiegend in elektronischer Form vorliegen und auf die ein schneller, sicherer und aktueller Zugriff gewährleistet sein muss. Informationsverarbeitung spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik (IT) maßgeblich unterstützt. Ein Ausfall von IT-Systemen muss weitgehend verhindert und insgesamt kurzfristig kompensiert werden können. Auch in Teilbereichen darf der stationäre Patientenversorgungsprozess nicht zusammenbrechen. Da unsere kritische Dienstleistung in der stationären Patientenversorgung sowie im Betrieb einer Notfallambulanz, eines Kreißsaales und einer Intensivstation liegt, sind die Verfügbarkeit und der Schutz dieser Informationen vor unberechtigtem Zugriff und vor unerlaubter Änderung von existenzieller Bedeutung. Daher gilt es die Verfügbarkeit, Integrität (Vollständigkeit und Richtigkeit) und Vertraulichkeit von Informationen angemessen sicherzustellen. Durch diese Leitlinie zur Informationssicherheit übernimmt der Geschäftsführer die Gesamtverantwortung für die Informationssicherheit. Aus dieser Verantwortung heraus führen wir ein Informationssicherheits-Managementsystem (ISMS) ein. Dazu gehören die Schaffung einer Informationssicherheitsorganisation und die Bereitstellung entsprechender Ressourcen zur Entwicklung eines angemessenen Sicherheitskonzeptes sowie die regelmäßige Überprüfung der Maßnahmen auf ihre Angemessenheit und Wirksamkeit.

3 Geltungsbereich

Diese Leitlinie gibt den Rahmen für die Informationssicherheit im DIAKO vor. Sie gilt verbindlich für alle Bereiche und Abteilungen.

4 Sicherheitsstrategie

Die Sicherheitsstrategie für das DIAKO besteht darin, mit wirtschaftlichem Ressourceneinsatz ein hinreichendes Maß an Sicherheit zu erreichen, um aktuellen und zukünftigen Risiken angemessen zu begegnen. Dieser Prozess wird durch die Einführung eines Informations-Sicherheits-Management-Systems (ISMS), orientiert an der ISO 27001 (nativ), etabliert. Dabei werden auch die Vorgaben des Branchenspezifischen Sicherheitsstandards für die Gesundheitsversorgung im Krankenhaus (B3S) sowie die IT-Sicherheitsverordnung (ITSVO-EKD) der evangelischen Kirche in Deutschland im angemessenen Umfang berücksichtigt.

5 Festlegung von Sicherheitszielen

Für das DIAKO werden auf dieser Basis die nachstehenden Ziele für die Informationssicherheit festgelegt:

Vertraulichkeit

Vertraulichkeit ist der Schutz vor unbefugter Preisgabe von Informationen. Vertrauliche Daten und Informationen dürfen ausschließlich einem berechtigten Personenkreis zur Verfügung stehen.

Integrität

Integrität bezeichnet die Sicherstellung der Korrektheit von Daten und der korrekten Funktionsweise von Systemen. Die physische und logische Unversehrtheit von Systemen, Anwendungen und Daten muss jederzeit gewahrt sein. Dies schließt auch die Verhinderung einer unberechtigten Erstellung oder Änderung von Informationen mit ein.

Verfügbarkeit

Systeme, Anwendungen, Daten und Informationen müssen den Berechtigten stets wie vorgesehen zur Verfügung stehen.

6 Festlegung von Schutzzielen

In Abwägung der Risiken, der Werte der zu schützenden Güter sowie des vertretbaren Aufwands an Personal und Finanzmitteln, sind die folgenden Aspekte zur Informationssicherheit besonders wichtig:

- Geschäftsprozesse, Anwendungen und Informationstechnik müssen sorgfältig durchdacht werden und einfach zu steuern sein. **Komplexe Strukturen**, die zu unnötigen Risiken führen, sind zu **vermeiden**.
- Gebäude und Räumlichkeiten werden durch ausreichende **Zutrittskontrollen** geschützt. Der Zugang zu den IT-Systemen wird durch angemessene **Zugangskontrollen** und der Zugriff auf die Informationen durch ein restriktives **Berechtigungskonzept** geschützt.
- Es ist darauf zu achten, dass **bei Investitionen** die Belange der Informationssicherheit angemessen **berücksichtigt** sind.
- Die Kommunikation mit **externen Netzen** ist besonders zu schützen. Dies betrifft sowohl Zugriffe von außen in unser Netzwerk (z.B. Fernwartung oder Partnernetzzugänge), als auch Zugriffe aus unserem Netzwerk in fremden Systemen.
- Der Informationssicherheitsbeauftragte ist frühzeitig **in Projekte einzubinden**, um schon in der Planungsphase sicherheitsrelevante Aspekte zu berücksichtigen. Sofern personenbezogene Daten betroffen sind gilt gleiches für den Datenschutzbeauftragten.

- Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine **umfassende Datensicherung** wird daher gewährleistet, dass der IT-Betrieb kurzfristig 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. Maßnahmen für den Notfall werden in einem separaten **Notfallvorsorgekonzept** zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.
- Sofern IT-Dienstleistungen an **externe Stellen** ausgelagert werden, werden von uns konkrete Sicherheitsanforderungen in den **Service Level Agreements** vorgegeben. Das Recht auf **Kontrolle** wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben erstellen wir ein detailliertes Sicherheitskonzept mit konkreten Maßnahmenvorgaben.

7 Verantwortlichkeiten

7.1 Geschäftsführung

Der Geschäftsführer initiiert den Informationssicherheitsprozess und stellt im angemessenen Umfang Ressourcen bereit, um die in dieser Leitlinie formulierten Ziele zu erreichen. Er überwacht kontinuierlich die Zielerreichung; dazu lässt er sich u.a. vom Informationssicherheitsbeauftragten berichten.

7.2 Informationssicherheitsbeauftragte

Der Informationssicherheitsbeauftragten und den Administratoren werden von der Leitung ausreichende finanzielle und zeitliche Ressourcen zur Verfügung gestellt, um sich regelmäßig weiterzubilden und zu informieren und die vom Management festgelegten Informationssicherheitsziele zu erreichen.

Die Informationssicherheitsbeauftragte ist verantwortlich für die Konzeption und Umsetzung der Informationssicherheitsmaßnahmen. Dazu arbeitet sie mit allen erforderlichen Stellen zusammen. Als Betriebsbeauftragte für den Datenschutz berücksichtigt sie gleichzeitig, ob personenbezogene Daten durch Maßnahmen oder Sicherheitsvorfälle betroffen sein könnten.

7.3 Betriebsbeauftragte für den Datenschutz

Die Informationssicherheitsbeauftragte ist zugleich als Betriebsbeauftragte für den Datenschutz nach Maßgabe des Datenschutzgesetzes der evangelischen Kirche (DSG-EKD) bestellt. Die Datenschutzbeauftragte hat ein ausreichend bemessenes Zeitbudget für die Erfüllung ihrer Pflichten zur Verfügung. Die Betriebsbeauftragte für den Datenschutz ist angehalten, sich regelmäßig weiterzubilden.

7.4 Mitarbeiterinnen und Mitarbeiter

Alle Mitarbeiterinnen und Mitarbeiter müssen sich möglicher Gefährdungen bewusst sein und sich sicherheitsgerecht verhalten. Dazu sollen Informationen als Sensibilisierungsmaßnahmen zur Informationssicherheit beitragen.

Durch Sicherheitsmängel im Umgang mit Informationen verursachte Ersatzansprüche, Schadensregulierungen und Image-Schäden müssen verhindert werden.

Im Umgang mit elektronischen Dokumenten und Informationen sind diese Leitlinie und vorhandene Anweisungen strikt zu befolgen. Das Schutzziel Integrität umfasst auch die Authentizität, d.h. die Echtheit, Zurechenbarkeit und Glaubwürdigkeit von Informationen.

Die IT-Nutzer/innen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen der Informationssicherheitsbeauftragten zu halten.

Des Weiteren unterstützen die Nutzer/innen durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

IT-Nutzer/innen nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Die Unternehmensleitung unterstützt dabei die bedarfsgerechte Fort- und Weiterbildung.

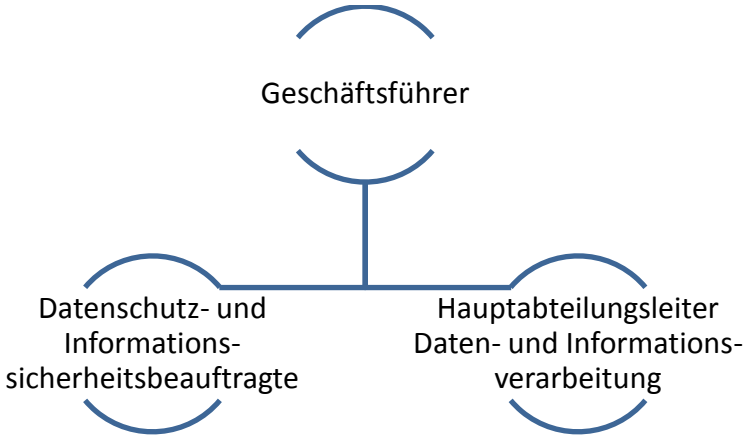
8 Etablierung eines Lenkungskreises für das ISMS

Der Lenkungskreis des ISMS bespricht alle Maßnahmen der Informationssicherheit und bereitet diese für die Umsetzung im klinischen Umfeld vor.

Ständige Mitglieder sind der Leiter der Hauptabteilung Daten- und Informationsverarbeitung sowie die Datenschutz- und Informationssicherheitsbeauftragte. Bei Bedarf werden weitere Akteure aus der IT Abteilung, der Verwaltung und den Bereichen Medizin und Pflege hinzugezogen.

Strategische Entscheidungen zur Informationssicherheit erfordern die Freigabe durch den Geschäftsführer. Die Führungskräfte des Hauses werden im Rahmen übergreifender Gremien (Krankenhauskonferenz, Chefarzt-Konferenz, Hauptabteilungsleiter-Konferenz) hierzu informiert.

9 Organisationsstruktur für Informationssicherheit



10 Aktualisierung der Leitlinie für Informationssicherheit

Im Rahmen des Informationssicherheitsprozesses überprüft die Informationssicherheitsbeauftragte diese Leitlinie jeweils spätestens nach zwei Jahren auf Aktualität und initiiert ggf. eine Anpassung.