Informationssicherheits-leitlinie

Inhaltsverzeichnis

1 Einleitung

Das Städtische Klinikum Dresden (SKDD) ist eine der führenden Gesundheitseinrichtungen in der Region Dresden und bietet seinen Patientinnen und Patienten eine umfassende stationäre und ambulante medizinische Versorgung. Zusätzlich dazu unterhält das SKDD eine eigene Medizinische Berufsfachschule.

Die Informationsverarbeitung spielt eine Schlüsselrolle für die Aufgabenerfüllung des SKDD. Alle wesentlichen strategischen und operativen Geschäftsprozesse, insbesondere auch die Kernkompetenz im Bereich der medizinischen und pflegerischen Patientenversorgung, sind in hohem Maße von einem sicheren und zuverlässigen Funktionieren der Informations-, Medizin- und Kommunikationstechnik sowie der Gebäude- und Versorgungstechnik abhängig.

Die vorliegende Informationssicherheitsleitlinie ist ein Bestandteil des Informationssicherheitsmanagementsystems (ISMS), das die Herstellung und den Erhalt des erforderlichen Sicherheitsniveaus der Informationen und Daten sicherstellt, die zur Erbringung der kritischen Dienstleistung der vollstationären Versorgung im SKDD notwendig sind.

Das ISMS beinhaltet Organisations- und Prozessstrukturen sowie ein Regelwerk, die insgesamt geeignet sind, Planung, Umsetzung und Überprüfung von Sicherheitsmaßnahmen im Geltungsbereich zu gewährleisten.

1.1 Geltungsbereich

Die Informationssicherheitsleitlinie gilt für das gesamte Städtische Klinikum. Das Ziel ist es, ein angemessenes Sicherheitsniveau zu erreichen und dauerhaft aufrecht zu erhalten, um damit das Vertrauen der Patientinnen und Patienten, der Mitarbeitenden sowie der Dienstleister und Lieferanten zu stärken.

Die Informationssicherheitsleitlinie ist für alle Mitarbeitenden und Geschäfts-/ Vertragspartner des SKDD verpflichtend. Das Dokument ist allen Mitarbeitenden und Geschäfts-/ Vertragspartnern des SKDD zugänglich zu machen. Detaillierte Richtlinien und Bestimmungen werden für die einzelnen Bereiche in separaten Dokumenten erstellt.

1.2 Ansprechpartnerin

Ansprechpartnerin für Fragen zu dieser Richtlinie ist die Informationssicherheitsbeauftragte (Kontakt: ISB@klinikum-dresden.de).

1.3 Verantwortlichkeiten

Diese Leitlinie hat die Betriebsleitung des SKDD freigegeben.

2 Informationssicherheitsziele und Stellenwert der Informationssicherheit

Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten und gespeicherten Daten.

Die Hauptaufgabe des SKDD ist die zuverlässige Sicherstellung der medizinischen Versorgung der Bevölkerung. Grundlegende Ziele der **Informationssicherheit** in diesem Zusammenhang sind die Realisierung von angemessener Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität von Informationen.

Verfügbarkeit von Dienstleistungen und Funktionen eines Informationssystems, IT-Systemen, der IT-Netzinfrastruktur oder auch von Informationen ist dann gegeben, wenn diese von den Anwenderinnen und Anwendern stets wie vorgesehen genutzt werden können.

Vertraulichkeit stellt den Schutz vor unbefugter Preisgabe von Informationen sicher. Vertrauliche Daten und Informationen dürfen ausschließlich Befugten in zulässiger Weise zugänglich sein.

Integrität bezeichnet die Sicherstellung der Korrektheit (Unversehrtheit) von Informationen und der korrekten Funktionsweise von Systemen.

Authentizität der Informationen ist sichergestellt, wenn sie von der angegebenen Quelle stammen.

Die Umsetzung dieser allgemeinen Schutzziele der Informationssicherheit sind von großer Bedeutung für die Gewährleistung der **Patientensicherheit** und **Behandlungseffektivität** im Städtischen Klinikum. Ein Ausfall der Informationstechnik oder Verletzungen der Vertraulichkeit und Integrität von Informationen kann die Existenz des SKDD gefährden.

Ziel des SKDD ist es, die Daten und IT-Systeme in allen technikabhängigen Bereichen in ihrer Verfügbarkeit so zu sichern, dass die zu erwartenden Ausfallzeiten der Systeme und der maximale Datenverlust toleriert werden können. Auch gilt es, die Integrität und Vertraulichkeit von sensiblen Unternehmensdaten und personenbezogenen Daten in ausreichender Weise zu garantieren; hierzu gehören Patientendaten genauso wie Personaldaten oder technische Unterlagen. Schadensfälle mit Gefährdung von Patientinnen und Patienten, hohen finanziellen Auswirkungen sowie/oder immateriellen Folgen in Form von Imageschäden für das SKDD müssen verhindert werden. Beeinträchtigungen hinsichtlich der Verfügbarkeit der unternehmenseigenen Applikationen können ebenso gravierende Auswirkungen nach sich ziehen wie Unregelmäßigkeiten in Bezug auf die Integrität und Vertraulichkeit der verarbeiteten bzw. benutzten Informationen. Die Verfügbarkeit, Vertraulichkeit und Integrität der Informationen, Anwendungen und IT-Systeme werden nicht nur durch Externe bedroht, sondern können auch durch interne Schwachstellen gefährdet werden.

Als Kritische Infrastruktur (KRITIS) nach §8a Absatz 2 des BSI-Gesetzes und nach §6 KritisV, gelten besondere Anforderungen an das SKDD bzgl. der Sicherstellung der kritischen Dienstleistung stationäre medizinische Versorgung. Die Maßnahmen für Informationssicherheit sollen auch dazu beitragen, dass die für das SKDD relevanten Gesetze, Vorschriften und vertraglichen Verpflichtungen eingehalten werden. Als wichtigste zu beachtende Rahmenbedingungen gelten dabei:

- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz)
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)
- Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz 2.0)
- Branchenspezifischer Sicherheitsstandards (B3S) „Medizinische Versorgung“
- Datenschutz-Grundverordnung (DSGVO)

Nach Inkrafttreten gelten zusätzlich:

- Gesetz zur Umsetzung der Richtlinie (EU) 2022/2557 und zur Stärkung der Resilienz von Betreibern kritischer Anlagen (KRITIS-DachG)
- NIS2-Umsetzungsgesetz (NIS2UmsuCG)

3 Grundsätze der Informationssicherheit

Die nachfolgenden Grundsätze bestimmen die Gestaltung der Informationssicherheit am Städtischen Klinikum:

- Gesetzliche, branchenspezifische und vertragliche Anforderungen an die Informationssicherheit werden erfüllt.
- Maßgebliche Kriterien für geeignete Sicherheitsmaßnahmen sind deren Wirksamkeit in Verbindung mit einem akzeptierbaren Restrisiko unter Berücksichtigung der wirtschaftlichen Angemessenheit.
- Alle Einrichtungen, die der Erstellung, Speicherung und Übertragung von Daten dienen, sind so ausgewählt, integriert und konfiguriert, dass für die auf ihnen verarbeiteten Daten zu jeder Zeit und unter allen Umständen ein angemessenes Maß an Vertraulichkeit, Integrität und Verfügbarkeit sichergestellt ist. Dies gilt auch für die Orte zur Aufbewahrung der Medien zur Datensicherung.
- Das Angebot regelmäßiger und anlassbezogener Schulungen und Sensibilisierungsmaßnahmen ist Bestandteil des Informationssicherheitsmanagementprozesses, um Anwenderinnen, Anwender und IT-Fachpersonal für die Belange der Informationssicherheit zu sensibilisieren und zu qualifizieren.
- Durch eine kontinuierliche Überprüfung der Wirksamkeit und Angemessenheit der Sicherheitsmaßnahmen sowie der vorhandenen Regelungen und deren Einhaltung wird das angestrebte Informationssicherheits- und Datenschutzniveau sichergestellt.
- Verletzungen der Informationssicherheit werden kommuniziert und dokumentiert, so dass zeitnah, angemessen und nachhaltig auf sie reagiert werden kann.

4 Informationssicherheitsorganisation

Als zentrale Sicherheitsinstanz ernennt die Klinikleitung eine **Informationssicherheitsbeauftragte** (ISB), die als Verantwortliche für das Informationssicherheitsmanagementsystem den Informationssicherheitsprozess steuert und als zentrale Ansprechpartnerin für Mitarbeitende und Dritte fungiert.

Sie ist direkt der Klinikleitung unterstellt, unterstützt sie in zentralen Fragen der Informationssicherheit und erstattet der Klinikleitung regelmäßig Bericht über den aktuellen Stand der Informationssicherheit, insbesondere über Risiken und Sicherheitsvorfälle.

Anforderungen, Aufgaben und Befugnisse sind in der Bestellungsurkunde detailliert aufgeführt.

Die Informationssicherheitsbeauftragte kann zu ihrer Unterstützung ein Informationssicherheitsmanagementteam bilden, dem Mitarbeitende aus den Bereichen Datenschutz, Risikomanagement, Qualitätsmanagement, Informations-, Versorgungs- und Medizintechnik sowie Vertreterinnen und Vertretern der medizinisch-pflegerischen Bereiche angehören.

5 Verantwortlichkeiten

Die **Klinikleitung** trägt die Gesamtverantwortung für die Informationssicherheit am SKDD. Sie ist insbesondere verantwortlich für:

- die Initiierung, Steuerung und Kontrolle des Sicherheitsprozesses und dessen kontinuierliche Verbesserung,
- die Entscheidung über (Risiko-)Maßnahmen, Restrisiken und deren Konsequenzen,
- die Bekanntgabe und Durchsetzung der Ziele der Informationssicherheit sowie der glaubhaften und nachhaltigen Vermittlung ihrer Bedeutung gegenüber Mitarbeitenden, Patientinnen und Patienten sowie Dritten,
- die Integration der Informationssicherheit in alle Prozesse und Projekte des SKDD,
- die Definition und Festlegung der erforderlichen Verantwortlichkeiten und Befugnisse (inkl. Sicherstellung der Trennung widersprüchlicher Aufgaben und Verantwortungsbereiche),
- die Schaffung entsprechender Rahmenbedingungen zur nachhaltigen Umsetzung des Informationssicherheitsmanagements durch Bereitstellung der notwendigen organisatorischen, personellen und finanziellen Ressourcen,
- die Umsetzung und Überprüfung eines wirksamen Informationssicherheitsmanagements durch fortlaufende Kontrolle der Zielerreichung,
- die Sicherstellung eines angemessenen Qualifikationsniveaus der Mitarbeitenden entsprechend ihrer Aufgaben, Kompetenzen und Verantwortlichkeiten.

Die **Informationssicherheitsbeauftragte** steuert die Umsetzung und Weiterentwicklung des Informationssicherheitsmanagementsystems am SKDD. Sie ist insbesondere verantwortlich für:

- die Steuerung und Koordinierung des von der Klinikleitung initiierten Informationssicherheitsprozesses und dessen Weiterentwicklung und Kontrolle,
- Initiierung der Erarbeitung konkreter Verbesserungsvorschläge zur Erreichung des angestrebten Informationssicherheitsniveaus durch die operativ verantwortlichen Organisationseinheiten,
- die Überprüfung der Umsetzung der Vorgaben zur Informationssicherheit,
- die Erstellung, Fortschreibung und Umsetzung dieser Leitlinie und weiterer abgeleiteter Richtlinien und sonstiger Dokumente,
- die Initiierung, Weiterentwicklung und Kontrolle von Sensibilisierungs- und Schulungsmaßnahmen der Mitarbeitenden,
- Prüfung und Freigabe neuer Anwendungen, Verfahren und Prozesse aus Sicht der Informationssicherheit,
- die Untersuchung informationssicherheitsrelevanter Ereignisse.

Die **IT-Leitung** ist die zentrale Instanz für die operative IT-Sicherheit. Sie ist insbesondere verantwortlich für:

- den sicheren Betrieb der IT,
- die Umsetzung geeigneter Sicherheitsmaßnahmen,
- die frühzeitige Einbindung der ISB in IT-Projekte.

Die **Prozess-/Anwendungsverantwortlichen** (Chefärzte, Chefärztinnen, Pflegedienst-, Ressort- und Abteilungsleitungen) tragen in dem ihnen zugewiesenen Zuständigkeitsbereich die Verantwortung für:

- die zugehörigen Informationen und Daten sowie die Planung und Umsetzung angemessener technischer und organisatorischer Maßnahmen zur Informationssicherheit in Abstimmung mit der ISB,
- die Einstufung der Schutzbedarfe/ Kritikalität der verantworteten Prozesse/ Anwendungen / Assets hinsichtlich der Schutzziele Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität unter Berücksichtigung der Patientensicherheit und Behandlungseffektivität in Abstimmung mit der ISB,
- die Abstimmung von Maßnahmen, die aus ihrer Sicht zur Verbesserung und Erhaltung der Informationssicherheit im eigenen Verantwortungsbereich ergriffen werden müssen, mit der ISB,
- die Erstellung und regelmäßige Aktualisierung von Notfallplänen bzw. Notbetriebsbeschreibungen für die verantworteten Prozesse bzw. Anwendungen,
- die Unterstützung der Umsetzung des Informationssicherheitsrisikomanagements durch die Analyse und Bewertung der von ihnen verantworteten Informationssicherheitsrisiken (unter Berücksichtigung des jeweiligen Schutzbedarfes), der Vorbereitung von Entscheidungen zur Behandlung und periodischen Überprüfung der verantworteten Informationssicherheitsrisiken einschließlich der zugeordneten Maßnahmen.

Die **Mitarbeitenden** tragen die Verantwortung, die Informationssicherheit durch verantwortungsbewusstes Handeln und Einhaltung der relevanten Gesetze, Vorschriften, Richtlinien, Anweisungen und vertraglichen Verpflichtungen zu gewährleisten. Sie gehen korrekt und verantwortungsvoll mit den von ihnen genutzten IT-Systemen, Daten und Informationen um und wirken aktiv an der Abwehr und Bekämpfung von materiellen und immateriellen Schäden mit. Im Kontext der medizinischen Versorgung existieren auch besondere Datenschutzanforderungen. Um die sensiblen Informationen angemessen zu schützen, halten die Mitarbeitenden ihre rechtlichen und ethischen Verantwortlichkeiten ein. Zusätzlich verpflichten sich alle Mitarbeitenden, Informationssicherheitsvorfälle und mögliche Informationssicherheitslücken an ihre Vorgesetzten und die Informationssicherheitsbeauftragte oder die IT zu melden. Es wird erwartet, dass alle Nutzenden von IT-Systemen die vorliegende Informationssicherheitsleitlinie kennen und beachten.

Externe Leistungserbringer, also Personen, Behörden und Unternehmen, die nicht zum Städtischen Klinikum gehören, für dieses aber Leistungen erbringen (Auftragnehmer), haben die Vorgaben des Auftraggebers zur Einhaltung der Informationssicherheitsziele gemäß dieser Leitlinie einzuhalten. Der Auftraggeber informiert den Auftragnehmer über diese Regeln und verpflichtet ihn in geeigneter Weise zur Einhaltung. Dazu gehört auch, dass der Auftragnehmer bei erkennbaren Mängeln und Risiken eingesetzter Sicherheitsmaßnahmen den Auftraggeber zu informieren hat.

6 Verstöße und Sanktionen

Alle Mitarbeitenden des Städtischen Klinikums werden zu einem sorgfältigen Umgang mit Daten, Informationen, Anwendungen, IT-Systemen und Kommunikationsnetzen verpflichtet. Eine Verletzung oder Gefährdung der Informationssicherheit durch vorsätzliche oder grob fahrlässige Handlungen, wie zum Beispiel

- der Missbrauch von Daten,
- der unbefugte Zugriff auf Informationen,
- die unbefugte Änderung von Informationen,
- die unbefugte Übermittlung von Informationen,
- die illegale Nutzung (auch Preisgabe) von Informationen,
- die Gefährdung der Informationssicherheit Dritter oder
- die wiederholte Missachtung vorhandener Dienstanweisungen

kann dienst- und arbeitsrechtliche sowie straf- und zivilrechtliche Folgen nach sich ziehen. Solche Verstöße gegen die Informationssicherheit sind unverzüglich der Informationssicherheitsbeauftragten zu melden.

7 Sicherung und Verbesserung der Informationssicherheit

Der Informationssicherheitsprozess ist regelmäßig auf seine Aktualität und Wirksamkeit zu überprüfen. Insbesondere sind die Maßnahmen regelmäßig daraufhin zu untersuchen, ob sie den betroffenen Mitarbeitenden bekannt, umsetzbar und in den Betriebsablauf integrierbar sind.

8 Gültigkeit

Die Informationssicherheitsleitlinie tritt mit Freigabe durch den Kaufmännischen Direktor in Kraft und ist jährlich durch die ausgebende Stelle zu prüfen. Die Klinikleitung bekennt sich zur Informationssicherheitsleitlinie und sichert deren Durchsetzung zu.