Informationssicherheitsleitlinie

Inhaltsverzeichnis

1 ZIELSETZUNG 2
2 GELTUNGSBEREICH 3
3 GELTUNGSDAUER UND REVISION 3
4 ZWECK 3
5 STELLENWERT DER INFORMATIONSSICHERHEIT 4
6 DEFINIERTE SCHUTZZIELE 5
7 SICHERSTELLUNG DER SCHUTZZIELE 6
8 KONTINUIERLICHE VERBESSERUNG 7

Abkürzungen:

DSB = Datenschutzbeauftragter

IS = Informationssicherheit

ISB = Informationssicherheitsbeauftragte

ISMS = Informationssicherheitsmanagementsystem

IKT = Informations- und Kommunikationstechnik

B3S = Branchenspezifische Sicherheitsstandard

Die in der Leitlinie gewählten Begrifflichkeiten und Ziele für die IS entsprechen den Formulierungen des B3S für die Gesundheitsversorgung im Krankenhaus. Nähere Erläuterungen hierzu stellt die DKG über Ihre Homepage zur Verfügung.

1 Zielsetzung

Diese Leitlinie ist Bestandteil der Unternehmenskultur und ist Ausdruck und Willenserklärung des Managements der Städtische Kliniken Mönchengladbach GmbH (SKMG). Sie umfasst den Zweck, Stellenwert und die Ziele der Informationssicherheit sowie Grundlagen und Grundsätze. Eine wesentliche Orientierung bietet der Branchenspezifische Sicherheitsstandard (B3S) und der ISO/IEC 27001 für die Gesundheitsversorgung im Krankenhaus:

- Regeln ändern sich in einer zunehmend dynamischen Welt.
- Informationssicherheit bedeutet zuerst Bewusstsein.
- Informationssicherheit ist ein Anspruch, dessen Verwirklichung trainiert werden muss.

Ziel dieser Informationssicherheitsleitlinie ist die Richtungsvorgabe bei der Informationssicherheit in Übereinstimmung mit Geschäftsanforderungen und geltenden Gesetzen und vertraglichen Anforderungen zur Verankerung des ISMS gemäß ISO/IEC 27001 und B3S. Die vorliegende Informationssicherheitsleitlinie definiert die Informationssicherheitspolitik der SKMG, welche unter Berücksichtigung der kritischen Dienstleistungen (kDL) in der:

„*vollstationären Versorgung***“**

als Handlungsleitfaden zur Hervorhebung der Relevanz der Informationssicherheitsziele, -Grundwerte, -Sicherheitsmaßnahmen und Aufrechterhaltung dieser Ziele unter dem Aspekt der kontinuierlichen Verbesserung herangezogen wird. Daher verstehen wir die Informationssicherheit als eine Verpflichtung, eine grundsätzliche Einstellung und einen Prozess der kontinuierlichen Verbesserung **(PDCA-Zyklus),** der zur Sicherstellung und Aufrechterhaltung der IS-Ziele im Hinblick auf **digitale**, aber auch **analoge** Daten und Informationen führen soll.

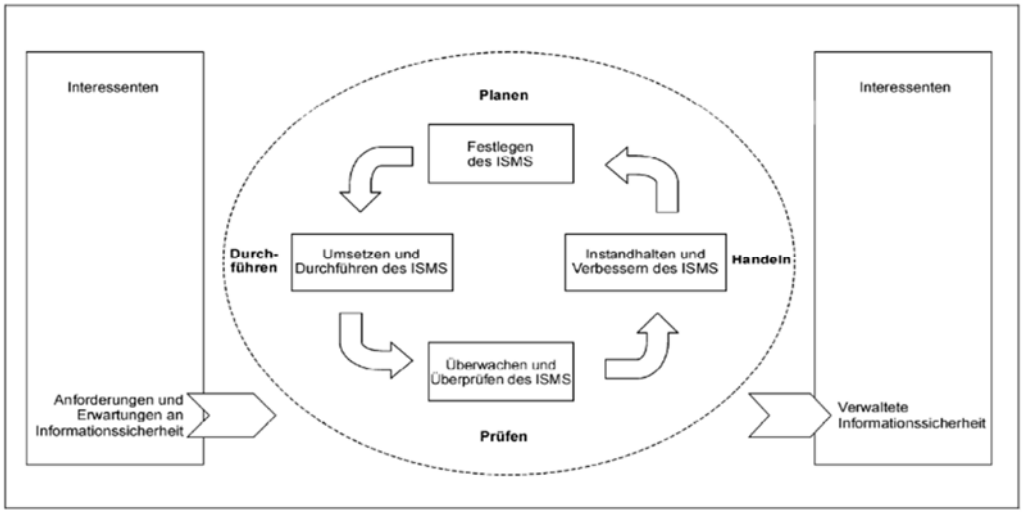

Abbildung: Lebenszyklus nach Deming - PDCA-Zyklus (Quelle: BNetzA, IT-Sicherheitskatalog)

2 Geltungsbereich

Der Geltungsbereich bezeichnet den Anwendungsbereich der ISO/IEC 27001 und B3S Zertifizierung. Zum Anwendungsbereich der Zertifizierung gehören die Planung, Wartung, Instandhaltung und Betrieb der Informations- und Datenverarbeitungssysteme sowie die Gesamtheit der ISMS-Relevanten Bereiche und kritische medizinische Dienstleistungen.

Begründung für die Auswahl:

- Start der Zertifizierungsbestrebungen mit Konzentration auf einen Kernbereich der Klinik
- Der Schutzbedarf der Informations- und Kommunikationstechnik um das Krankenhausumfeld ist hoch.
- Die vollstationäre Versorgung nimmt einen bedeutenden Anteil unserer Geschäftsanforderungen ein.
- Wir wählen daher bewusst einen großen und bedeutsamen Anwendungsbereich aus.
- Auch ist uns bewusst, dass diese Informationssicherheit gelebt werden muss,
- Diese ganzheitliche (erweiterte) Konzentration stellt einen dynamischen Prozess dar, der dazu führen soll die Informationssicherheit innerhalb der Organisationsgrenzen zu erhöhen und diese kontinuierlich (in einem zweijährigen Überwachungszyklus) zu optimieren.

3 Geltungsdauer und Revision

Die Geltungsdauer des vorliegenden Dokumentes ist bis zum Erscheinen einer neueren Version gültig. Das vorliegende Dokument wird regelmäßig auf Aktualität, Vollständigkeit geprüft und bei Bedarf angepasst.

Verantwortlich: Informationssicherheitsbeauftragter des Unternehmens

Revisionszyklus: jährlich oder anlassbezogen

4 Zweck

Unsere moderne Gesellschaft ist in hohem Maße von einer funktionierenden medizinischen Versorgung abhängig. Fehlen diese kritischen Dienstleistungen innerhalb der medizinischen Handlungsfelder eines Krankenhauses, wie beispielsweise innerhalb der:

Aufnahme, **Diagnostik**, **Therapie** und **Pflege,**

kommt die Versorgung der Patienten mit notwendiger Patientensicherheit und Behandlungseffektivität innerhalb kürzester Zeit zum Erliegen und lebensnotwendige und lebensrettende Maßnahmen und Dienstleistungen können nicht mehr erbracht werden. Durch dieses hohe Maß an Abhängigkeiten ist eine funktionierende IKT-Infrastruktur unumgänglich. Neben den „normalen" Ursachen des Ausfalls einer solchen IKT-Infrastruktur treten heute insbesondere Ursachen auf, die auf die starke horizontale Vernetzung der Computertechnologie und auf die zunehmende Digitalisierung der Medizintechnik zurückzuführen sind. Die Hauptprobleme sind heute vielfach die Schwachstellen in Hard- und Software sowie in den organisatorischen Abläufen, die es ermöglichen, ernsthafte Schäden anzurichten.

In diesem Zusammenhang ist das Primärziel der SKMG die Sicherstellung und Aufrechterhaltung der **medizinischen vollstationären Versorgung**. Die SKMG sieht ihre Hauptaufgabe darin, ihre kritischen Geschäftsprozesse dahingehend mit angemessenen technischen und organisatorischen Maßnahmen zu schützen, sodass die Versorgungssicherheit der medizinischen Dienstleistungen zu jedem Zeitpunkt gegeben ist.

Der Zweck dieser Informationssicherheitsleitlinie liegt in der Betonung des fortlaufend angestrebten Sicherheitsniveaus und verpflichtet alle adressierten Akteure zur Anerkennung und Einhaltung der Maßnahmen, die letztlich im Sinne der **kontinuierlichen Verbesserung** zur Optimierung und Erreichung des definierten Sicherheitsniveaus beitragen sollen. Demzufolge stellt die vorliegende Informationssicherheitsleitlinie die **Relevanz der Informationssicherheit** in den Vordergrund – also die Sicherheit von analogen und digitalen Prozesse, Systeme, Informationen und Daten, und verabschiedet daher diese Informationssicherheitsleitlinie für seine Mitarbeiter, Patienten, Lieferanten, Dienstleister und Dritten.

5 Stellenwert der Informationssicherheit

Informations- und Kommunikationstechnologie (IKT) spielt eine Schlüsselrolle für unsere Aufgabenerfüllung. Sie ist ein unverzichtbarer integraler Bestandteil der definierten medizinischen Versorgungsprozesse, insbesondere im Hinblick auf die Kritischen Dienstleistungen.

Der Einsatz der vernetzen Computertechnologie trägt demzufolge zur Sicherstellung und Aufrechterhaltung der geforderten, hohen Versorgungssicherheit, um auch weiterhin eine sichere und effektive Patientenversorgung zu bewahren. Hierbei stehen die Sicherstellung und Aufrechterhaltung der **Patientensicherheit** und **Behandlungseffektivität** im Vordergrund.

In diesem Zusammenhang werden alle wesentlichen operativen Funktionsbereiche und Aufgaben innerhalb der medizinischen Versorgung durch Information- und Kommunikationstechnik maßgeblich unterstützt. Das Vertrauen unserer Patienten, Mitarbeiter, Lieferanten und Dritte und letztlich unser Geschäftserfolg beruhen darauf, dass wir insbesondere

- die gesetzlichen und regulativen und selbstauferlegten Vorgaben **regelmäßig überprüfen und einhalten**,
- unsere kritischen Geschäftsprozesse und Dienstleistungen, die maßgeblich für die Versorgungsicherheit sind, **präventiv, reaktiv und detektiv** schützen,
- die **Vertraulichkeit, Integrität** und **Authentizität** der Gesundheitsdaten unserer Patienten wahren,
- Nachvollziehbarkeit und Transparenz unserer Dienstleistungen gewährleisten,
- Risiken minimieren,
- die Sicherstellung und Aufrechterhaltung der Betriebsfähigkeit **(Verfügbarkeit)** der IT-Systeme und Informationen und Daten bewahren,
- die notwendigen fachlichen**, personellen und finanziellen Ressourcen** zur Sicherstellung und Aufrechterhaltung der o.g. Punkte ermöglichen.

Für die SKMG ist die Gewährleistung der Informationssicherheit nicht nur Verpflichtung zur Erfüllung gesetzlicher und regulatorischer Auflagen, sondern auch ein Gütezeichen für patientenwohlorientierte Dienstleistungen. Informationssicherheit hat damit einen bedeutenden unternehmerischen Stellenwert.

6 Definierte Schutzziele

Zur Sicherstellung eines Sicherheitsniveaus für die Nutzer und deren Daten/Informationen, das den gesetzlichen Anforderungen entspricht, gelten die folgenden Sicherheitsziele für den expliziten ISMS-Anwendungsbereich und die IT-Landschaft:

Verfügbarkeit

ist die Zur-Verfügung-Stellung von Diensten und -Dienstleistungen, die es den Benutzern jederzeit (mit Ausnahme zumutbarer Ausfallzeiten) ermöglichen, diese im zugesicherten Rahmen zu nutzen. Im Einzelnen wird sichergestellt, dass eine angemessene Verfügbarkeit gewährleistet ist. Durch die Vorgaben des IT-Sicherheitskatalogs wird die Verfügbarkeit gesondert in Betracht gezogen.

Vertraulichkeit

ist der Schutz vor unbefugter Preisgabe von Nachrichten, Daten und Informationen gegenüber anderen Nutzern, unautorisierten Mitarbeitern oder Dritten. Vertrauliche Daten und Informationen werden ausschließlich Befugten in der zulässigen Weise zugänglich gemacht. Dies beinhaltet für den IT- Informationsverbund insbesondere:

- Vermeidung unbefugter Zutritte
- Verhinderung des unbefugten Zugangs
- Verhinderung des unbefugten Zugriffs auf sensible Daten und Systeme
- verschlüsselter externer Transport der Daten

Integrität

beinhaltet den Schutz vor unerlaubter Veränderung oder Verfälschung/Manipulierung von Informationen. Dies betrifft die Daten, die im internen IT- Informationsverbund gespeichert sind und die Daten, die über das Internet übertragen werden. Sofern unautorisierte Veränderungen erfolgen, sind diese feststellbar. Auch die Konfiguration von Diensten und Systemen darf nicht unautorisiert verändert werden.

Authentizität

die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden. Der Begriff wird nicht nur verwendet, wenn die Identität von Personen geprüft wird, sondern auch bei IT-Komponenten oder Anwendungen.

Patientensicherheit

Patientensicherheit ist das Produkt aller Maßnahmen der medizinischen Versorgung, die darauf gerichtet sind, Patienten vor vermeidbaren Schäden in Zusammenhang mit der Diagnose und Heilbehandlung zu bewahren. Unter „Patientensicherheit“ versteht man daher, das Vermeiden, die Verhütung und Verbesserung von unerwünschten Ergebnissen oder Schäden durch Gesundheitsversorgungsmaßnahmen.

Behandlungseffektivität

Die Sicherstellung und Aufrechterhaltung der Effektivität bzw. Wirksamkeit einer Gesundheitsmaßnahme.

7 Sicherstellung der Schutzziele

Unsere Daten und unsere IT-Systeme und die dazugehörige IT-Infrastruktur werden in allen medizinischen, medizintechnischen und kaufmännischen Bereichen in ihrer Verfügbarkeit so gesichert, dass die zu erwartenden Stillstands-Zeiten toleriert werden können. Der kontinuierliche Verbesserungsprozess stellt deshalb sicher, dass auftretende Vorfälle und daraus folgende Probleme ausgewertet und entsprechende Verbesserungen zur Einhaltung vereinbarter Service Level umgesetzt werden können.

Zur Vermeidung von Fehlfunktionen und Unregelmäßigkeiten in Daten und IT-Systemen (Integritätsschutz) werden sowohl informationstechnische – logische Sicherheitsmechanismen als auch physische und organisatorische Sicherheitsmaßnahmen eingesetzt. Die generellen Anforderungen an Vertraulichkeit und Authentizität haben ebenfalls ein hohes, an Gesetzeskonformität orientiertes Niveau. Für die Daten, die über das Internet übertragen werden, gelten entsprechende höhere Anforderungen an die Vertraulichkeit, Authentizität und Integrität d. h. z.B. die Daten müssen während der Übertragung in geeigneter Weise geschützt werden.

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme ist eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt. Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Schutzprogramme insbesondere zum Schutz vor Schadprogrammen werden auf entsprechenden IT-Systemen eingesetzt. Alle Internetzugänge werden durch ein geeignetes Firewall-Konzept redundant gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer durch eine sicherheitsbewusste Arbeitsweise diese Sicherheitsmaßnahmen und informieren bei Auffälligkeiten die entsprechend festgelegten Meldestellen.

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.

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 Notfallhandbuch 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, wird von dem IT-Dienstleister das gleiche Sicherheitsniveau erwartet. Dies wird dann in entsprechenden Service Level Agreements (SLA) vorgegeben und in Verträgen dokumentiert. Das Recht auf Kontrolle wird festgelegt. Für umfangreiche oder komplexe Outsourcing-Vorhaben hat die SKMG ein detailliertes Sicherheitskonzept Outsourcing mit konkreten Maßnahmenvorgaben erstellt.

Alle Anwender und Mitarbeiter werden zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen sensibilisiert. Mitarbeiter und Auftragnehmer müssen ihre technischen, personellen, aber auch organisatorischen Verantwortlichkeiten in Bezug auf Informationssicherheit annehmen, verstehen und bei ihren Tätigkeiten berücksichtigen. Die Mitarbeiter der medizinischen Fachabteilungen haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des ISB zu halten und müssen im eigenen Verantwortungsbereich entsprechende sicherheitstechnische und sicherheitsorganisatorische Maßnahmen umsetzen, sowie zum Erhalt und Verbesserung der Informationssicherheit und Versorgungsicherheit der medizinischen Dienstleistungen beitragen.

Zur effizienten Erreichung der o.g. Zielsetzungen werden u.a. auch präventive Sicherheitsmaßnahmen (vorbeugende Maßnahmen), detektierende Maßnahmen (Früherkennungssysteme) und reaktive Maßnahmen (Wiederherstellungsverfahren) eingesetzt.

8 Kontinuierliche Verbesserung

Die Geschäftsführung bildet für die Belange der Informationssicherheit die oberste Instanz und wird stetig in allen Informationssicherheitsprozessen insbesondere Hervorhebung und Bekanntmachung der Informationssicherheitsleitlinie, Risikomanagement mit Risikobetrachtung, Risikobewertung und somit Risikobehandlung vollständig integriert.

Die Geschäftsführung wird in Zügen der IS-Prozessen vollständig und ausführlich über das Vorhaben, Projektergebnisse sowie die identifizierten Risiken und daraus entwickelten Risikomaßnahmen informiert. Als oberste Instanz trägt die Geschäftsführung die Verantwortung für die Umsetzung der Risikomaßnahmen, durch die Risiken minimiert oder beseitigt werden. Verbleibende nicht vollständig reduzierbare Risiken werden akzeptiert. Hierbei werden die erforderlichen Ressourcen zur effektiven Erreichung und Aufrechterhaltung der Informationssicherheitsziele den Fachkräften, Entscheidungsträger zur Verfügung gestellt. Im Rahmen eines sich ständig wiederholenden PDCA-Zyklus werden die IS-Prozesse kontinuierlich verbessert.

Zu den kontinuierlichen Verbesserungsprozessen gehören:

- angesetztes prozessuales Reviewverfahren zur Überprüfung der Konformität - jährlich
- angesetztes dokumentarisches Reviewverfahren zur dynamischen Optimierung der IS-Dokumente - jährlich?
- jährlich angesetztes Risikomanagementverfahren zur dynamischen Identifizierung und Bewertung der Sicherheitslage, Risiken und Chancen,
- jährlich angesetzten Schulungen (Online- / oder Präsenzschulungen zur IS),
- jährlich angesetztes Internes Audit zur Wirksamkeitsprüfung und
- jährlich angesetzte externe Überwachungsprüfungen sowie externe Konformitätsüberprüfungen sowie
- fachliche Überprüfung und Ursachenanalyse hinsichtlich des Umgangs mit den Nichtkonformitäten.