Weisung

Informationssicherheit IT-Mitarbeitende

Informatik / Geschäftsleitung

■ Dokumenteigenschaften

Änderungsdatum	24.06.2025
Gültig ab	Freigabe
Version	1.01
Ersetzt Version	1.00 vom 01.12.2021
Verfasst durch	Thomas Huber, Othmar Wyss, Daniel Michel (Redguard)
Freigegeben durch	Geschäftsleitung xx.xx.xxxx
Prozessverantwortlich	Information Security Officer

■ Dokumentenverlauf

Änderungsdatum	Version	Bearbeiter	Änderungen
0.10	10.12.2020	IT	Initialversion
0.20	12.02.2020	Othmar Wyss	Überarbeitung nach Review Spitäler fmi AG
0.30	03.06.2021	Thomas Huber, O. Wyss	Überarbeitung nach Review Spitäler fmi AG
0.40	06.08.2021	Th. Huber, O. Wyss	Überarbeitung nach Abstimmung mit Spitäler fmi AG
0.45	28.09.2021	IT	Review durch Redguard
0.50	21.10.2021	Othmar Wyss	Review / Abstimmung
0.70	01.11.2021	IT	Überarbeitung (Integration best. Weisung «Nutzung IT, Telekom)
0.80	17.11.2021	IT	Überarbeitung nach Feedback O. Wyss
1.00	01.12.2021	IT	Version zur Freigabe
1.01	24.06.2025	Marco Filli	Überarbeitung und Review
1.02	19.11.2025	Marco Filli	Anpassungen nach Feedback durch Geschäftsleitungssitzung vom 27.10.2025

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel und Zweck

Die Richtlinie zur Informationssicherheit definiert die Mindestanforderungen an die Informationssicherheit der Spitäler fmi AG und übersetzt die Zielsetzung des Informationssicherheitskonzeptes in konkrete und messbare Informationssicherheitsanforderungen. Das Ziel der vorliegenden Richtlinie ist es, ein angemessenes Sicherheitsniveau über die gesamte Organisation hinweg aufzubauen und aufrechtzuerhalten.
Diese Mindestanforderungen orientieren sich an der internationalen Informationssicherheitsnorm ISO/IEC 27001. Weiter werden die Vorgaben aus der Gesetzgebung des Datenschutzes sowie zum elektronischen Patientendossier berücksichtigt

1.2 Geltungsbereich

Die vorliegende Richtlinie richtet sich an die Abteilung Informatik und Digitalisierung.
Die Weisung über die Nutzung der Informatik- und Telekommunikationsmittel gilt auch für IT Mitarbeitende der Abteilung Informatik

1.3 Änderungen

Änderungsanträge werden durch den Leiter Informatik und den Informationssicherheitsbeauftragten beurteilt und umgesetzt.

1.4 Kontrolle

Die Überprüfung der Richtlinie auf Zweckmässigkeit und Aktualität ist jährlich durch den Informationssicherheitsbeauftragten sicherzustellen und im Dokumentenverlauf zu dokumentieren.

1.5 Ersatz von Dokumenten

Das vorliegende Dokument ersetzt folgende Dokumente:

- Weisung über die Nutzung der Informatik- und Telekommunikationsmittel, Version 2

1.6 Inkrafttreten

Die vorliegende Richtlinie wird nach Abnahme durch die Geschäftsleitung in Kraft gesetzt.

1.7 Referenzierte und mitgeltende Dokumente

Name des Dokuments
Konzept Informationssicherheit
Weisung über die Nutzung der Informatik- und Telekommunikationsmittel
Weisung Datenschutz
Handbuch Informationssicherheit und Datenschutz
Geheimhaltungsvereinbarung für Externe
Richtlinie Projektmanagement
Konzept Entsorgung Spitäler fmi AG
Notfall Checkliste – im nicht Öffentlichen Sharepoint Bereich (Kontaktdaten)
Bewertung Kritikalität Security-Incident

2 Organisation

2.1 Verantwortlichkeiten

Die grundlegende Informationssicherheitsorganisation ist im Informationssicherheitskonzept definiert. Die Informatik arbeitet im Rahmen der Umsetzung von Massnahmen eng mit der Informationssicherheitsorganisation zusammen.
Weitere Verantwortlichkeiten sind in der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel definiert.

2.2 Management von Informationssicherheitsvorfällen

2.2.1 Identifikation und Klassifikation von Sicherheitsvorfällen

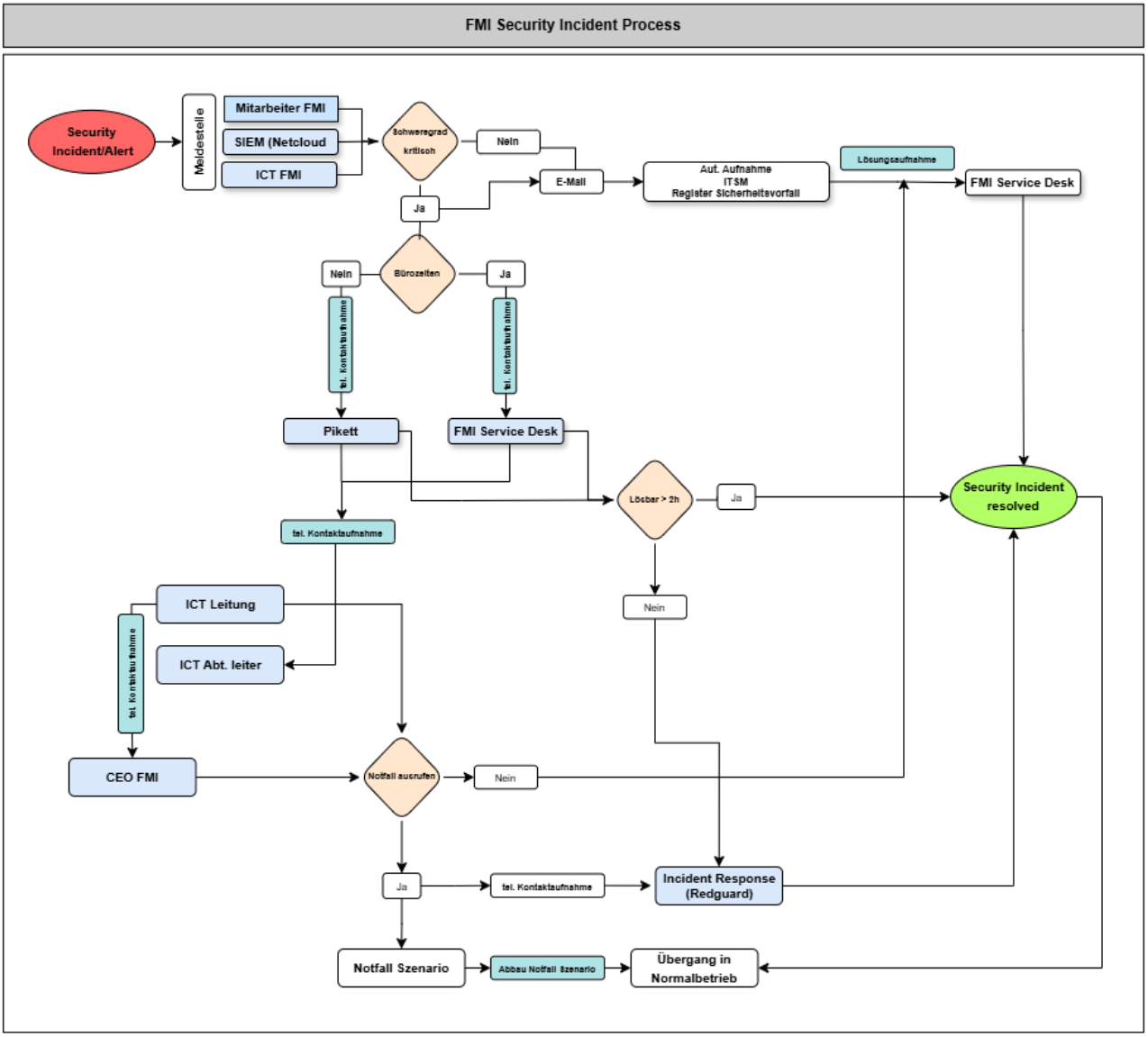
Erkannte oder vermutete bzw. gemeldete Sicherheitsvorfälle sind entsprechend ihrer Auswirkungen und Dringlichkeit zu behandeln.
Die Priorisierung und Bewertung von Vorfällen im Bereich der Informationssicherheit wird anhand Kapitel 2.2.4 vorgenommen, zur Priorisierung kann das Hilfsmittel Bewertung Kritikalität Security Incident genutzt werden.
Für die Einstufung der Dringlichkeit eines Vorfalls werden folgende Stufen unterschieden:

Stufe	Einstufungskriterien
Stufe 1: Schwerwiegender Sicherheitsvorfall	▪ Datenabfluss von oder Zugriff durch Unberechtigte auf besonders schützenswerten Daten ▪ Beeinträchtigung des Zugriffs auf alle Daten ▪ Beeinträchtigung des Betriebs aller betriebsrelevanten Systeme ▪ Personenschaden (z.B. Patienten)
Stufe 2: Mittelschwerer Sicherheitsvorfall	▪ Datenabfluss von und Zugriff durch Unberechtigte auf nicht besonders schützenswerten Daten ▪ Beeinträchtigung des Zugriffs auf geschäftskritische Daten (Kernprozess ist betroffen) ▪ Beeinträchtigung des Betriebs mehrerer Systeme
Stufe 3: Normaler Sicherheitsvorfall	▪ Zugriff durch Unberechtigte auf nicht besonders schützenswerte Daten ohne Datenabfluss ▪ Beeinträchtigung des Zugriffs auf vereinzelte Datensammlungen ▪ Beeinträchtigung des Betriebs einzelner Systeme
Stufe 4: Geringer Sicherheitsvorfall	▪ Zugriff durch Unberechtigte auf Systeme und ohne Zugriff auf Daten ▪ Beeinträchtigung des Zugriffs auf vereinzelte Datensätze ▪ Beeinträchtigung des Betriebs eines einzelnen nicht betriebsrelevanten Systems

2.2.2 Meldung von Sicherheitsvorfällen

Informationssicherheitsvorfälle oder Feststellungen die zu einem Sicherheitsvorfall führen können, werden gemäss der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel an den Service Desk gemeldet. Gemeldete oder selbst festgestellte (potenzielle) Vorfälle werden durch den Service Desk als Incident im Ticketing System erfasst und als Security Incident gekennzeichnet.
Nach Bekanntwerden eines grösseren Sicherheitsvorfalls (Stufe 1 und Stufe 2) oder nach Feststellung von Risiken und Schwachstellen, die zu einem Sicherheitsvorfall Stufe 1 oder Stufe 2 führen können, ist der Informationssicherheitsverantwortliche beziehungsweise der Informationssicherheitsbeauftragte umgehend zu informieren. Dieser beurteilt den Vorfall und definiert das weitere Vorgehen.

Im Zweifelsfall ist ein Vorfall als Sicherheitsvorfall der Stufe 1 zu behandeln und mit entsprechender Priorität zu behandeln. Die Stufe kann im späteren Verlauf der Behandlung angepasst werden.



2.2.3 Information und Kommunikation

Die Kommunikation bezüglich Informationssicherheitsvorfällen gegenüber internen als auch externen Personen und Anspruchsgruppen erfolgt gemäss der in der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel definierten Verantwortlichkeiten.

2.2.4 Priorisierung und Behandlung von Vorfällen

Zur Priorisierung kann das Hilfsmittel Bewertung Kritikalität Security Incident aufgefüllt werden.

Stufe	Beschreibung
Stufe 1:	Die Informationssicherheitsverantwortliche Stelle sowie die IT-Leitung ist unverzüglich zu kontaktieren. Sind dieser nicht erreichbar, so sind die entsprechenden Stellvertreter zu informieren, siehe dazu die Organisation IT-Krisenstab in der Notfall Checkliste. Für den Vorfall ist ein Security Incident zu erfassen. Der Security Incident wird sofort bearbeitet. Die Behandlung des Vorfalls erfolgt gemäss der Notfall Checkliste.
Stufe 2:	Die Informationssicherheitsverantwortliche Stelle sowie die IT-Leitung ist unverzüglich zu kontaktieren. Sind dieser nicht erreichbar, so sind die entsprechenden Stellvertreter zu informieren, siehe dazu die Organisation IT-Krisenstab in der Notfall Checkliste. Für den Vorfall ist ein Security Incident zu erfassen. Der Security Incident wird sofort bearbeitet. Die Behandlung des Vorfalls erfolgt gemäss der Notfall Checkliste.
Stufe 3:	Für den Vorfall ist ein Security Incident zu erfassen. Der Security Incident wird innerhalb von 48 Stunden bearbeitet.
Stufe 4:	Für den Vorfall ist ein Security Incident zu erfassen. Der Security Incident wird innerhalb von 72 Stunden bearbeitet.

2.2.5 Dokumentation und Protokollierung

Die Behandlung eines Sicherheitsvorfalls ist zu dokumentieren. Insbesondere schriftlich festzuhalten sind.

Dokumentation	Beschreibung
Meldung	▪ Die Meldung soll mindestens folgende Angaben enthalten: ▪ Angaben gemäss Ticketingsystem wie Nr., Datum, Titel, etc. ▪ Angaben der meldenden Person ▪ Zeitpunkt der Erkennung sowie der Meldung (Datum und Uhrzeit) ▪ Art und Beschreibung des Sicherheitsvorfalls ▪ Betroffene Daten und Systeme ▪ Einschätzung potenzieller Folgen (z.B. Ausbreitung auf weitere Systeme, erhöhte Risiken für betroffene Personen) ▪ Getroffene Sofortmassnahmen ▪ Weitere relevante Angaben zum Vorfall
Beurteilung und Priorisierung	Die Beurteilung eines Sicherheitsvorfalls sowie der Entscheid der Priorisierung inkl. Begründung sind schriftlich zu dokumentieren.
Massnahmen und Behandlungsstatus	Massnahmen, die im Verlauf der Vorfallbehandlung definiert und umgesetzt werden, sind zusammen mit dem jeweiligen Behandlungsstatus zu dokumentieren.

Neue Erkenntnisse zum Vorfall, umgesetzte Massnahmen sowie erreichte Meilensteine sind laufend zu protokollieren. Die Nachvollziehbarkeit während der ganzen Behandlung eines Sicherheitsvorfalls ist zu gewährleisten.

2.2.6 Sicherstellung von Beweisen

Da ein Sicherheitsvorfall rechtliche Schritte zur Folge haben kann, beispielsweise bei einem Verstoss gegen das Datenschutzgesetz, sind allfällige Beweise zu sichern. Dabei ist darauf zu achten, dass die eigene Strafbarkeit vermieden wird (z.B. bei Screenshots von illegalen Inhalten).
Physische Dokumente sind zusammen mit der Dokumentation des Vorfalls im Original und für Unberechtigte unzugänglich zu verwahren. Zudem sind Massnahmen zu treffen, dass die Integrität von Originalen sichergestellt und nachgewiesen werden kann.

Digitale Daten sowie IT-Mittel, die im Zusammenhang stehen mit einem Informationssicherheitsvorfall, sind für Unberechtigte unzugänglich aufzubewahren. Für digitale Daten sind Kopien anzulegen, der Kopiervorgang ist zu protokollieren und darf nur im 4-Augen-Prinzip erfolgen. Forensische Tätigkeiten sind auf die erstellten Kopien zu beschränken, um die Integrität von Originalen zu gewährleisten.

2.2.7 Nachbearbeitung von Sicherheitsvorfällen

Ist die Behandlung eines Sicherheitsvorfalls abgeschlossen, sind Erkenntnisse zur Behandlung festzuhalten und im Sinne der kontinuierlichen Verbesserung in die vorliegende Richtlinie sowie in die relevanten Prozesse einfliessen zu lassen.
Weiter sind Sicherheitsvorfälle mindestens nach Abschluss der Behandlung im Risikomanagement zu berücksichtigen, um sicherzustellen, dass durch Vorfälle aufgedeckte Risiken weiter behandelt werden.

2.2.8 Kontinuitäts- und Notfallplanung

Für alle geschäftskritischen Applikationen muss eine Kontinuitäts- und Notfallplanung erstellt und dokumentiert sein.

2.3 Informationssicherheit in Projekten

2.3.1 Projektmanagement Prozess

Informatikprojekte werden in vier Phasen (Initialisierung, Konzept, Realisierung und Einführung, Abschluss) umgesetzt. Das Thema Informationssicherheit wird bereits in der Initialisierungsphase adressiert, gegebenenfalls ist der Informationssicherheitsbeauftragte beizuziehen. Nachfolgende Kapitel dienen als Leitfaden, um in den jeweiligen Phasen die Vorgaben bezüglich Informationssicherheit zu erfüllen.

2.3.2 Phase Initialisierung

2.3.2.1 Identifizierung des Schutzbedarfs

Für Systeme und Anwendungen muss bei der Projektinitialisierung eine Schutzbedarfsanalyse durchgeführt werden. Die Systeme und Anwendungen sind im dafür vorgesehenen System zu dokumentieren. Im Rahmen der Projektinitialisierung ist die Projektleitung für die Durchführung der Identifizierung des Schutzbedarfs verantwortlich. Der Informationssicherheitsbeauftragte unterstützt die Projektleitung bei Bedarf bei der Durchführung der Schutzbedarfsanalyse. Die Analyse ist spätestens nach der erfolgten Durchführung beim Informationssicherheitsverantwortlichen oder Informationssicherheitsbeauftragten zur Prüfung einzureichen. Abhängig vom Resultat der Schutzbedarfsanalyse sind zusätzliche Anforderungen zu berücksichtigen. Im Kontext von Personendaten beispielsweise eine Vorabkontrolle durch die Datenschutzaufsicht des Kantons gemäss Art 17a des Kantonalen Datenschutzgesetzes.

2.3.2.2 Definition von Sicherheitsanforderungen

Bei der Erarbeitung der Anforderungen sind die Vorgaben der vorliegenden Richtlinie sowie der Richtlinie Informationssicherheit MA zu berücksichtigen.
Die identifizierten Anforderungen bezüglich Informationssicherheit werden in einem Grobkonzept erfasst. Dieses wird in der nächsten Projektphase (Konzept) benötigt.

2.3.3 Phase Konzept

Die formulierten Anforderungen aus dem Grobkonzept werden in der Phase Konzept detaillierter in einem Feinkonzept dokumentiert. Der Projektleiter ist dafür verantwortlich, dass die sicherheitsrelevanten Anforderungen in diesen Dokumenten abgedeckt sind. Offene Punkte bezüglich Informationssicherheit sind in einer Pendenzenliste zu führen.

2.3.4 Phase Realisierung und Einführung

Alle im Feinkonzept definierten Sicherheitsanforderungen müssen bei der Realisierung und Einführung eines Systems oder einer Anwendung berücksichtigt werden. Sicherheitsrelevante Punkte aus der Pendenzenliste werden in dieser Phase bearbeitet. Zusätzlich kann eine technische Sicherheitsprüfung des eingeführten Systems oder der Anwendung durchgeführt werden.

2.3.5 Phase Abschluss

Erkenntnisse aus dem Projekt sind zentral festzuhalten. Des Weiteren sind folgende Punkte nach Abschluss des Projektes in Bezug auf die Informationssicherheit zu prüfen:

- Die Einstufung des Schutzbedarfs entspricht dem aktuellen Stand.
- Die für das System oder die Anwendung verantwortliche Person ist im Verzeichnis aufgeführt.
- Alle sicherheitsrelevanten Punkte in der Pendenzenliste sind geschlossen.
- Eine technische Überprüfung auf Schwachstellen hat stattgefunden (optional).

3 Daten

3.1 Schutzbedarfsanalyse

Für sämtliche Systeme und Anwendungen muss eine Schutzbedarfsanalyse durch den Business Owner oder den Projektleiter durchgeführt werden. Die Schutzbedarfsanalyse orientiert sich an den im Informationssicherheitskonzept festgehaltenen Informationssicherheitsaspekten.

Informationssicherheitsaspekt	Kriterien
Vertraulichkeit	Personendaten: 1. Keine Personendaten 2. Personendaten 3. besonders schützenswerte Personendaten Klassifizierung (gem. Kapitel 2.2): 1. Nicht klassifiziert 2. Intern 3. Vertraulich
Verfügbarkeit	Servicezeiten: 1. Standard (08:00 - 12:00 und 13:30 - 17:00) 2. Erhöht (spezifische SLA) 3. Hoch (7x24h)
Integrität	Anforderungen: 1. Keine speziellen Anforderungen 2. Spezielle Anforderungen

Für die Durchführung der Schutzbedarfsanalyse kann die entsprechende Vorlage verwendet werden.

3.2 Nutzung von Personendaten

Bei vorgelagerten und nicht produktiven Umgebungen (z.B. Entwicklung, Test, Schulung, Integration) dürfen zu keinem Zeitpunkt Daten aus einer produktiven Umgebung ohne vorgenommene Anonymisierung verwendet werden. Die Anonymisierung hat so zu erfolgen, dass keine Rückschlüsse auf die ursprüngliche Person mehr möglich sind. Falls keine oder keine genügende Anonymisierung möglich ist, muss auf den nicht produktiven Umgebungen derselbe Schutzbedarf gewährleistet werden wie bei den produktiven Systemen. Werden in Test- und Entwicklungssystemen Echtdaten mit persönlichen oder anderen sensitiven Informationen verwendet, ist die Bewilligung des Business Owners und des Datenschutzverantwortlichen einzuholen.

4 Systeme

4.1 Verwaltung von IT-Mitteln

Die Verwaltung sämtlicher IT-Mittel der Spitäler fmi AG liegt in der Verantwortung der Informatik und erfolgt über die Systemverwaltungs-Applikation.
Werden IT-Mittel von Spitäler fmi AG vergeben, sind die Herausgabe sowie die Rücknahme zu dokumentieren.
Die Liste der vergebenen IT-Mittel ist bei Änderungen zu aktualisieren und mindestens jährlich zu überprüfen.
Datenträger (z.B. CD-ROMs, DVD, USB-Sticks, Tapes, Festplatten, etc.) und Geräte, welche nicht im Einsatz sind, aber potenziell schützenswerte Daten enthalten, müssen so aufbewahrt werden, dass unberechtigte Personen keinen Zugriff darauf haben.
Datenträger, welche Daten von Spitäler fmi AG enthalten oder zwischenspeichern, sind zudem so zu entsorgen, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind. Das sichere Löschen und Entsorgen von nicht mehr benutzten Datenträgern hat gemäss dem Entsorgungskonzept der Spitäler fmi AG zu erfolgen.
Hardware, welche Daten von Spitäler fmi AG bearbeitet und Speichermedien beinhaltet, ist vor der Entsorgung oder Wiederverwendung auf das Vorhandensein von Daten zu prüfen. Daten von Spitäler fmi AG sind zu entfernen oder sicher zu überschreiben. Für Geräte, welche durch Dritte bereinigt werden, ist eine Bescheinigung über die Bereinigung zu verlangen.

4.2 Endgeräteschutz

Für Endgeräte der Mitarbeitenden werden adäquate Schutzmassnahmen geplant und umgesetzt. Die Vorgaben gelten auch für Geräte, welche für den Fernzugriff eingesetzt werden.

4.2.1 Konfiguration von Endgeräten

Für die Mitarbeitenden sowie für die Administratoren sind persönliche Benutzerkonten einzurichten. Gast-Benutzer auf Geräten sind, wo möglich, zu deaktivieren.
Die Standardkonfiguration sowie Sicherheitseinstellungen auf Endgeräten sind so zu schützen, dass diese weder absichtlich noch unbeabsichtigt durch Mitarbeitende verändert oder deaktiviert werden können. Dies gilt auch für die Einstellungen von Virenschutzprogrammen.
Bei der Erstinstallation von Systemen müssen die vordefinierten Benutzerkonten, Initialpasswörter oder Zugriffsrechte kontrolliert und, sofern sie nicht benötigt werden, gelöscht oder angepasst werden.
Die Möglichkeiten zur Installation von nicht freigegebener Software sind auf Endgeräten von Mitarbeitenden soweit möglich technisch einzuschränken.

4.3 Schutz vor Schadsoftware

Alle Clients und Server-Systeme werden mit einem aktivierten Virenschutzprogramm ausgestattet. Die Signaturen der Virenschutzprogramme werden mindestens täglich aktualisiert. Jeglicher virenanfällige Datenverkehr muss über das Virenschutzprogramm laufen (E-Mail, Internet, USB-Stick, CD/DVD-Rom, mobile Lösungen usw.). Die Autorun-Funktion beim Anschluss von externen Datenträgern ist bei allen Betriebssystemen (Arbeitsplatzsysteme und Server) zu deaktivieren. Mindestens einmal pro Monat sind zudem sämtliche lokalen Datenträger der Systeme vollständig auf Schadsoftware zu prüfen. Die Prüfung soll so durchgeführt werden, dass die betrieblichen Abläufe nicht wesentlich beeinflusst werden.

4.4 Patch Management

Sicherheitsrelevante Aktualisierungen (Patches) des Betriebssystems oder installierter Zusatzsoftware werden mindestens monatlich vorgenommen. Die Aktualisierungen müssen zeitlich so geplant werden, dass betriebliche Abläufe bei Aktualisierungen möglichst nicht beeinflusst werden.

4.5 Change-Management

Im Rahmen des Change-Managements sind die sicherheitstechnischen und geschäftskritischen Funktionalitäten zu überprüfen und gegebenenfalls anzupassen.
Die Nachvollziehbarkeit von Änderungen muss gewährleistet sein.

4.6 Lebenszyklus von Systemen

Die Informationssicherheit ist über den gesamten Lebenszyklus von Systemen sicherzustellen. Dies betrifft sowohl die Entwicklung und Einführung, als auch die Änderung sowie Ablösung eines Systems.
Bei der Einführung eines Systems im Rahmen eines Projektes gelten die Vorgaben zum Projektmanagement gemäss Kapitel 2.3. Für die Ablösung oder Entsorgung von Systemen sind zudem die Vorgaben aus Kapitel 4.1 **Fehler! Verweisquelle konnte nicht gefunden werden.** zu berücksichtigen.
Für produktive Systeme sind Wartungsverträge mit Lieferanten abzuschliessen. Wird erkannt, dass der Lebenszyklus überschritten wird oder eine Versorgungslücke besteht, dann muss dies als Risiko aufgenommen werden.

4.7 Backups

Die Wiederherstellung und -verwendbarkeit von Daten nach einem Datenverlust sind sicherzustellen. Die Wiederherstellung ist regelmässig zu proben. Die Datensicherung muss getrennt von den produktiven Ablagen aufbewahrt werden. Schreib- und Lösch- Zugriffe auf Datensicherungen sind so restriktiv wie möglich zu halten.

4.8 Überwachung der Verfügbarkeit von Diensten

Kritische Systemkomponenten, wie zum Beispiel der noch verfügbare Speicherplatz eines Datenbankservers, sind mittels geeigneten Werkzeugs zu überwachen. Die Überwachung stellt sicher, dass Anomalien rechtzeitig durch die Informatik erkannt und Massnahmen eingeleitet werden können. Bei der Überwachung ist darauf zu Achten, dass durch die Überwachung keine Überbelastung der produktiven Systeme stattfindet.

4.9 Protokollierung

Zur Erfüllung gesetzlicher Nachweispflichten, zur Aufrechterhaltung des ordnungsgemässen Betriebs, zum Zweck der Gefahrenabwehr durch Erkennen von Anomalien und zum Nachweis von Verantwortlichkeiten sind Protokolldaten zu erheben und zu speichern. Grundsätzlich sind nur Protokollinformationen zu erheben, welche regelmässig ausgewertet werden. Es ist dabei nach dem Grundsatz der Verhältnismässigkeit zu verfahren.
Fernzugriffe auf Daten und Systeme müssen immer protokolliert werden. Die Rückverfolgbarkeit ist zu gewährleisten.
Für alle betriebsrelevanten Systeme und Systeme mit sensitiven Daten sind Vorgaben zur Protokollierung zu definieren. Folgende Aktivitäten werden (möglichst in pseudonymer Form) für IT-Systeme aufgezeichnet, überwacht und regelmässig ausgewertet:

- Login und Logout
- Erfolgreiche und abgewiesene Zugriffsversuche auf Systeme und Daten
- Veränderungen an der Systemkonfiguration
- Vergabe und Änderung von Privilegien und Benutzerkonten
- Alle Aktionen, die erhöhte Privilegien benötigen
- Aktivierung und Deaktivierung von Schutz- oder Authentisierungs-Systemen

Die Systemuhren (Rechneruhren) werden synchronisiert, um exakte Aufzeichnungen sicherzustellen.
Die Zugriffsrechte auf Protokolldaten werden restriktiv und nach dem Need-to-Know-Prinzip vergeben.

4.10 Zugriffsmanagement

4.10.1 Verwalten von Zugriffsberechtigungen

Jeder Zugriff auf ein System wird mit einem Zugriffsschutz gesichert. Für die Vergabe der Zugriffsberechtigungen wird ein rollenbasiertes Berechtigungskonzept geführt.
Details werden in der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel im Kapitel 6 geregelt.

4.10.2 Zugriffe auf E-Mails

Für Zugriffe auf E-Mail-Postfächer sind die Berechtigungen zu definieren und auf ein Minimum zu beschränken. E-Mails, die im persönlichen Ordner (persoenlich) eines Mitarbeitenden abgelegt sind, dürfen durch die Informatik auch im Notfall nicht eingesehen werden.

4.10.3 Netzwerkzugriffe

Für Netzwerkzugriffe sind zusätzlich folgende Vorgaben zu beachten:

- Für Mitarbeitende ist der Zugriff nur auf interne Dienste zu ermöglichen, deren Benutzung ihnen ausdrücklich gestattet wurde. Der Zugriff muss durch Authentifizierungssysteme geprüft werden.
- Schnittstellen zu fremden Netzwerken sind zu genehmigen. Bestimmte betrieblich notwendige Programme werden durch den Informationssicherheitsverantwortlichen und IT-Leiter bewilligt und durch den Fachbereich Informatik freigeschaltet.

4.10.4 Betriebssystemzugriffe

Für Betriebssystemzugriffe gelten zusätzlich folgende Vorgaben:

- Der Zugriff auf Betriebssysteme darf nur über ein sicheres Anmeldeverfahren erfolgen.
- Der Zugriff auf Systemdienstprogramme (z.B. Managementkonsole) ist zu beschränken. Der Zugriff ist, wo immer technisch möglich, zu authentifizieren.

4.10.5 Fernzugriffe

Werden Fernzugriffe beantragt, prüft die Informatik, ob eine Bewilligung der Direktion notwendig ist. Der Mitarbeitende wird über die Bewilligung oder eine begründete Ablehnung des Zugriffs informiert. Die bewilligten Fernzugriffe werden dokumentiert und durch den Informationssicherheitsverantwortlichen oder den Informationssicherheitsbeauftragten sowie durch die Informatik mindestens jährlich auf ihre Notwendigkeit hin überprüft, insbesondere wenn es sich um Fernzugriffe aus dem Ausland handelt.
Die Informatik stellt sicher, dass die bewilligten Fernzugriffe auf Daten und Systeme von Spitäler fmi AG nur über geschützte Verbindungen möglich sind (z.B. via VPN).
Fernzugriffe auf Daten und Systeme von Spitäler fmi AG bedürfen einer Zweifaktor-Authentifizierung. Ist dies nicht möglich, definiert die Informatik im Einzelfall alternative Sicherheitsmassnahmen und setzt diese um. Entsprechende Ausnahmen benötigen eine Bewilligung durch den Informationssicherheitsverantwortlichen oder Informationssicherheitsbeauftragten.
Die Informatik ist für die Installation und Konfiguration der technischen Hilfsmittel bzw. deren Überprüfung sowie für die Überwachung der Fernzugriffe verantwortlich. Die Systemberechtigungen dürfen nur nach definieren Szenarien gemäss Kapitel «Fernzugriffe» in der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel vergeben werden.

5 Netzwerk und Kommunikation

5.1 Trennung von Netzwerken

Die einzelnen Netze und Anwendungen werden in Zonen unterteilt und in einem Zonenkonzept festgehalten. Die Zonierung erfolgt dabei unter Berücksichtigung des Schutzbedarfs der einzelnen Netze und der darin bearbeiteten Daten. Für das Netzmanagement wird ein Rollen- und Berechtigungskonzept erstellt und umgesetzt. Das Rollen- und Berechtigungskonzept wird mindestens jährlich geprüft und aktualisiert. Spezielle Tätigkeiten und zugehörige Zugriffe auf Informationen im Netzmanagement müssen im Konzept abgebildet werden.
Alle erforderlichen Netzübergänge werden regelmässig kontrolliert. Regeländerungen (Firewall-Changes) müssen freigegeben und gemäss Planung umgesetzt sowie protokolliert werden.
Systeme, auf die direkt oder indirekt aus einem öffentlichen Netz zugegriffen werden kann, müssen durch geeignete Sicherheitsmechanismen vom Internet getrennt sein (Firewall, Proxy, etc)
Das Wireless LAN wird ebenfalls im Zonenkonzept festgehalten. Das öffentliche Wireless LAN muss vom internen Netz getrennt sein.

5.2 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

Test- und Entwicklungssysteme müssen von Produktivsystemen getrennt werden, um das Risiko unautorisierter Zugriffe oder unautorisierter Änderungen an der Betriebsumgebung zu verringern.
Müssen für Einzeltests oder einen Pilotbetrieb produktive Systeme der Organisation auf Testnetze zugreifen, dürfen nur die am Test beteiligten Systeme und Benutzer auf das Testsystem zugreifen.

5.3 Netzübergänge

Jede Kommunikation zwischen den Netzen von Spitäler fmi AG und öffentlichen Netzwerken muss über einen Security Gateway geführt werden. Security Gateways dürfen die einzige Schnittstelle zwischen den beiden Netzen bilden.
Der Security Gateway bzw. die Firewall ist so zu wählen, dass die Möglichkeit besteht, Netzwerkbereiche mit unterschiedlichen Sicherheitsniveaus unter Berücksichtigung der vorliegenden Richtlinie zu verbinden.
Die Nutzung von Netzübergängen wird regelmässig kontrolliert. Datenverbindungen oder Dienste eines Netzüberganges, welche eine Gefährdung für das Netzwerk der Spitäler fmi AG darstellen, müssen durch die Konfiguration von Sicherheitseinrichtungen unterbunden werden. Ist dies nicht oder nur mit unverhältnismässigem Aufwand möglich, können alternativ Nutzungsregelungen für die Mitarbeitenden erlassen werden. Die Einhaltung muss in diesem Fall kontrolliert werden.
In der Voreinstellung für Netzübergänge zu Dienstleistern muss der Datenverkehr blockiert und nach Genehmigung freigeschalten werden.
Alle Übergänge zwischen dem Netz von Spitäler fmi AG und anderen Netzen sind zu prüfen und auf ein Minimum zu begrenzen.

5.4 Vorgabe von Kommunikationsprofilen

Für jeden Dienst muss explizit festgelegt werden, für welche Benutzer und/oder PC-Arbeitsplätze dieser zugelassen ist.
Es dürfen nur Dienste zugelassen werden, welche unbedingt notwendig sind. Wird eine Freigabe für die Nutzung eines Dienstes beantragt, für den noch keine Regelung besteht, ist ebenfalls zu prüfen, ob und für welche Benutzer und/oder PC-Arbeitsplätze dieser zugelassen werden soll. Dienste, welche nicht freigegeben wurden, müssen in den Voreinstellungen soweit möglich unterbunden werden.
Aktive Inhalte in Downloads oder Angeboten aus öffentlichen Netzwerken dürfen erst an Systeme im internen Netz der Spitäler fmi AG ausgeliefert werden, wenn diese durch ein System auf ihr systemkonformes Verhalten geprüft werden. Die aktiven Inhalte sind dabei in einer geschützten Umgebung als Ganzes auf ihren Funktionsumfang zu prüfen und gegebenenfalls zu filtern.
Ausnahmeregelungen, insbesondere für neue Dienste und kurzzeitige Änderungen (z.B. für Tests) sind möglich, sofern der Informationssicherheitsverantwortliche seine Zustimmung gegeben hat. Diese ist vorgängig einzuholen.

5.5 Nutzung des internen Netzwerks

Für neue Geräte im internen Netzwerk ist ein Antrag gemäss dem Einbindungsprozess von neuen Geräten zu erstellen. Die Informatik prüft, ob das neue Gerät die Anforderungen bezüglich Informationssicherheit erfüllt.
Der Informationssicherheitsbeauftragte kann zur Unterstützung beigezogen werden. Wird ein Gerät nicht bewilligt aber muss aufgrund der betrieblichen Notwendigkeit trotzdem eingesetzt werden, benötigt es eine Ausnahmebewilligung auf Stufe Geschäftsleitung. Die Risiken müssen ausgewiesen und durch den Informationssicherheitsbeauftragten an die Geschäftsleitung rapportiert werden. Wird eine Ausnahme bewilligt, muss sichergestellt werden, dass die Sicherheit des internen Netzwerks nicht gefährdet ist. Zudem sind die Netze durch die Informatik regelmässig auf nicht zugelassene Geräte zu prüfen.

5.6 Nutzung des Internets

Der Internetverkehr wird aus sicherheitstechnischen Gründen aufgezeichnet. Nur im Rahmen eines Sicherheitsvorfalls oder auf Antrag der Geschäftsleitung dürfen die Aufzeichnungen ausgewertet. Betrifft eine Auswertung personenbezogene Daten, muss der Datenschutzverantwortliche beigezogen werden.
Weitere Details werden in der Weisung über die Nutzung der Informatik- und Telekommunikationsmittel beschrieben.