Weisung

Weisung über die Nutzung der Informatik- und Telekommunikationsmittel

Informatik / Geschäftsleitung

Spitäler Frutigen Meiringen Interlaken AG

Dokumenteigenschaften

Änderungsdatum	27.01.2026
Gültig ab	Freigabe
Version	4.3
Ersetzt Version	4.1
Verfasst durch	Thomas Huber (CTO Spitäler fmi AG); Othmar Wyss, Daniel Michel (Redguard); Monika Stucki (Redguard); Christian Fritz (Redguard); Marco Filli (ISO Spitäler fmi AG)
Freigegeben durch	Geschäftsleitung xx.xx.xxxx
Prozessverantwortlich	Informationssicherheitsbeauftragte:r (ISB)
Klassifizierung	intern

Dokumentenverlauf

Änderungsdatum	Version	Bearbeiter	Änderungen
10.12.2020	0.10	Redguard AG	Initialversion
12.12.2020	0.20	Redguard AG	Überarbeitung nach Review Spitäler fmi AG (Othmar Wyss)
03.06.2021	0.30	Redguard AG	Überarbeitung nach Review Spitäler fmi AG (Thomas Huber und Othmar Wyss)
06.08.2021	0.40	Redguard AG	Überarbeitung nach Abstimmung mit Spitäler fmi AG (Thomas Huber und Othmar Wyss)
28.09.2021	0.45	Redguard AG	Review durch Christian Fritz
21.10.2021	0.50	Redguard AG	Review / Abstimmung mit Othmar Wyss
01.11.2021	0.70	Redguard AG	Überarbeitung (Integration best. Weisung «Nutzung IT, Telekom»)
17.11.2021	0.80	Redguard AG	Überarbeitetung nach Feedback von Othmar Wyss
01.12.2021	1.00	Redguard AG	Finale Version zur Unterzeichnung GL
11.10.2022	1.10	Redguard AG	Review Workshop mit Artur Konowalczuk
17.10.2022	1.11	Redguard AG	Review Workshop mit Artur Konowalczuk
09.11.2022	1.12	Redguard AG	Überarbeitung durch Redguard
09.01.2023	1.14	Redguard AG	Neues Design und Ergänzung mit Glossar
18.01.2023	1.15	Redguard AG	Anpassungen nach Feedback von Artur Konowalczuk
25.01.2023	1.17	Redguard AG	Versionsnummer mit Konzept angeglichen, Bereitstellung für Review durch O.Wyss
06.02.2023	2.0	Othmar Wyss	Review. Bereit für Genehmigung
17.10.2024	3.0	Swiss Infosec	Ergänzungen
09.05.2025	4.0	Stephanie Müller	Überarbeitungen Rollen Kap. 2.3
23.06.2025	4.1	Marco Filli	Review und aufarbeiten für Genehmigung
07.11.2025	4.2	Marco Filli	Anpassungen nach Feedback durch Geschäftsleitungssitzung vom 27.10.
27.01.2026	4.3	Marco Filli	Anpassungen nach Feedback durch Geschäftsleitungssitzung vom 27.10.

■

Inhaltsverzeichnis

1 Einleitung

1.1 Ziel und Zweck

Die vorliegende Weisung beschreibt die wichtigsten Regeln zur Informationssicherheit bei der Nutzung der Informatik- und Telekommunikationsmittel der Spitäler fmi AG. Sie zeigt auf, was im Alltag zu beachten ist, damit die Daten und Systeme der Spitäler fmi AG zuverlässig geschützt bleiben – egal, ob du im Büro, unterwegs oder im Homeoffice arbeitest.

Die Vorgaben orientieren sich an anerkannten Standards wie der ISO/IEC 27001, berücksichtigen aber auch gesetzliche Anforderungen wie den Datenschutz, das elektronische Patientendossier oder die Medizinprodukteverordnung. Alles, was rechtlich und fachlich zu beachten ist, ist im übergeordneten Konzept Informationssicherheit im Kapitel „Vorgaben und Richtlinienlandschaft“ beschrieben.

1.2 Geltungsbereich

Diese Weisung gilt für alle Personen, welche mit Daten, Informationen oder IKT-Mitteln der Spitäler fmi AG arbeiten oder auf solche zugreifen, dabei wird nicht unterschieden, ob diese intern oder extern eingestellt sind.

Wenn du im Bereich Informatik und Digitalisierung arbeitest oder mit IT-Lieferanten zu tun hast, gelten ergänzend die Vorgaben der Weisung_Informationssicherheit_MA-IT.

Wenn externe IT-Dienstleister oder IT-Lieferanten für die Spitäler fmi AG arbeiten, musst du sicherstellen, dass sie diese wichtigen Sicherheitsvorgaben kennen und einhalten. Die Einhaltung dieser Vorgaben wird regelmässig gemeinsam mit dem Informationssicherheitsbeauftragten und dem Bereich Informatik und Digitalisierung überprüft.

1.3 Änderungen

Du hast eine Idee oder einen Hinweis, wie diese Weisung verbessert werden kann?
Änderungsvorschläge kannst du jederzeit beim Leiter Informatik und Digitalisierung, beim Informationssicherheitsverantwortlichen oder dem Informationssicherheitsbeauftragten, sowie beim Meldeportal für Ideen einreichen.

Wie solche Änderungen geprüft und umgesetzt werden, ist im übergeordneten Konzept Informationssicherheit, Kapitel „Änderungen“, beschrieben.

1.4 Kontrolle

Die vorliegende Weisung wird mindestens einmal pro Jahr durch den Informationssicherheitsverantwortlichen überprüft und bei Bedarf ergänzt, damit sie jeweils aktuell und praxistauglich bleibt.

1.5 Ersatz von Dokumenten

Diese Version ersetzt die bisher gültige «Weisung über die Nutzung der Informatik- und Telekommunikationsmittel»

1.6 Inkrafttreten

Sie tritt in Kraft, sobald sie von der Geschäftsleitung freigegeben wurde.

1.7 Referenzierte und mitgeltende Dokumente

Dokumentenname
Konzept Informationssicherheit
Weisung_Informationssicherheit_MA-IT
Weisung Datenschutz
Handbuch Informationssicherheit und Datenschutz
Geheimhaltungsvereinbarung für Externe
Geheimhaltungsvereinbarung
Richtlinie Projektmanagement
Konzept Entsorgung Spitäler fmi AG
Merkblatt Phishing

2 Organisation

2.1 Verantwortlichkeiten

Die generelle Organisation zur Informationssicherheit ist im Konzept Informationssicherheit geregelt. Zusätzlich gibt es bestimmte Rollen mit klaren Aufgaben und Zuständigkeiten:

- **Business Owner:in** (aus dem Fachbereich)
  Du bist für eine Applikation verantwortlich? Dann definierst und gewährleistest du den nötigen Schutzbedarf für diese Applikation und die darin enthaltenen Daten. Deine Rolle wird im Asset Management vom Bereich Informatik und Digitalisierung festgehalten.
- **Applikationsverantwortliche**:r (Informatik und Digitalisierung)
  Du bist auf Seiten der IT für eine Applikation zuständig? Dann unterstützt du den/die Business Owner:in bei der Bewertung und Umsetzung des passenden Schutzbedarfs. Auch deine Rolle wird im Asset Management gepflegt.
- **Projektleiter:in**
  Wenn du ein Projekt leitest, musst du dafür sorgen, dass die Ziele der Informationssicherheit im Projektablauf gemäss den Vorgaben der Spitäler fmi AG eingehalten werden.
- **Mitarbeitende**
  Du bist verpflichtet, die Regeln zur Informationssicherheit einzuhalten und aktiv umzusetzen – ganz gleich, in welchem Bereich du arbeitest.

2.2 Sensibilisierung

Die Informationssicherheitsverantwortliche Person sorgt dafür, dass du und alle anderen Mitarbeitenden eure Verantwortung in Sachen Informationssicherheit kennt und wahrnehmt.

Alle Mitarbeitenden, mit Zugriff auf Daten oder IKT-Mittel der Spitäler fmi AG, werden mindestens einmal pro Jahr zu relevanten Sicherheitsthemen geschult und entsprechend sensibilisiert.

2.3 Vorgehen bei Informationssicherheitsvorfällen

Ein Informationssicherheitsvorfall, auch «Security Incident» genannt, ist ein Ereignis, welches gegen das Konzept Informationssicherheit, die vorliegende Weisung oder den Datenschutz verstösst.
Dazu gehören alle Fälle, bei welchen Vertraulichkeit, Verfügbarkeit, Integrität oder Nachvollziehbarkeit von Informationen gefährdet oder verletzt werden.

Wenn du einen Vorfall entdeckst oder den Verdacht hast, dass etwas nicht stimmt, melde dich sofort beim Service Desk.
Du erreichst ihn während der Arbeitszeiten (Mo–Fr, 07:30–12:00 / 13:30–17:00). Ausserhalb dieser Zeiten steht dir der 24/7-Pikettdienst des Bereichs Informatik und Digitalisierung zur Verfügung.

Wer macht was im Fall eines Sicherheitsvorfalls?

Du als Mitarbeitende:r
- Du meldest (potenzielle) Vorfälle direkt beim Service Desk oder beim Pikettdienst
- Du hältst dich an die Vorgaben zur Geheimhaltung und sprichst nicht mit Dritten über den Vorfall

Service Desk
- Handelt Vorfälle mit geringer oder normaler Dringlichkeit direkt mit dir ab
- Meldet schwerwiegende Fälle umgehend an die Informationssicherheitsverantwortliche oder -beauftragte Person

Pikettdienst
- Leitet Meldungen mit niedriger Dringlichkeit an den Service Desk weiter und informiert dich darüber
- Meldet schwerwiegende Fälle ebenfalls an die zuständigen Personen in der Informationssicherheit

Bereich Informatik und Digitalisierung (IT)
- Koordiniert die Kommunikation mit betroffenen externen Dienstleistern – gemeinsam mit der Informationssicherheitsverantwortlichen oder -beauftragten Person

Dienstleistende
- Müssen Vorfälle, welche sie feststellen, sofort dem Service Desk melden

Informationssicherheitsverantwortliche:r (ISV)
- Kommuniziert intern bei schwerwiegenden Vorfällen
- Klärt mit der Geschäftsleitung, ob externe Kommunikation nötig ist und, wenn ja, wie sie abläuft

Informationssicherheitsbeauftragte:r (ISB)
- Bewertet Vorfälle, hilft bei der Behebung und unterstützt die verantwortliche Person

Datenschutzkoordinator:in (DSK)
- Ist erste Ansprechstelle für Datenschutzfragen innerhalb der Spitäler fmi AG
- Arbeitet eng mit dem externen Datenschutzbeauftragten zusammen

Externe:r Datenschutzbeauftragte:r (DSB)
- Unterstützt die Datenschutzkoordination fachlich
- Details dazu findest du im Konzept Informationssicherheit

Wenn es sich um einen meldepflichtigen Datenschutzvorfall handelt, informiert die/der Datenschutzverantwortliche nach Rücksprache mit der Geschäftsleitung den kantonalen Datenschutzbeauftragten, dies geschieht spätestens innert 72 Stunden nach Bekanntwerden.
Bei Fällen, welche nicht unter den kantonalen Leistungsauftrag fallen (z. B. Personaldaten), wird zusätzlich der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) informiert.
Bei einem Cyberangriff meldet die/der Informationssicherheitsbeauftragte den Vorfall innerhalb von 24 Stunden nach deren Entdeckung an das Bundesamt für Cybersicherheit, (BACS). Dies geschieht ebenfalls in Absprache mit der Geschäftsleitung.
https://security-hub.ncsc.admin.ch/#/attack-reports/create - CSH - Create attack report

Wenn Partner oder Lieferanten betroffen sind, erfolgt die externe Kommunikation, nach Rücksprache mit der Geschäftsleitung, klar und transparent durch die zuständige Stelle.

2.4 Informationssicherheit in IKT-Projekten

Wenn du ein Projekt leitest, bist du dafür verantwortlich, die Themen Informationssicherheit und Datenschutz bereits in der Initialisierungsphase zu berücksichtigen. So lassen sich spätere Überraschungen wie Mehrkosten durch eine verpflichtete Eingabe bei der Datenschutzaufsichtsstelle oder Sicherheitsrisiken vermeiden.
Als Projektleiter:in klärst du zu Beginn den Schutzbedarf der betroffenen Systeme und Daten. Für den späteren Betrieb ist dann der/die Business Owner:in dafür verantwortlich, dass die Einstufung des Schutzbedarfs korrekt bleibt.
Falls du dabei Unterstützung brauchst, kannst du dich an die/den Informationssicherheitsbeauftragte:n wenden, sie oder er unterstützt dich bei der Schutzbedarfsanalyse beratend.

3 Grundlegende Informationen zur Datensicherheit/-bearbeitung

Geschäftliche Daten dürfen von Mitarbeitenden lediglich im Rahmen ihrer Geschäftstätigkeit genutzt und bearbeitet werden.

3.1 Clear Desk Policy

Unter der Clear-Desk-Policy versteht man, dass vertrauliche Informationen am Arbeitsplatz so geschützt werden, dass Unbefugte keinen Zugriff auf diese haben. Diese Massnahme dient dazu, die unbefugte Einsichtnahme, Verwendung oder Entwendung von Informationen zu verhindern.

Die Anforderungen richten sich nach dem Risiko und Zugänglichkeit des Arbeitsplatzes:

- In öffentlich einsehbaren oder allgemein zugänglichen Arbeitsplätzen wie z.B. beim Empfang oder offen zugänglichen Büros ohne Türschliesssystem dürfen vertrauliche Dokumente nicht unbeaufsichtigt offen herumliegen. Ausdrucke, Notizen oder Akten sind stets so zu verstauen, dass sie für Dritte nicht unbeaufsichtigt offen einsehbar oder zugänglich sind.

- In Räumlichkeiten mit eingeschränktem Zugang (z.B. Büros mit Zutrittskontrolle via Badge und einem kleinen Berechtigungskreis, wie der Patientenadministration oder dem HR) muss beim Verlassen des Arbeitsplatzes mindestens sichergestellt werden, dass die Bürotür geschlossen ist. Der Zugang zu diesen Räumlichkeiten geschieht geschützt (Badge) und wird im Schliesssystem protokoliert. Diese Protokolle können entsprechend bewertet und ausgewertet werden.

Vertrauliche Daten müssen vor unbefugten Zugriff geschützt aufbewahrt werden.

Es gelten folgende Grundsätze:

- Keine Ausdrucke im Drucker oder Kopierer liegen lassen
- Keine vertraulichen Informationen direkt im Altpapier entsorgen
- Keine Passwortnotizen am Arbeitsplatz aufbewahren
- Computer sind beim Verlassen des Arbeitsplatzes zu sperren («Windows-Taste» + L)
- Mobile Geräte und Speichermedien der Spitäler fmi AG nicht unbeaufsichtigt liegen lassen.

3.2 Verschlüsselte Kommunikation

Insbesondere beim Versand von besonders schützenswerten Personendaten oder anderen sensitiven Inhalten per E-Mail, ist sicherzustellen, dass der Versand solcher Daten verschlüsselt, z.B. mittels HIN-Mail, erfolgt.
Ein teilen vertraulicher Informationen oder Daten via SMS oder z.B. WhatsApp ist untersagt.
Der Bereich Informatik und Digitalisierung kann dich hier bei der Wahl des korrekten Kommunikationskanals unterstützen.

3.2.1 Überprüfung verschlüsselter Verbindungen

Auch Schadsoftware (z. B. Ransomware) nutzt verschlüsselte Verbindungen um unbemerkt mit dem jeweiligen Angreifer zu kommunizieren.
Um solche Bedrohungen zu erkennen, werden bestimmte verschlüsselte Datenverbindungen automatisiert und gezielt zentral überprüft, bevor sie das interne Netzwerk der Spitäler fmi AG erreichen oder verlassen.

Die Kontrolle erfolgt ausschliesslich zum Schutz der IT-Infrastruktur und der darin gespeicherten Daten.

3.3 Social Engineering

Beim Social Engineering versuchen Angreifer, durch gezielte Täuschung an vertrauliche Informationen oder Zugangsdaten zu gelangen.
Dabei werden gezielt Mitarbeitende angesprochen, um Vertrauen zu gewinnen und Menschen dazu zu bringen, ungewollt Zugang zu IT-Systemen oder sensiblen Daten zu ermöglichen. Diese Kontaktaufnahmen geschehen auf verschiedenen Kanälen (z.B. E-Mail, SMS oder ein Anruf).

Typische Merkmale solcher Angriffe:

- Die Angreifer geben sich als Kollegen, Behördenvertreter, externe Partner oder IT-Mitarbeitende aus.
- Sie verwenden scheinbar internes Wissen oder Fachbegriffe, die sie sich zuvor beschafft haben.
- Sie wirken dringlich oder emotional: z. B. als gestresste Kollegin, als drohender «Kunde» oder mit einem verlockenden Angebot wie Geld oder Gutscheinen.
- Wenn eine Person nicht reagiert, wird der Versuch bei der nächsten Ansprechperson wiederholt – oft so lange, bis jemand darauf eingeht.

So kann man sich schützen:

- Vorsicht walten lassen besonders bei ungewöhnlichen Anfragen per E-Mail oder Telefon – auch wenn sie vermeintlich von einer bekannten Person stammen.
- Im Zweifel persönlich nachfragen, ob die Anfrage tatsächlich von der betreffenden Person stammt.
- Verdächtige E-Mails sollten dem Service Desk gemeldet werden.
- Niemals Passwörter, Kreditkartendaten oder vertrauliche Informationen telefonisch oder per E-Mail weitergeben.

Social Engineering ist schwer erkennbar und genau darauf setzen die Angreifer.

4 Bearbeitung von Daten

Mitarbeitende dürfen geschäftliche Daten nur für ihre Aufgaben bei der Spitäler fmi AG verwenden und bearbeiten.
Zulässig sind insbesondere Tätigkeiten im Rahmen der Patientenversorgung, der Administration, der Abrechnung, der Qualitätssicherung sowie gesetzlicher Pflichten.
Nicht zulässig sind private, fachfremde oder externe Zwecke.

Zulässig	Nicht zulässig
Nutzung von Patientendaten zur Behandlung, Pflege oder Betreuung im eigenen Aufgabenbereich	Einsicht in Patientendaten aus Neugier oder ohne konkreten Arbeitsauftrag
Verwendung geschäftlicher Daten für administrative Aufgaben (z.B. Terminplanung, Dokumentation, Abrechnung)	Nutzung geschäftlicher Daten für private Zwecke oder private Projekte
Bearbeitung von Daten zur Erfüllung gesetzlicher, organisatorischer oder qualitätssichernder Pflichten	Weitergabe oder Nutzung von Daten für externe oder fachfremde Zwecke ohne entsprechende Berechtigung

4.1 Klassifizierung von Daten

Bei Spitäler fmi AG werden alle Daten einer Klassifizierungsstufe zugeordnet, sofern du bei der Erstellung von Daten keine explizite Klassifizierung vollziehst, werden diese als «Intern» klassifiziert. Die zuständige Person (Business Owner:in) sorgt dafür, dass die Daten gemäss dieser Einstufung korrekt verarbeitet und geschützt werden.

Klassifizierung	Erläuterung	Personenkreis
Nicht klassifiziert	Sämtliche der Öffentlichkeit zugängliche Daten wie beispielsweise aus dem Internet. Die freie Kommunikation und Weitergabe dieser Informationen sind erlaubt.	Die Informationen sind uneingeschränkt für alle zugänglich.
Intern	Alle Unternehmensdaten, welche nicht für die Öffentlichkeit bestimmt und nicht als vertraulich klassifiziert sind.	Die Informationen sind grundsätzlich nur Mitarbeitenden der fmi und dedizierten, extern beauftragten Partnern zugänglich.

Klassifizierung	Erläuterung	Personenkreis
Vertraulich	Als Vertraulich werden Informationen klassifiziert, welche einen besonderen Schutzbedarf aufweisen (zum Beispiel Patientendaten). Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile, welche bei Spitäler fmi AG bearbeitet werden, sind zwingend als Vertraulich zu klassifizieren.	Der Personenkreis, welcher auf als Vertraulich klassifizierte Informationen Zugang hat, ist so klein wie möglich zu halten. Die Informationen sind grundsätzlich nur den im Behandlungspfad/Supportprozess involvierten Personen zugänglich zu machen. Persönliche Notizen von behandelnden Ärzten, therapeutischem Fachpersonal, Pflegepersonal oder des Sozialdienstes dürfen nur dem jeweiligen Verfasser zugänglich sein.

Ein unsachgemässer Umgang mit vertraulichen Daten kann für Spitäler fmi AG folgende Schäden zur Folge haben:

- rechtliche Konsequenzen
- finanzieller Schaden
- Schaden für die Geschäftszwecke und Ziele
- Verlust von Ansehen und Vertrauen bei der einheimischen Bevölkerung, Feriengästen und insbesondere Patientinnen und Patienten

4.2 Personenbezogene Daten

Der/die Datenschutzberater:in ist Anlaufstelle für alle Fragen zum Datenschutz und erfüllt die Aufgaben gemäss dem Konzept Informationssicherheit.
Wenn du unsicher bist, wie du mit Personendaten umgehen sollst – oder wenn du einen möglichen Missbrauch erkennst –, melde dich sofort bei dem/der Datenschutzberater:in.
Beim Bearbeiten von Personendaten und Personaldaten beachtest du die Weisung Datenschutz sowie die Weisung zum Personaldatenschutz.

4.3 Umgang mit Daten

Du darfst Daten nur erfassen und bearbeiten, wenn du dazu berechtigt bist und auch nur für den vorgesehenen Zweck. Die private Nutzung von Geschäftsdaten ist nicht erlaubt.
Personenbezogene Daten darfst du nicht auf privaten Geräten (z. B. Laptop, Smartphone, USB-Stick) speichern oder bearbeiten.
Wenn Daten von mehreren Personen intern genutzt werden sollen, speichere sie in den dafür vorgesehenen Systemen (z. B. SharePoint, Netzlaufwerke, Fachapplikationen).
Vermeide es, Daten lokal im persönlichen Benutzerverzeichnis (z. B. auf dem Desktop) zu speichern – dort sind sie weder sicher noch für andere zugänglich. Wenn du Daten ausnahmsweise lokal speichern musst, übertrage sie so schnell wie möglich ins richtige System und lösche die lokale Kopie.

Bewahre physische und digitale Daten immer so auf, dass Unbefugte keinen Zugriff haben – egal, ob im Büro, unterwegs oder im Homeoffice.
Wenn du deinen Arbeitsplatz verlässt, achte darauf, dass intern oder vertraulich klassifizierte Daten nicht offen sichtbar oder zugänglich sind (siehe dazu Kap. 3.1 Clear Desk).

Wenn du vertrauliche Daten an externe Personen übermittelst (z. B. per E-Mail oder Internet), achte darauf, dass die Übertragung verschlüsselt erfolgt. Nutze dazu nur durch die Informatik freigegebene Systeme. Besonders schützenswerte Personendaten – zum Beispiel Gesundheitsdaten – darfst du ausschliesslich verschlüsselt (z. B. über HIN) oder gemäss den geltenden Prozessen und Verfahren weitergeben.

4.3.1 Verwendung externer Datenträger (z.B. USB-Sticks)

Wenn du Daten auf externen Datenträgern speicherst oder transportierst (z. B. USB-Stick oder externe Festplatte), musst du dafür zwingend verschlüsselte Datenträger verwenden.

Nutze ausschliesslich von der Informatik freigegebene und geschützte Speichermedien. Diese verfügen in der Regel über eine automatische Verschlüsselung, zum Beispiel BitLocker oder einer integrierten Hardwareverschlüsselung.
Entsprechende freigegebene Speichermedien können beim Bereich Informatik und Digitalisierung bezogen werden.

Nicht verschlüsselte Datenträger darfst du weder zum Transport noch zur Mitnahme von Daten verwenden.

Wenn du einen Datenträger gerade nicht brauchst, bewahre ihn so auf, dass niemand unbefugt darauf zugreifen kann, zum Beispiel in einem verschlossenen Schrank oder einer abschliessbaren Schublade.

4.3.2 Physische Dokumente / Ausdrucke

Physische Dokumente, welche Personendaten oder intern bzw. vertraulich klassifizierte Informationen enthalten, musst du gemäss dem Entsorgungskonzept der Spitäler fmi AG sicher entsorgen, sprich du darfst solche Unterlagen nicht über normale Abfalleimer oder die Altpapiersammlung entsorgen.

4.3.3 Aufbewahrung / Löschung

Wenn du Daten aufbewahrst oder archivierst, musst du die geltenden Aufbewahrungspflichten einhalten. Weitere Informationen dazu findest du in der Weisung Datenschutz. Daten, welche weder betrieblich noch rechtlich benötigt werden, sind zu löschen. Die Löschung darf nur durch berechtigte Personen durchgeführt werden.
Wo möglich, informiere vorab den zuständigen Business Owner.

Hinweis: Aufbewahrungspflichten gelten z. B. für Verträge, Personalunterlagen oder medizinische Dokumente. Wenn du unsicher bist, frag bei dem/der Datenschutzberater:in oder deiner Leitung nach.

4.4 Umgang mit E-Mail

Der Nutzen deiner fmi-E-Mail-Adresse ist für geschäftliche Zwecke vorgesehen.
Eine private Nutzung ist nur in beschränktem Rahmen erlaubt, etwa für gelegentliche persönliche Mitteilungen. Als private Nutzung gilt jede Anwendung, welche keinen direkten Zusammenhang mit deiner Tätigkeit bei Spitäler fmi AG hat. Die geschäftliche E-Mail-Adresse darf nicht für private Newsletter, Online-Anmeldungen oder persönliche Geschäfte verwendet werden.

Wenn du deine E-Mail-Adresse ausnahmsweise für private Zwecke nutzt, richtest du im Postfach den Ordner «persoenlich» ein und verwendest ihn konsequent für alle privaten Nachrichten. Sollte es zu einem Notfall kommen, beispielsweise bei plötzlicher Abwesenheit oder einem Sicherheitsvorfall, kann dein E-Mail-Postfach durch berechtigte Personen, unter Einhaltung der jeweiligen Prozesse, eingesehen werden. Dieser Zugriff erfolgt ausschliesslich zur Sicherstellung des Geschäftsbetriebs, unter Einhaltung des Vier-Augen-Prinzips und wird protokolliert. Persönlich gekennzeichnete E-Mails oder solche im Ordner «persoenlich» werden in einem solchen Fall nicht geöffnet.

Der Versand vertraulich klassifizierter Daten per E-Mail an externe Empfänger ist nur erlaubt, wenn die Übertragung verschlüsselt erfolgt – beispielsweise über HIN. Unverschlüsselte E-Mails gelten als unsicher, da sie leicht von Dritten mitgelesen oder manipuliert werden können.

Um dich vor Phishing und Schadsoftware zu schützen, prüfe E-Mails jeweils aufmerksam, achte dabei besonders auf Absender, Betreff, Links Anhänge und den Inhalt.

Bitte beachte folgende Punkte beim Umgang mit E-Mails:

- Leite geschäftliche E-Mails nie an private E-Mail-Konten weiter (z. B. Bluewin, Gmail) – solche Dienste erfüllen die gesetzlichen Anforderungen für unser Spitalumfeld nicht.
- Öffne keine E-Mails, wenn dir der Absender oder der Betreff verdächtig vorkommt.
- Nutze deinen gesunden Menschenverstand: Wenn du z. B. keinen Vertrag mit Swisscom oder Sunrise hast, sind E-Mails von diesen Absendern in der Regel betrügerisch.
- Öffne niemals Anhänge, die dir verdächtig erscheinen – auch nicht von vermeintlich bekannten oder vertrauenswürdigen Absendern, sondern prüfe immer:
  - Passt der Text zur Person?
  - Ist die Sprache auffällig (z. B. Englisch bei deutschsprachigem Absender)?
  - Erwartest du z.B. die Datei im Anhang?
- Öffne keine E-Mails mit Spassprogrammen oder kuriosen Inhalten, sie enthalten oft Schadsoftware.
- Phishing-Mails, die dich zur Eingabe von Passwörtern, Bankdaten oder Codes (z. B. PIN/TAN) auffordern, musst du sofort löschen. Gib niemals vertrauliche Informationen per E-Mail weiter.
- Wenn dir ein Link verdächtig vorkommt, klicke ihn nicht an und kopiere ihn auch nicht.
- Melde die E-Mail stattdessen sofort dem Service Desk – Sie können den Inhalt prüfen, ohne ein Risiko einzugehen.
- Wenn du versehentlich auf einen Phishing-Link geklickt hast, melde das sofort dem Service Desk.
  Das kann jeder Person passieren. Nicht melden kann aber schwerwiegende Folgen für Spitäler fmi AG haben.
- Antworte niemals auf Spam-Mail, das bestätigt nur, dass deine Adresse aktiv ist, und du erhältst noch mehr unerwünschte Nachrichten.
- Informiere den Service Desk und dein Team, wenn du verdächtige E-Mails erhältst.
  Teilt eure Erfahrungen – so erkennt ihr gemeinsam typische Merkmale schneller und schützt euch besser.
- Wenn du dir unsicher bist: Frag beim Service Desk nach – lieber einmal zu viel als einmal zu wenig.

Weitere Hinweise dazu findest du im Merkblatt Phishing. Wenn dir eine E-Mail verdächtig vorkommt oder du unsicher bist, leitest du sie umgehend an den Service Desk weiter. Anhänge oder Links in verdächtigen E-Mails darfst du auf keinen Fall öffnen.

4.4.1 Abwesenheiten

Denk bei Ferien oder geplanten Abwesenheiten daran, den Abwesenheitsassistenten in deinem E-Mail-Postfach zu aktivieren. So informierst du Absender:innen automatisch über deine Abwesenheit.

Bei unvorhergesehenen Abwesenheiten – zum Beispiel bei Krankheit – kann deine vorgesetzte Stelle beim Service Desk die Aktivierung des Abwesenheitsassistenten veranlassen. Das erfolgt ohne Zugriff auf deine E-Mails.

Sollte es in einem Notfall dringend notwendig sein, auf geschäftsrelevante E-Mails zuzugreifen, kann dies über den Service Desk beantragt werden. Ein solcher Zugriff erfolgt ausschliesslich zur Sicherstellung des Geschäftsbetriebs, unter Einhaltung des Vier-Augen-Prinzips und wird protokolliert.
Persönlich gekennzeichnete E-Mails oder Nachrichten im Ordner «persoenlich» werden nicht geöffnet.

4.4.2 Mailsicherung (Backup) und Archivierung

Damit wichtige Informationen nicht verloren gehen, werden alle E-Mails, sowohl gesendete als auch empfangene Nachrichten, inklusive Anhänge, automatisch gespeichert. Dabei wird nicht unterschieden, ob es sich um geschäftliche oder private Inhalte handelt.

Die Speicherung erfolgt systemseitig über eine spezialisierte Software. Sie dient dazu, rechtlich relevante E-Mails, zum Beispiel im Zusammenhang mit Dokumentationspflichten oder Nachweispflichten, entsprechend der Gesetzlichen Fristen aufzubewahren.

Die gespeicherten E-Mails sind nicht direkt für IT-Mitarbeitende einsehbar. Der Zugriff ist technisch geschützt und darf nur unter klar geregelten Voraussetzungen erfolgen – zum Beispiel im Notfall und mit entsprechender Berechtigung nach dem Vier-Augen-Prinzip.

5 Nutzung von Informations- und Kommunikationstechnologie-Mittel

IKT-Mittel (Informations- und Kommunikationstechnologie-Mittel) sind alle technischen Geräte, Programme und Systeme, welche zur Erfassung, Verarbeitung, Speicherung oder Übertragung von Informationen dienen. Dazu gehören zum Beispiel Computer, Tablets, Mobiltelefone, E-Mail, Fachanwendungen, Netzwerke und Speicherlösungen.
Alle IKT-Mittel der Spitäler fmi AG werden durch den Bereich Informatik und Digitalisierung verwaltet. Wenn du private IKT-Mittel geschäftlich nutzen willst, brauchst du vorgängig die Freigabe durch den Bereich Informatik und Digitalisierung.
Sowohl IKT-Mittel der Spitäler fmi AG als auch freigegebene private IKT-Mittel dürfen nicht missbräuchlich verwendet werden.

Verboten sind insbesondere:
- das Herunterladen oder Verbreiten von rassistischen, pornografischen oder anderweitig verletzenden Inhalten
- das absichtliche Versenden von schädlichem Code (z. B. Viren, Würmern, Trojanern oder Bots)
- das Versenden von Spam oder unerwünschten Massenmails

Wenn du bei der Nutzung von Informatikmitteln auf Störungen oder Sicherheitsprobleme stösst, informiere bitte umgehend den Service Desk.

Der Bereich Informatik und Digitalisierung setzt adäquate Schutzmassnahmen für alle IKT-Mittel um. Du darfst diese Schutzmassnahmen weder verändern noch umgehen. Konfigurationen, Deinstallationen oder das Deaktivieren von Sicherheitseinstellungen sind nur mit ausdrücklicher, schriftlicher Autorisierung erlaubt.
IKT-Mittel, welche nicht durch den Bereich Informatik und Digitalisierung konfiguriert wurden, dürfen nicht im internen Netzwerk der Spitäler fmi AG verwendet werden. Externe Geräte, die nicht zur Spitäler fmi AG gehören, dürfen nur über das Gäste-Netz «fmi-Public» verbunden werden.
Auf IKT-Mitteln der Spitäler fmi AG darf ausschliesslich Software eingesetzt werden, welche durch den Bereich Informatik und Digitalisierung freigegeben wurde. Die Installation erfolgt zentral durch den Bereich Informatik und Digitalisierung.

Software und Applikationen der Spitäler fmi AG dürfen nicht kopiert und nicht privat genutzt werden.
Die zur Verfügung gestellten Systeme dürfen von dir weder verändert, repariert, erweitert noch selbst entsorgt werden.
Für mobile Arbeitsplätze und Homeoffice gelten grundsätzlich die gleichen Regeln wie an internen Arbeitsplätzen der Spitäler fmi AG.

5.1 Private Nutzung

Die technischen Geräte und Programme der Spitäler fmi AG – wie Computer, E-Mail oder Internetzugang – sind in erster Linie für die Arbeit bestimmt. Eine begrenzte private Nutzung ist erlaubt, zum Beispiel das Lesen einer privaten E-Mail oder eine kurze Internetsuche, solange dadurch weder das System übermässig belastet noch dein Arbeitsablauf gestört wird. Die Speicherung privater Daten auf IKT-Mitteln der Spitäler fmi AG ist grundsätzlich nicht erlaubt.

Eine Ausnahme gilt für dienstlich zur Verfügung gestellte Smartphones und Tablets: Dort darfst du private Daten speichern, sofern sie klar als privat gekennzeichnet sind – zum Beispiel durch eigene Ordner oder eindeutige Bezeichnungen.

Beachte dabei, dass die Spitäler fmi AG keine Haftung für Verlust, Löschung oder Beeinträchtigung privater Daten auf geschäftlichen Geräten, unabhängig davon, ob die Speicherung erlaubt war oder nicht übernimmt.
Grundsätzlich sind folgende Regeln einzuhalten:

- Für dienstliche Zwecke darfst du nur Applikationen verwenden, welche durch die Spitäler fmi AG freigegeben wurden. Diese Apps wurden auf Sicherheit und Datenschutz geprüft.
- Im Falle eines Geräteverlusts oder aus Sicherheitsgründen kann es jederzeit zur vollständigen Löschung des Geräts kommen, davon sind auch private Daten betroffen. Eine Haftung der Spitäler fmi AG für solche Verluste ist ausgeschlossen.
- Private Daten musst du, soweit möglich, klar kennzeichnen und getrennt von geschäftlichen Informationen speichern.

Beachte ausserdem: Bei der automatischen Sicherung (Backup) von Geräten erfolgt keine Unterscheidung zwischen privaten und geschäftlichen Inhalten, die Daten werden gemeinsam gesichert.

5.2 Verwendung mobiler IKT-Mittel

Wenn du mobile Geräte wie Smartphones oder USB-Sticks einsetzt, über welche auf Daten der Spitäler fmi AG zugegriffen werden kann, musst du die geltenden Sicherheitsvorgaben zum Datenschutz, Diebstahlschutz und zur Datensicherung einhalten.
Alle IKT-Mittel, insbesondere mobile Geräte, musst du so aufbewahren, dass sie nicht entwendet werden können. An öffentlichen Orten dürfen mobile Geräte nicht unbeaufsichtigt für dritte zugänglich sein.
Bei Verlust, Diebstahl oder beim Verdacht auf Manipulation eines IKT-Mittels musst du den Service Desk umgehend informieren. Der Service Desk ist berechtigt, bei vermissten Geräten oder aus Sicherheitsgründen eine Remote-Löschung durchzuführen.
Für den physischen Zugang zu IKT-Mitteln gelten zusätzlich die Vorgaben gemäss Ziffer 6.1 dieser Weisung.

5.2.1 Notebooks

Es gelten die folgenden zusätzlichen Regeln für den Einsatz von Notebooks:

- Verbinde dein Notebook mindestens einmal pro Woche mit dem Netzwerk der Spitäler fmi AG, damit automatische Updates (z. B. Virensignaturen, Programmupdates und Sicherheitspatches) installiert werden können.
- Die lokale Speicherung von Daten auf Spitäler fmi AG -Notebooks ist grundsätzlich erlaubt, da die Festplatten durch die IT mit BitLocker verschlüsselt sind. Bitte achte in diesem Fall darauf, dass die Originaldaten zusätzlich auf dem vorgesehenen Netzwerklaufwerk der Spitäler fmi AG abgelegt werden – so sind sie gesichert und für die entsprechenden Mitarbeiter zugänglich.

5.2.2 Smartphone / Tablets

Dienstlich eingesetzte Smartphones und Tablets sind im zentralen Verwaltungssystem für mobile Geräte (MDM, Mobile Device Management) der Spitäler fmi AG registriert.

Dieses System ermöglicht es der IT, Geräte zentral zu verwalten, Sicherheitsvorgaben durchzusetzen und die Verbindung zur Verwaltungs-App herzustellen, etwa um verlorene Geräte zu sperren oder Sicherheitsrichtlinien durchzusetzen.
Für die geschäftliche Nutzung von Smartphones und Tablets gelten folgende Vorgaben:

- Du darfst keine Veränderungen am Betriebssystem vornehmen (z. B. Jailbreak bei iPhones).
- Auf dem Gerät muss ein Passwort mit mindestens 6 nicht aufeinanderfolgenden Ziffern gesetzt werden. Eine Fingerprint-Identifikation oder FaceID ersetzt den Passwortschutz nicht vollständig.
- Nach 10 fehlerhaften Passworteingaben werden alle Daten auf dem Gerät automatisch gelöscht.
- Die Funktion zur Remote-Löschung muss aktiviert sein.
- Du musst regelmässig System- und App-Updates installieren. Bei ausstehenden Updates kann die Informatik den Zugriff auf Systeme sperren.
- Der automatische Zugriffsschutz (z. B. Bildschirmsperre) muss sich spätestens nach 5 Minuten Inaktivität aktivieren.
- Ausserhalb der E-Mail-App (inkl. Kontakten) dürfen keine Geschäftsdaten lokal auf dem Gerät gespeichert oder bearbeitet werden.

Wird ein Gerät entsorgt oder weitergegeben, werden vorgängig sämtliche Daten auf diesem Gerät unwiderruflich gelöscht.

5.2.3 Private Geräte

Wenn du ein privates Gerät (z. B. Smartphone oder Tablet) für den geschäftlichen Einsatz freigegeben bekommen hast (siehe Ziffer 5), musst du darauf achten, dass private und geschäftliche Daten klar voneinander getrennt sind, zum Beispiel durch eine separate Arbeitsumgebung (Container-Lösung).

Bei Verlust oder Diebstahl kann die IT die geschäftlichen Daten aus der Ferne löschen und das Gerät, wenn gewünscht, unbrauchbar gemacht werden.

Auf allen anderen privaten Geräten darfst du keine Daten der Spitäler fmi AG bearbeiten oder speichern. Der Zugriff auf E-Mails und Kalender ist nur erlaubt, wenn du ein Gerät verwendest, welches entweder von der Spitäler fmi AG zur Verfügung gestellt oder offiziell durch die IT freigegeben und mit einer MDM-Lösung abgesichert wurde.

5.2.4 Speichermedien

Die Verwendung von privaten USB-Sticks oder anderen nicht freigegebenen Speichermedien (z. B. externe Festplatten, SD-Karten, DVDs) für geschäftliche Zwecke ist nicht erlaubt.
Aus Sicherheitsgründen darfst du keine externen Datenträger oder persönliche USB-Geräte – wie USB-Gadgets oder Zubehör – an Systeme der Spitäler fmi AG anschliessen. Solche Geräte können Schadsoftware enthalten und stellen ein Risiko für das gesamte Netzwerk der Spitäler fmi AG dar.

Wenn du ein zugelassenes externes Speichermedium (z. B. einen USB-Stick) anschliesst, wird automatisch eine Sicherheitsprüfung auf Schadsoftware durchgeführt. Erscheint im Anschluss eine Warnmeldung, unternimm bitte keine eigenen Schritte, sondern informiere den IT-Service Desk umgehend und lasse die Warnmeldung geöffnet, damit der Service Desk diese lesen und entsprechende Schritte zur Lösung einleiten kann.

5.3 Umgang mit Störungen und Vorfällen

5.3.1 Umgang mit Störungen

Eine Störung liegt vor, wenn IT-Systeme, Programme oder Netzwerkverbindungen nicht wie gewohnt funktionieren und dadurch deine Arbeit beeinträchtigt wird.

In solchen Fällen kontaktierst du den Service Desk. Dieser dokumentiert die Störung, kümmert sich um die Behebung oder koordiniert bei Bedarf die Weiterleitung an externe Dienstleister.

Auch automatische Warnmeldungen oder Fehlermeldungen meldest du direkt dem Service Desk und lässt dabei die Warnmeldung geöffnet, damit der Service Desk diese lesen und entsprechende Schritte zur Lösung einleiten kann.

5.3.2 Umgang mit Informationssicherheitsvorfällen und Datenschutzvorfällen

Vermutete oder tatsächlich eingetretene Informationssicherheits- und/oder Datenschutzvorfälle sind gemäss den geltenden Prozessen sofort zu melden.
Beispiele:

- Verdacht eines Virenbefalls
- Unerlaubter Systemeingriffs durch nicht-berechtigte Dritte via Internet
- Phishing
- Versand von klassifizierten Informationen an einen falschen Empfänger

5.3.3 Reparatur und Entsorgung

Defekte IKT-Mittel musst du der Informatik übergeben. Sie kümmert sich um die Reparatur oder stellt bei Bedarf ein Ersatzgerät bereit.

Wenn ein IKT-Mittel nicht repariert werden kann oder an Drittpersonen weitergegeben werden soll, sorgt die Informatik dafür, dass alle Daten fachgerecht gelöscht werden, bevor das Gerät entsorgt oder übergeben wird.

Datenträger (z. B. USB-Sticks), welche Daten der Spitäler fmi AG enthalten oder zwischenspeichern, musst du so entsorgen, dass kein Rückschluss auf die gespeicherten Inhalte möglich ist. Die sichere Löschung und Entsorgung erfolgt gemäss dem Entsorgungskonzept der Spitäler fmi AG.

6 Benutzeridentifikation und Passwort

Alle Systeme, die bei der Spitäler fmi AG im Einsatz sind, sind mit einem Zugriffsschutz gesichert. Du meldest dich an einem System mit deiner User-ID (Benutzernamen) und einem Passwort oder mit einem Badge und PIN an. So werden dir die Systemzugriffe und Berechtigungen zugewiesen, welche deiner Funktion entsprechen. Durch diese eindeutige Identifikation ist es möglich, deine Tätigkeiten auf den Systemen bei Bedarf nachzuvollziehen, etwa im Rahmen von Sicherheitsüberprüfungen oder bei Vorfällen.

Wenn du deinen Arbeitsplatz verlässt – zum Beispiel in der Pause, bei einer Besprechung oder am Arbeitsschluss –, musst du unbefugten Zugriff verhindern, indem du:

- die passwortgeschützte Bildschirmsperre aktivierst (Windows + L),
- dich vom System abmeldest oder
- das Gerät herunterfährst.

Wenn bei der Anmeldung mehr als fünf falsche Passworteingaben erfolgen, wird dein Benutzerkonto automatisch gesperrt. Die Sperre wird nach 15 Minuten automatisch aufgehoben oder kann durch den Servicedesk manuell zurückgesetzt werden.

6.1 Umgang mit Zugangs- und Zugriffsberechtigungen

Zugangs- und Zugriffsberechtigungen werden bei der Spitäler fmi AG rollenbasiert und nach dem Need-to-Know-Prinzip vergeben. Deine direkte vorgesetzte Stelle ist dafür verantwortlich, dass du nur die Zugriffe erhältst, welche für deine Aufgaben notwendig sind. Es dürfen nur Berechtigungen beantragt werden, die zur Ausübung deiner Funktion tatsächlich erforderlich sind.
Du erhältst deinen Benutzernamen (User-ID) und ein Initialpasswort erst nach einer kontrollierten Schulung auf den Systemen sowie nach Erhalt des Konzepts und dieser Weisung zur Informationssicherheit.
Die Kenntnisnahme dieser Vorgaben bestätigst du mit deiner Unterschrift.
Nach der Prüfung und Freigabe durch den Bereich Informatik und Digitalisierung erhältst du das Schreiben «PC-Anwendung». Darin findest du deine Zugangsdaten. Das Initialpasswort musst du beim ersten Login zwingend in ein persönliches Passwort ändern. Dieses Passwort muss den Vorgaben gemäss Ziffer 6.2 entsprechen.
Wenn du intern die Funktion oder Abteilung wechselst, werden deine bestehenden Berechtigungen überprüft und entsprechend angepasst, respektive gelöscht. Neue Berechtigungen musst du oder deine vorgesetzte Stelle über den IAM-Shop beantragen. Nach Freigabe werden sie durch die Informatik vergeben. Bei Rollenzuweisungen erfolgt die systemseitige Anpassung durch das HR.
Wenn du die Spitäler fmi AG verlässt, ist das HR dafür verantwortlich, deinen Austritt rechtzeitig im System zu erfassen. So wird der automatische Entzug der Zugriffsrechte angestossen. Bei Expressaustritten muss das HR den Bereich Informatik und Digitalisierung direkt informieren, damit die Berechtigungen umgehend manuell entzogen werden können.

Für Fernzugriffe musst du eine Bestellung im IAM-Shop erfassen. Die Freigabe erfolgt durch den Bereich Informatik und Digitalisierung, und – falls erforderlich – zusätzlich durch die Direktion. Wenn du gegen Sicherheitsvorgaben beim Fernzugriff verstösst, kann dir der Zugriff entzogen werden.

Der Zutritt zu Gebäuden oder bestimmten Bereichen (z. B. Technikräume, Sitzungszimmer) erfolgt mit einem persönlichen Badge, der durch den Bereich Technik und Sicherheit auf Basis des rollenspezifischen Berechtigungskonzepts ausgestellt wird.

- Du darfst deinen Badge nicht an andere Personen weitergeben.
- Bewahre ihn stets so auf, dass kein Dritter Zugriff darauf hat.
- Türen zu nicht öffentlich zugänglichen Bereichen dürfen nicht für unberechtigte oder unbekannte Personen offengehalten werden.
- Personen ohne Badge, welche sich in gesicherten Bereichen aufhalten, sind nach dem Grund ihrer Anwesenheit zu fragen und gegebenenfalls einer zuständigen Ansprechperson zuzuführen.
- Besucherinnen und Besucher in gesicherten Bereichen müssen jederzeit durch berechtigte Mitarbeitende begleitet werden.

6.2 Umgang mit Passwörtern

Ein sicherer Umgang mit Passwörtern ist zentral für den Schutz der Systeme und Daten der Spitäler fmi AG. Passwörter schützen deinen persönlichen Zugang und verhindern, dass Unbefugte auf vertrauliche Informationen zugreifen können.

Passwörter sind persönlich – du darfst sie nicht weitergeben. Gruppenpasswörter sind nicht erlaubt.
Wenn du ein Passwort versehentlich weitergegeben hast oder ein Missbrauch vermutet wird, informiere sofort den Service Desk und ändere das Passwort.
Bei ungewöhnlichen Anmeldeversuchen, verdächtigen Aktivitäten oder möglichen Fremdzugriffen musst du den Service Desk und deine vorgesetzte Person benachrichtigen.
Wenn du dein Passwort unter Beobachtung eingeben musst (z. B. in öffentlichen Bereichen), sei besonders vorsichtig – im Zweifelsfall Passwort ändern.
Passwörter dürfen nicht im Klartext gespeichert, nicht aufgeschrieben und nicht auf Funktionstasten hinterlegt werden. Wenn du es ausnahmsweise notieren musst, bewahre es so sicher auf wie eine Kreditkarte.
Wenn du mehrere Passwörter verwendest, müssen diese sich voneinander unterscheiden.

Erstellung sicherer Passwörter

- Benutzerpasswörter müssen mindestens 12 Zeichen lang sein.
- Administrationspasswörter benötigen mindestens 16 Zeichen.
- Verwende möglichst lange, leicht merkbare Passphrasen – zum Beispiel ganze Sätze oder deren Abkürzungen.

Beispiele:
„Heute beginnt mein Dienst um 7 Uhr.“ → HebemeDu-7U.
„Am Freitag trinke ich keinen Kaffee.“ → AmfrTrIckK1!

Gross- und Kleinbuchstaben, Zahlen und Sonderzeichen erhöhen die Sicherheit, aber wichtiger als Komplexität ist die Länge und Unvorhersehbarkeit.

Vermeide unbedingt:

- Namen, Geburtsdaten oder Benutzerkennungen
- Zahlenfolgen wie 1234 oder Tastaturmuster wie qwertz
- Ableitungen bestehender Passwörter wie Passwort2024, Passwort2025

Passwortwechsel

- Du kannst dein Passwort jederzeit selbst ändern.
- Dein neues Passwort darf nicht einfach aus dem alten ableitbar sein.
- Die Wiederverwendung alter Passwörter ist nicht möglich – das System verhindert dies automatisch über die Passwort-Historie.

Weitere hilfreiche Informationen werden im Merkblatt Passwörter beschrieben.

6.3 Zugangsdaten von Web-Portalen und sonstigen Diensten

Zugangsdaten zu externen Webportalen oder Onlinediensten, wie z. B. Gesundheitsplattformen oder Fachportalen, musst du sicher verwalten.
Du darfst keine Zugangsdaten in E-Mails, Dateien oder handschriftlich auf dem Schreibtisch aufbewahren.

7 Netzwerk und Kommunikation

Wenn du über fmi-fremde Netze arbeitest – z. B. über ein öffentliches WLAN oder einen privaten Internetanschluss –, darfst du dies nur über eine durchgängig verschlüsselte Verbindung tun.

- Die Verschlüsselung erfolgt über einen VPN-Zugang, der von der Informatik zur Verfügung gestellt wird.
- Diesen VPN-Zugang kannst du im IAM-Shop beantragen

7.1 Nutzung von Diensten

Die Freigabe von IT-Diensten erfolgt in Abstimmung mit den Fachbereichen unter Einhaltung von Sicherheits-, Datenschutz- und Betriebsanforderungen. Der Bereich Informatik und Digitalisierung ist für die Bereitstellung und den Betrieb dieser Dienste verantwortlich.
Du darfst nur freigegebene Dienste verwenden. Was nicht freigegeben ist, wird – wo möglich – systemseitig gesperrt. Falls es für einen bestimmten Dienst noch keine Regelung gibt, frag zuerst beim Bereich Informatik und Digitalisierung nach, bevor du ihn nutzt.
Auch Programme aus dem Internet oder Webdienste wie Cloud-Anwendungen darfst du nicht einfach selbst installieren oder verwenden. Wenn du zusätzliche Tools für deine Arbeit brauchst, kannst du einen Antrag stellen – geprüft wird dabei, ob das Tool technisch, rechtlich und organisatorisch zu Spitäler fmi AG passt.

7.2 Nutzung des internen Netzwerks

IKT-Mittel von Kunden, externen Mitarbeitenden oder nicht zugelassene private Geräte von Mitarbeitenden der Spitäler fmi AG dürfen nicht an das interne Netz oder an Systeme der Spitäler fmi AG angeschlossen werden. Für solche Geräte stellt der Bereich Informatik und Digitalisierung ein separates Gäste-WLAN zur Verfügung
Ausnahmen sind nur mit ausdrücklicher Bewilligung durch den Bereich Informatik und Digitalisierung erlaubt.

7.3 Nutzung des Internets

Du darfst das Internet nur mit einem durch den Bereich Informatik und Digitalisierung freigegebenen oder vorinstallierten Browser nutzen. Dabei müssen die vorgesehenen Sicherheitseinstellungen verwendet werden.
Wenn du mit einem IKT-Mittel der Spitäler fmi AG arbeitest, das mit dem internen Netzwerk verbunden ist, darfst du das Internet ausschliesslich für geschäftliche nutzen. Eine private Nutzung ist nur in geringem Umfang erlaubt. Filme, Videos oder TV-Streams zur Unterhaltung sind nicht gestattet, dies gilt auch bei der Nutzung über den Fernzugriff.
Du bist dir bewusst, dass du beim Surfen mit geschäftlichen Geräten die Spitäler fmi AG nach aussen repräsentierst. Entscheidend ist dabei nicht dein persönliches Empfinden, sondern die Wirkung auf Dritte.

Verhaltensregeln bei der Internetnutzung

- Keine Webseiten aufrufen, die dem Image der Spitäler fmi AG schaden (z. B. mit pornografischen, extremistischen, rassistischen oder rechtswidrigen Inhalten).
- Keine Aktivitäten, die materiellen oder immateriellen Schaden verursachen.
- Urheberrechte respektieren – Inhalte nur mit ausdrücklicher Erlaubnis nutzen.
- Privatsphäre schützen, besonders im Umgang mit Personendaten.
- Verwende dein geschäftliches Login nie für private Internetdienste (z. B. Webshops, Newsletter).
- Geschäftsrelevante Infos aus dem Internet sind kritisch auf Echtheit, Aktualität und Glaubwürdigkeit zu prüfen.

Besondere Vorgaben für Internet-Dienste

- Teile keine klassifizierten Informationen in Chats oder sozialen Netzwerken
- Nutze nur durch den Bereich Informatik und Digitalisierung freigegebene Cloud-Dienste und Onlinespeicher

Der Bereich Informatik und Digitalisierung kann den Zugriff auf bestimmte Webseiten oder Dienste jederzeit sperren. Aus Sicherheitsgründen oder bei drohender Überlastung des Netzwerks können Einschränkungen auch kurzfristig und ohne Vorankündigung erfolgen. In allen anderen Fällen wird die Einschränkung rechtzeitig angekündigt.

7.3.1 Social Media

7.3.1.1 Nutzung von sozialen Medien

- Während der Arbeitszeit ist die Nutzung sozialer Medien auf arbeitsbezogene Inhalte und Öffentlichkeitsarbeit beschränkt.
- Welche Social-Media-Kanäle geschäftlich genutzt werden dürfen, wird durch die Spitäler fmi AG festgelegt
- Veröffentliche keine internen oder vertraulichen Informationen über die Spitäler fmi AG, Mitarbeitende oder Patientinnen und Patienten
- Daten über Mitarbeitende dürfen nur veröffentlicht werden, wenn diese ausdrücklich zugestimmt haben und nur unter Einhaltung der Datenschutzvorgaben

7.3.1.2 Sicherheit in sozialen Medien

- Soziale Medien bergen erhebliche Sicherheitsrisiken, oft unbeabsichtigt durch eigene Beiträge
- Vermeide Fotos vom Arbeitsplatz, selbst harmlose Details (z. B. sichtbare Kundendaten auf Ordnern) können problematisch sein
- Keine Infos über Ferien, Team-Events oder Abwesenheiten posten, solche Hinweise werden gezielt für Angriffe genutzt
- Denk daran: Jede noch so unwichtig scheinende Information kann für jemanden wertvoll sein

7.3.2 Künstliche Intelligenz

Der Einsatz von KI-Systemen, zum Beispiel Chatbots, Bilderkennungsdiensten oder Textgeneratoren, ist an rechtliche, datenschutzrechtliche und sicherheitsrelevante Vorgaben gebunden, insbesondere im Gesundheitswesen.
Die IT stellt sicher, dass nur solche KI-Dienste genutzt werden, welche diesen Anforderungen entsprechen. Eine Nutzung ist daher nur zulässig, wenn sie vorgängig durch den Bereich Informatik und Digitalisierung genehmigt wurde.
Eigene Installationen oder frei verfügbare Tools aus dem Internet, zum Beispiel als App oder Browser-Erweiterung, dürfen nicht auf IKT-Mitteln der Spitäler fmi AG verwendet werden.

Gib keine vertraulichen Informationen in KI-Systeme ein. Dazu gehören insbesondere Patientendaten sowie interne oder schützenswerte Dokumente. Auch das Hochladen sensibler Dateien auf öffentlich zugängliche Webtools (z. B. ChatGPT) ist nicht erlaubt.
Wenn du Inhalte nutzt, die mit Hilfe von KI erstellt wurden, prüfe diese immer sorgfältig:

- Stimmen die Informationen?
- Sind sie aktuell?
- Woher stammen sie?

KI-Ergebnisse, insbesondere bei medizinischen, rechtlichen oder sicherheitsrelevanten Entscheidungen, dürfen nicht ungeprüft übernommen werden.

Wenn du ein neues KI-Tool einsetzen möchtest oder einen speziellen Anwendungsfall hast, kannst du einen Antrag stellen. Der Bereich Informatik und Digitalisierung prüft dann, ob der Einsatz technisch, rechtlich und organisatorisch möglich ist.

Zur Sicherheit kann der Zugang zu bestimmten KI-Diensten jederzeit technisch eingeschränkt oder gesperrt werden.

7.4 Fernzugriffe
Für den Fernzugriff auf Daten und Systeme der Spitäler fmi AG dürfen nur vom Bereich Informatik und Digitalisierung freigegebene Werkzeuge verwendet werden. Die Zugriffsvergabe erfolgt nach dem Need-to-know-Prinzip und unter Berücksichtigung des eingesetzten Geräts.
Möchtest du aus dem Ausland auf Systeme von Spitäler fmi AG zugreifen, brauchst du vorgängig eine spezielle Bewilligung.
Die Notwendigkeit eines Fernzugriffs wird durch den Informationssicherheitsverantwortlichen bzw. dem Informationssicherheitsbeauftragten gemeinsam mit dem Leiter Informatik und Digitalisierung und in Rücksprache mit der vorgesetzten Stelle geprüft und entsprechend freigegeben.
Geräte, mit welchen auf vertrauliche oder besonders schützenswerte Personendaten zugegriffen werden kann, dürfen nur mit ausdrücklicher Bewilligung über die Schweizer Landesgrenze hinaus mitgenommen werden.

Wenn du den Fernzugriff nutzt, bist du verpflichtet, die Vorgaben der Spitäler fmi AG zur Informationssicherheit einzuhalten. Zudem musst du eine entsprechende Geheimhaltungsvereinbarung unterzeichnen. Solltest du beim Fernzugriff Störungen, Unregelmässigkeiten oder Hinweise auf unberechtigte Zugriffe feststellen oder kommt es zum Verlust oder Diebstahl eines entsprechenden Geräts, musst du den Service Desk umgehend informieren. Die Behebung von Problemen darf ausschliesslich durch den Bereich Informatik und Digitalisierung erfolgen.

7.5 Funknetze
Für die Sicherheit beim Arbeiten im Netzwerk der Spitäler fmi AG gelten folgende Punkte:
- Die Verbindung mit dem WLAN der Spitäler fmi AG ist auf Gerätschaften der Spitäler fmi AG beschränkt
- Nicht durch den Bereich Informatik und Digitalisierung freigegebene Geräte oder auch private Geräte dürfen nur im Gäste Netzwerk verbunden werden und es dürfen keine Geschäftsdaten mit diesen Geräten bearbeitet werden

Arbeitest du von unterwegs oder von zuhause mit einem Gerät, zum Beispiel ein Laptop, der Spitäler fmi AG so gilt folgendes:
- Verbinde dich grundsätzlich nur mit vertrauenswürdigen und gesicherten WLAN-Netzen, die Nutzung von öffentlichen und ungeschützten Netzwerken ist zu vermeiden
- Damit du auf Daten der Spitäler fmi AG zugreifen kannst, ist eine VPN Verbindung notwendig. Diese VPN Verbindung wird grundsätzlich nur auf Firmengeräten der Spitäler fmi AG genehmigt, für die Arbeit mit Geräten, welche nicht durch die Spitäler fmi AG verwaltet werden, kann mit der Informatik eine entsprechende Lösung gesucht werden

8 Protokollierung

8.1 Persönlichkeitsrechte der Mitarbeitenden
Die Spitäler fmi AG wahrt die Privatsphäre ihrer Mitarbeitenden am Arbeitsplatz. Gleichzeitig ist die Protokollierung bestimmter Nutzungsdaten für den sicheren, rechtmässigen und stabilen Betrieb der IT-Systeme notwendig.

Protokolle werden ausfolgenden Gründen erstellt:
- Sicherstellung der Informations-, Daten- und Systemsicherheit
- Analyse und Behebung technischer Fehler
- Optimierung von Systemen und Prozessen

Sämtliche Verkehrs- und Logdaten (z. B. gewählte Telefonnummern, Internetprotokolle, E-Mail-Metadaten, übertragenes Datenvolumen) werden vollautomatisch aufgezeichnet und anonymisiert zu statistischen Zwecken ausgewertet. Dabei wird nur festgehalten, wann welche Verbindungen aufgebaut wurden und nicht deren Inhalte.

Eine personenbezogene Auswertung erfolgt nur, wenn:

- technische Probleme eine detaillierte Analyse erfordern oder
- ein begründeter Verdacht auf Missbrauch vorliegt wie etwa bei Verstössen gegen verbindliche Vorgaben.

In einem solchen Fall informiert die Leitung Informatik und Digitalisierung die Direktion der Spitäler fmi AG, welche über das weitere Vorgehen entscheidet. Die Auswertung wird durch eine von der Direktion bestimmte Fachperson aus der Informatik oder durch eine externe Stelle vorgenommen.

- Diese Auswertung unterliegt der Schweigepflicht
- Mitarbeitende, gegen welche sich ein Verdacht richtet, werden in das Verfahren einbezogen

9 Ausserordentlicher Zugriff (Notfallzugriff)

Wenn du abwesend oder nicht erreichbar bist und gleichzeitig dringend auf geschäftsrelevante Daten in deinem persönlichen Arbeitsbereich zugegriffen werden muss, kommt der Notfallzugriff zur Anwendung.
Der Notfallzugriff steht der Spitäler fmi AG in folgendem Umfang zu:

- Zugriff auf dein persönliches E-Mail-Postfach
- Dies kann nötig sein, wenn du keine Stellvertretung eingerichtet oder die Abwesenheitsmeldung nicht oder falsch konfiguriert hast oder wenn geschäftlich wichtige E-Mails sonst nicht zugänglich sind
- Zugriff auf lokal gespeicherte Informationen
- Das kann erforderlich sein, wenn wichtige Geschäftsdaten an nicht vorgesehenen Speicherorten abgelegt wurden, z. B. lokal auf dem Laufwerk C:\, und dadurch für andere nicht zugänglich sind.

9.1 Ablauf

Bei jedem Notfallzugriff ist folgender Ablauf zwingend einzuhalten:

1 Kontaktaufnahme mit der betroffenen Person
  Der Linienvorgesetzte versucht vorgängig, die betroffene Mitarbeiterin oder den betroffenen Mitarbeiter telefonisch zu erreichen und ein mündliches Einverständnis einzuholen.
2 Einwilligung durch die Personalabteilung
  Ist die betroffene Person nicht erreichbar, kann die Personalabteilung auf Antrag des Vorgesetzten die Einwilligung zum Zugriff erteilen.
3 Zugriff unter Aufsicht
  Der Zugriff erfolgt durch den Linienvorgesetzten im Beisein des zuständigen Systemadministrators, welcher die notwendigen Aktionen vornimmt, insbesondere:
  a) Konfiguration einer Stellvertretung oder Aktivierung der Abwesenheitsmeldung
  b) Verschiebung von E-Mails oder Dateien an den vorgesehenen Speicherort
4 Dokumentation
  Der Notfallzugriff ist zu dokumentieren und gemeinsam mit der erteilten Einwilligung im Personaldossier der betroffenen Person abzulegen.

Information an die betroffene Person
Die betroffene Mitarbeiterin oder der betroffene Mitarbeiter ist schriftlich über den erfolgten Zugriff zu informieren.

10 Austritt aus dem Unternehmen

Beim Austritt aus der Spitäler fmi AG oder dem Ende eines Vertragsverhältnisses musst du alle geschäftlichen Unterlagen und überlassenen IKT-Mittel unaufgefordert zurückgeben, einschliesslich allfälliger Geräte für den Fernzugriff. Das Zurückbehalten von Kopien oder Sicherungen ist nicht erlaubt.
Geschäftsrelevante Dokumente, E-Mails oder Daten dürfen nicht eigenmächtig gelöscht werden.

Du hast die Möglichkeit, im Beisein einer Person aus der Informatik persönliche E-Mails oder private Daten auf ein eigenes Speichermedium zu übertragen und anschliessend manuell aus den Systemen der Spitäler fmi AG zu löschen.
Machst du von dieser Möglichkeit keinen Gebrauch, gilt: Die verbleibenden Daten werden als geschäftsrelevant betrachtet und dürfen entsprechend bearbeitet werden.

Für Daten in Backups gelten die Regelungen gemäss Ziffer 4.4.2 und 5.1.
Mit dem Ablauf deines letzten Arbeitstags werden sämtliche Zugriffsrechte deaktiviert.

10.1 Geschäftskontrolle

Aus geschäftlichem Interesse darf die Spitäler fmi AG auf E-Mail-Postfächer und geschäftliche Inhalte wie Kalender oder Kundenanfragen zugreifen, auch über deinen Austritt hinaus. Das heisst: die Spitäler fmi AG ist berechtigt, dein E-Mail-Postfach einzusehen, wenn dies für den Geschäftsbetrieb notwendig ist.

Deine E-Mail-Adresse wird nach deinem Austritt deaktiviert. Personen, welche dir weiterhin schreiben, erhalten eine automatische Rückmeldung mit dem Hinweis, dass das Postfach nicht mehr aktiv betreut wird und an wen sie sich stattdessen wenden sollen.

E-Mails, die nach deinem Austritt eingehen und offensichtlich privater Natur sind, werden nicht gelesen.

11 Kontrolle

Deine vorgesetzte Stelle ist berechtigt, die Einhaltung dieser Weisung zu überprüfen und bei Bedarf durchzusetzen. Zusätzlich können Kontrollen durch den Bereich Informatik und Digitalisierung sowie durch den Informationssicherheitsbeauftragten durchgeführt werden.

Wenn bei einer Kontrolle ein Missbrauch im Umgang mit Informatikmitteln festgestellt wird oder du diese Weisung missachtest oder verletzt, können die Spitäler fmi AG entsprechende Konsequenzen einleiten. Dazu gehören disziplinarische Massnahmen, arbeitsrechtliche Sanktionen oder, je nach Schwere des Falls, auch zivil- oder strafrechtliche Schritte.

12 Glossar

Begrifflichkeit	Definition
Datenträger	Alle Medien, auf denen Daten zum Zwecke der Verarbeitung in einer durch maschinelle Hilfsmittel lesbaren und ausdeutbaren Form niedergelegt werden können
HIN	HIN ist eine Lösung, welche den Teilnehmern eine sichere Kommunikation, sichere Zusammenarbeit und einen sicheren Zugriff auf verschiedene Anwendungen ermöglicht
Integrität	Integrität bedeutet, dass es nicht möglich sein darf, Daten unerkannt bzw. unbemerkt zu ändern
ISO/IEC 2700x	Die Normreihe ISO 27000 enthält viele Teilnormen zum Thema Informationsicherheitsmanagement. Die zentrale Norm ist die ISO 27001. Sie besteht auf allgemeinen Anforderungen an «System zum Management der Informationssicherheit» (ISMS) im Hauptteil und einem umfangreichen Anhang A mit spezifischen Sicherheitsanforderungen
IKT	Abkürzung für Informations- und Kommunikationstechnik
IT	Informationstechnik, Abkürzung für den Bereich Informatik und Digitalisierung
Nachvollziehbarkeit	Nachvollziehbarkeit bedeutet, dass jegliche Änderungen im Zusammenhang mit Informationstechnik zugeordnet werden können und im Nachhinein nachweisbar sind
Need to know-Prinzip	Einem System oder einer Person wird nur der Zugang zu den Informationen gewährt, die sie zur Erfüllung ihrer Aufgaben benötigt (unterschiedliche Aufgaben oder Rollen bedeuten unterschiedliche Need-to-know-Informationen und damit unterschiedliche Zugangsprofile)
USB-Stick	Datenträger zur temporären Speicherung bzw. zum Austausch von Daten
Verfügbarkeit	Ist die Fähigkeit eines Systems, zu einem bestimmten Zeitpunkt oder während eines bestimmten Zeitintervalls eine geforderte Funktion unter gegebenen Bedingungen erfüllen zu können, vorausgesetzt, dass die erforderlichen Mittel bereitgestellt sind
Vertraulichkeit	Vertraulichkeit bedeutet, dass Daten nur von autorisiertem Personal eingesehen oder weitergegeben werden können. Wenn Sie Ihre Daten vertraulich behandeln möchten, müssen Sie klar definieren, wer wie darauf zugreifen kann