Ausgedruckt ist die Aktualitᵃ t nicht sichergestellt!

Inhalt

1 Geltungsbereich 2
2 Ziel und Zweck 2
3 Abkürzungen und Definitionen 2
4 Beschreibung 2
4.1 Bedeutung der Informationssicherheit und des Datenschutzes 2
4.2 Informationssicherheitsgrundsätze 3
5 Mitgeltende Dokumente 4
6 Inkrafttreten 4

Ausgedruckt ist die Aktualitᵃ t nicht sichergestellt!

1 Geltungsbereich

Kliniken Maria Hilf GmbH

Die vorliegende Informationssicherheitsleitlinie gilt für alle Hersteller, Dienstleister und externe Mitarbeiter, die für die Kliniken Maria Hilf GmbH tätig sind und die in Verarbeitungsprozesse personenbezogener Daten und in den Geschäftsprozessen zum Einsatz und zur Nutzung von vernetzten und nicht vernetzten Geräten, Betriebs- u. Anwendungssystemen und deren Komponenten involviert sind, soweit diese für die Erbringung kritischer Dienstleistungen (kDL) notwendig sind.

2 Ziel und Zweck

Mit der Leitlinie legt die Geschäftsführung die verbindlichen Vorgaben und Ziele zur laufenden Überwachung und Verbesserung der Informationssicherheit und des Datenschutzes in der Kliniken Maria Hilf GmbH fest. Mit dieser „Leitlinie zur Informationssicherheit und zum Datenschutz für Dienstleister und Dritte" wird jedem Dienstleister ein Grundverständnis und ein Sicherheitsbewusstsein für Informationssicherheit und Datenschutz vermittelt. Ziel ist es, dass jeder Dienstleister aktiv an der kontinuierlichen Verbesserung des Informationssicherheits- u. Datenschutzniveaus mitwirkt.

3 Abkürzungen und Definitionen

Abkürzung	Erläuterung
ISDS-Team	Kernteam für Informationssicherheit u. Datenschutz der Kliniken Maria Hilf GmbH
ISMS	Informationssicherheitsmanagementsystem
KDG	Gesetz über den kirchlichen Datenschutz
KDG-DVO	Durchführungsverordnung zum Gesetz über den kirchlichen Datenschutz
kDL	Kritische Dienstleistung

4 Beschreibung

4.1 Bedeutung der Informationssicherheit und des Datenschutzes

Moderne Patientenversorgung erfordert zunehmend den Einsatz stets aktueller Informationstechnologien, um die Aufgabenerfüllung der Kliniken Maria Hilf GmbH im Sinne der Patienten und weiterer Partner sicher, effizient und effektiv zu gestalten. Patienteninformationen, technische Daten und andere Assets sind Ressourcen, deren Schutz für die Aufgabenerfüllung und das Ansehen der Kliniken Maria Hilf GmbH maßgeblich sind. Aufgaben, Prozesse und die Aufbauorganisation unterliegen einem stetigen Wandel und einer Anpassung der technischen Möglichkeiten. In Abwägung der zu schützenden Werte, der gesetzlichen Anforderungen und der damit verbundenen Risiken wird ein angemessenes Informationssicherheitsniveau geschaffen. Beim Umgang mit Informationen aller Art wird in der Kliniken Maria Hilf GmbH darauf geachtet, dass dem Schutzbedarf entsprechend Rechnung getragen wird. Die Informationssicherheit beinhaltet den Datenschutz und die IT-Sicherheit.

Zur Wahrung der Informationssicherheit dienen die folgenden Schutzziele:

- **Vertraulichkeit**

  Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen ohne gesetzliche oder vertragliche Grundlage oder Erlaubnis des Eigentümers der Informationen.

- **Integrität**

  Integrität bedeutet Schutz vor Änderungen von Informationen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.

Ausgedruckt ist die Aktualitᵃ t nicht sichergestellt!

- **Authentizität**

  Authentizität bedeutet, dass die Informationen von Demjenigen stammen, von dem sie zu stammen vorgeben.

- **Verfügbarkeit**

  Verfügbarkeit bedeutet, dass Prozesse, Informationen, Funktionen und Informationssysteme immer dann verfügbar sind, wenn ein autorisierter Benutzer sie bearbeiten bzw. in Anspruch nehmen will. „Verfügbar" heißt in diesem Zusammenhang auch, dass der Zugriff auf Informationen, Funktionen und Betriebsmittel bedarfsgerecht gewährleistet ist.

- **Patientensicherheit**

  Patientensicherheit wird definiert als die Freiheit von unvertretbaren Risiken einer physischen Verletzung oder eines Schadens an der Gesundheit von Menschen. Dies schließt auch die Vermeidung einer nachhaltigen psychischen Belastung ein.

- **Behandlungseffektivität**

  Behandlungseffektivität stellt das zielgerichtete Zusammenwirken der beteiligten Prozesse und Informationen zur medizinischen Behandlung des Patienten, ggf. auf Basis eines Informationsaustausches zwischen unterschiedlichen verantwortlichen Organisationseinheiten, sicher.

4.2 Informationssicherheitsgrundsätze

Für den Betrieb des Informationssicherheits-Managementsystems gelten folgende Grundsätze:

1. Für Unternehmenswerte wie Informationen, IT-Systeme und IT-Anwendungen sind Eigentümer benannt, die für die Sicherheit der jeweiligen Unternehmenswerte verantwortlich sind.
2. Risiken aus der Nutzung der Informationen und Informationssysteme werden frühzeitig identifiziert und auf ein akzeptiertes Restrisiko minimiert. Hierzu betreiben die Kliniken Maria Hilf GmbH ein IS-Risikomanagement.
3. Kosten und Nutzen von Sicherheitsmaßnahmen stehen in einem angemessenen Verhältnis, ggf. werden Maßnahmen über einen längeren Zeitraum umgesetzt.
4. Vorgaben und Maßnahmen orientieren sich an anerkannten Standards und Best Practices zur Informationssicherheit. Systeme und Komponenten werden gemäß den Erkenntnissen aus dem IS-Risikomanagement der Kliniken Maria Hilf GmbH behandelt.
5. Gesetzliche, vertragliche und sonstige Vorgaben für die Informationssicherheit werden identifiziert und durch angemessene Maßnahmen umgesetzt. Die Umsetzung und Berücksichtigung erfolgt in den entsprechenden Fachbereichen der Kliniken Maria Hilf GmbH.
6. Zugriff, Zugang (Benutzerverwaltung mit unterschiedlichen Rollen und Rechten) und Zutritt (Schließsysteme, Zutrittskontrollsysteme, …) zu den Informationswerten sind auf das notwendige Maß beschränkt.
7. Alle wesentlichen Aktivitäten und Ereignisse im Bereich der Informationssicherheit müssen transparent und im erforderlichen Umfang nachvollziehbar sein. Zur Dokumentation und Beschreibung wurden die Leitlinien (intern und extern) sowie Richtlinien und Sicherheitskonzepte ausgearbeitet. In Abhängigkeit vom Umfang und der Art und Weise der Aufgabenerfüllung durch den Auftragnehmer kann es erforderlich sein, dass dieser die entsprechenden Richtlinien und Sicherheitskonzepte beachten muss. Dies ist bei Bedarf und im Zweifel mit dem ISDS-Team der Kliniken Maria Hilf GmbH abzustimmen.
8. Verfahren für den Betrieb bzw. die Wiederherstellung des Betriebs der wesentlichen Informationssysteme wurden dokumentiert.
9. Für die an der Verarbeitung von Informationen beteiligten Beschäftigten sowie Auftragnehmern werden angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen.

Ausgedruckt ist die Aktualitᵃt nicht sichergestellt!

10. Die Beschäftigten werden hinsichtlich des sicheren Umgangs mit Informationswerten informiert, geschult und sensibilisiert. Sie sind angehalten, die entsprechenden Vorgaben umzusetzen. Entsprechendes gilt, falls erforderlich, auch für Auftragnehmer.
11. Die Wirksamkeit der Vorgaben und Maßnahmen zur Informationssicherheit werden kontinuierlich überprüft und verbessert. Zur Überprüfung werden die verschiedenen Audits gemäß dem ISMS-Auditprogramm der Kliniken Maria Hilf GmbH durchgeführt und entsprechend dokumentiert.

5 Mitgeltende Dokumente

- Anweisung zu Arbeits-, Brand-, Datenschutz und IT-Sicherheitsbestimmungen/-hinweise für Fremdfirmen
- B3S „Medizinische Versorgung"
- KDG
- KDG-DVO
- Verpflichtungserklärung Datengeheimnis für Externe
- Verschwiegenheitserklärung für Mitarbeitende für Lieferanten/Dienstleister
- Zusatzvereinbarung zur Gewährleistung der Informationssicherheit in den Kliniken Maria Hilf

6 Inkrafttreten

Durch die Freigabe dieser Informationssicherheitsleitlinie für Hersteller, Dienstleister und externe Mitarbeiter durch die Geschäftsführung der Kliniken Maria Hilf GmbH ist diese ab sofort gültig und in allen enthaltenden Punkten ausnahmslos anzuwenden.

Verteilung:

Einstellen auf die Homepage der Kliniken Maria Hilf GmbH.

Den Dienstleistern und Dritten ist durch die jeweiligen Auftraggeber die Leitlinie nachweislich bekannt zu geben.