Konzept

Informationssicherheit

Informatik / Geschäftsleitung

Spitäler Frutigen Meiringen Interlaken AG

■ Dokumenteigenschaften

Änderungsdatum	27.01.2026
Gültig ab	Freigabe
Version	3.4
Ersetzt Version	
Verfasst durch	Daniel Michel (Redguard); Thomas Huber (CTO Spitäler fmi AG) Christian Fritz (Redguard); Artur Konowalczuk (Leiter Informatik und Digitalisierung Spitäler fmi AG)
Freigegeben durch	Geschäftsleitung xx.xx.xxxx
Prozessverantwortlich	Informationssicherheitsbeauftragte Stelle
Klassifizierung	intern

■ Dokumentenverlauf

Änderungsdatum	Version	Bearbeiter	Änderungen
11.12.2019	0.10	Redguard AG	Initialversion
13.01.2020	0.20	Redguard AG	Überarbeitung gemäss Inputs L. IT
14.01.2020	0.30	Redguard AG	Interner Review und Überarbeitung Redguard
15.01.2020	0.40	Redguard AG	Version an Leiter IT
02.03.2020	0.50	Redguard AG, Leiter Informatik	Überarbeitete Version gemäss Inputs Leiter Informatik
02.04.2020	0.60	Redguard AG	Version an Leiter Informatik
16.04.2020	0.62	Redguard AG	Überarbeitete Version an Datenschutzbeauftragten
29.04.2020	0.70	Redguard AG	Überarbeitete Version gemäss Inputs Freigebende
31.07.2020	0.90	Thomas Huber, CTO fmi	Anpassungen und neues Kapitel: „3. Vorgehen“
25.08.2020	0.91	Redguard AG	Review gemäss Input CTO
02.10.2020	1.0	Thomas Huber, CTO fmi	Korrekturen nach Input VR
11.10.2022	1.10	Artur Konowalczuk und Redguard AG	Workshop Review IS Konzept
17.10.2022	1.11	Artur Konowalczuk und Redguard AG	Workshop Review IS Konzept
08.11.2022	1.12	Redguard AG	Anpassungen und Aktualisierungen
10.11.2022	1.13	Redguard AG	Vorschlag IS Organisation 2023
02.12.2022	1.14	Redguard AG	Anpassungen nach Besprechung mit A.Konowalczuk
09.01.2023	1.15	Redguard AG	Ergänzungen und Glossar
18.01.2023	1.16	Redguard AG	Ergänzungen und Anpassungen nach Feedback O.Wyss und A.Konowalczuk
25.01.2023	1.17	Redguard AG	Ergänzungen und Anpassungen nach Besprechung mit A.Konowalczuk
06.02.2023	2.0	Othmar Wyss	Review. Bereit für Genehmigung
09.05.2025	3.0	Stephanie Müller	Rollendefinition, Aktualisierung Dokument
22.05.2025	3.1	Marco Filli	Review und vorbereiten für Genehmigung
15.09.2025	3.2	Marco Filli	Entfernen Organigram nach Rückmeldung Review
19.11.2025	3.3	Marco Filli	Überarbeiten nach Review durch Geschäftsleitungssitzung vom 27.10.2025

27.01.2026	3.4	Marco Filli	Überarbeiten nach Review durch Geschäftsleitungssitzung vom 26.01.2026

Inhaltsverzeichnis

1 Einleitung

Die Spitäler fmi AG bietet an ihren Standorten Frutigen, Meiringen und Interlaken eine qualitativ hochstehende medizinische Versorgung und einen 24-Stunden-Notfalldienst in Frutigen und Interlaken an. Als kompetenter Partner für alle Gesundheitsfragen bieten die Spitäler fmi AG ein umfassendes medizinisches Angebot für Einheimische und Touristen. Weitere medizinische Dienstleistungen stehen in Ergänzung dazu und sind auf die Bedürfnisse der Patienten abgestimmt.

1.1 Ziel und Zweck

Das Informationssicherheitskonzept der Spitäler fmi AG definiert die Basis des Informationssicherheitsmanagements und legt damit den Grundstein für ein gemeinsames Verständnis sowie für eine ganzheitliche und bedürfnisgerechte Adressierung der Informationssicherheit bei der Spitäler fmi AG. Für ihre Aufgabenerfüllung ist die Spitäler fmi AG von zuverlässig **funktionierenden Systemen** der Informations- und Kommunikationstechnologie abhängig. Ebenso muss die Sicherstellung der **Integrität und Vertraulichkeit der Daten** gewährleistet sein. Das Informationssicherheitskonzept schafft die Grundlage zur Informationssicherheit, indem sie das von den Spitäler fmi AG angestrebte Informationssicherheitsniveau, die Informationssicherheitsziele sowie die geeigneten Massnahmen definiert. Weiter beinhaltet das Konzept eine Beschreibung der Informationssicherheitsorganisation sowie deren Rollen und Aufgaben.

1.2 Geltungsbereich

Das Informationssicherheitskonzept und die damit zusammenhängenden Dokumente (siehe Kapitel 1.8 und 2.4) gelten für alle Standorte der Spitäler fmi AG. Die Vorgaben richten sich an alle Personen, die elektronische Daten verarbeiten. Sie richten sich auch an Mitarbeitende der Spitäler fmi AG mit befristeter Anstellung und an Dritte, die auf Grund besonderer vertraglicher Vereinbarungen Daten im Sinn der Vorgaben bearbeiten. Die Spitäler fmi AG stellt durch den Abschluss entsprechender Vereinbarungen sicher, dass mit der Bearbeitung von Informationen beauftragte Dritte die Vorgaben beachten und einhalten.

1.3 Geltungsbereich Lieferanten

Verträge, welche im Rahmen der gesamten Lieferkette der Spitäler fmi AG neu erstellt, verlängert oder verändert werden, müssen die Anforderungen dieses Konzepts erfüllen. Insbesondere sind folgende Punkte bei Verträgen mit Dritten einzuhalten:

- Bei Dienstleistungen durch Dritte sind die Anforderungen an die Informationssicherheit schriftlich zu vereinbaren und zu dokumentieren. Es sind alle Anforderungen zu adressieren, die sich mit dem Zugriff auf Informationen, deren Verarbeitung, Speicherung und Weitergabe sowie mit der Bereitstellung der entsprechenden Infrastrukturkomponenten befassen.
- Dienstleistende dürfen spezifisch erhobene Daten nur für ihren ursprünglich vorgesehenen Zweck verwenden und entsprechend ihrem Auftrag bearbeiten.
- Dienstleistende haben eine Informationspflicht bei allfälligen Verstössen, Datenschutzverletzungen, Sicherheitsvorfällen oder Sicherheitslücken.

1.4 Änderungen

Änderungen am Konzept Informationssicherheit können durch Geschäftsleitungsmitglieder, die Leitung Informatik, der Datenschutzverantwortlichen Person oder der Informationssicherheitsverantwortlichen Person beantragt werden. Änderungsanträge werden durch die Informationssicherheitsorganisation beurteilt und umgesetzt. Vorgenommene Änderungen werden der Geschäftsleitung zur Prüfung vorgelegt. Die Informationssicherheitsrichtlinie wird nach Inkrafttreten und nach jeder Änderung den Mitarbeitenden der Spitäler fmi AG zur Kenntnis gebracht.

1.5 Kontrolle

Das Informationssicherheitskonzept wird jährlich durch die Informationssicherheitsbeauftragte Person auf Zweckmässigkeit und Aktualität überprüft.

1.6 Ersatz von Dokumenten
Das vorliegende Dokument ersetzt keine bestehenden Dokumente.

1.7 Inkrafttreten
Das Informationssicherheitskonzept wird nach der Abnahme der Geschäftsleitung in Kraft gesetzt.
Die Geschäftsleitung bestätigt mit der Abnahme:

- Dass das vorliegende Informationssicherheitskonzept die Gewährleistung und Umsetzung von Datensicherheit und Datenschutz in der Spitäler fmi AG beschreibt.
- dass die in diesem Konzept Informationssicherheit beschriebenen Forderungen, Grundsätze und Verfahren für alle Beteiligten verbindlich sind.

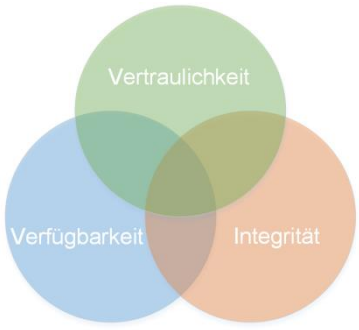
1.8 Mitgeltende Dokumente

Dokumentenname
Weisung_Informationssicherheit_MA-IT
Weisung über die Nutzung der Informatik- und Telekommunikationsmittel

2 Informationssicherheit

2.1 Zielsetzung der Informationssicherheit
Viele Funktionen und Aufgaben der Spitäler fmi AG werden durch Informations- und Kommunikationstechnologie (IKT) unterstützt. Der Schutz von IKT-Systemen und Daten spielt somit für die Spitäler fmi AG eine wichtige Rolle. Die gezielte und angemessene Adressierung der Informationssicherheit soll die Spitäler fmi AG wirkungsvoll vor potenziellen Schäden schützen.

Ganz konkret ist es das Ziel dieses Informationssicherheitskonzepts die **Vertraulichkeit**, **Verfügbarkeit** und **Integrität** der Daten sicherzustellen. Das Konzept gilt für sämtliche Bereiche, in welchen Daten elektronisch verarbeitet, transferiert oder gespeichert werden:



Vertraulichkeit
Im Rahmen der Informationsverarbeitung der Spitäler fmi AG muss sichergestellt sein, dass die Anforderungen an die Vertraulichkeit, geltenden Gesetzen und Normen entsprechen.

Verfügbarkeit
Die Informationsverarbeitung der Spitäler fmi AG ist so zu sichern, dass deren Ausfallzeiten toleriert werden können und die kritischen Geschäftsprozesse nicht negativ beeinträchtigt werden.

Integrität
Fehlfunktionen und Unregelmässigkeiten in der Informationsverarbeitung der Spitäler fmi AG dürfen nur in Ausnahmefällen auftreten, so dass die Richtigkeit, Unversehrtheit und Nachvollziehbarkeit der Daten und Informationen sichergestellt ist.

Ferner soll sichergestellt sein, dass die im Rahmen der Informationssicherheit getroffenen Massnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Wert der zu schützenden Informationen und IKT-Systeme stehen.
Das vorliegende Konzept Informationssicherheit orientiert sich an der Handlungsempfehlung von Kritis[1] (Schutz Kritischer Infrastrukturen) und NCSC[2]. Zur Definition, Umsetzung und Überwachung von Sicherheitsmassnahmen

[1] https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html
[2] https://www.ncsc.admin.ch/ncsc/de/home.html

wird ein Informations Sicherheits Management System (ISMS) aufgebaut. Das ISMS orientiert sich an den Standards ISO/IEC 27001:2017 und NIST Cybersecurity Framework[3].

2.2 Informationssicherheitsniveau

Das Informationssicherheitsniveau zeigt einerseits den Ist-Zustand der Informationssicherheit der Spitäler fmi AG und definiert andererseits den langfristig zu erreichenden Soll-Zustand. Zur Bestimmung des Ist- und Soll-Zustands des Informationssicherheitsniveaus der Spitäler fmi AG wird in Anlehnung an CMMI[4] ein Maturitätsmodell definiert (s. Anhang – Kapitel 4.1), mit welchem der Erfüllungsgrad der einzelnen ISO/IEC 27001:2017 Kapitel regelmässig (mindestens 1x pro Jahr) gemessen wird.

Initial wurde unter anderem durch Mitglieder der Geschäftsleitung, die Leitung Informatik und Digitalisierung, die Datenschutzverantwortliche Person sowie durch die verantwortliche Person für das Riskmanagement das langfristig zu erreichende Soll-Niveau pro Kapitel definiert. Pro Kapitel werden zudem jährlich die folgenden zwei Tätigkeiten durchgeführt:

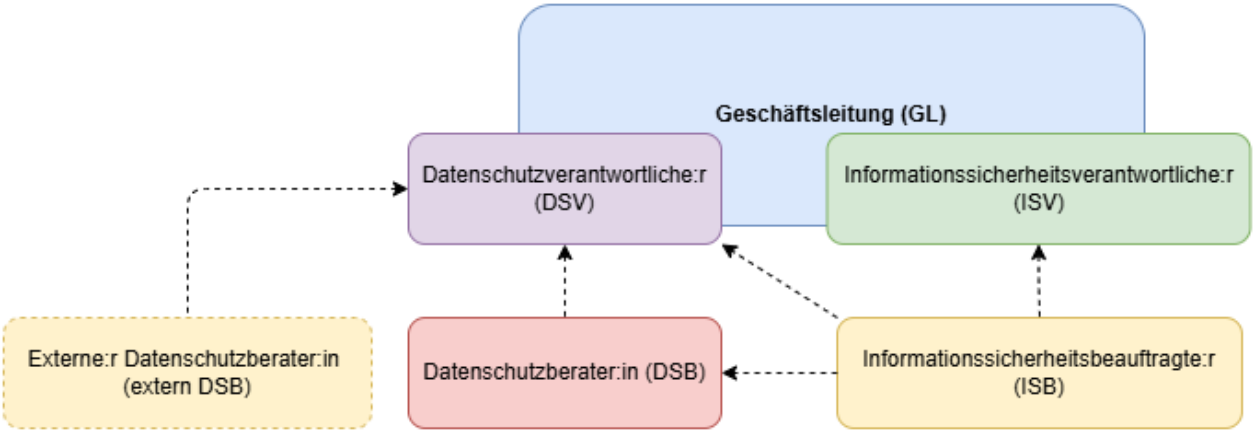
- identifizieren des aktuellen Ist-Niveaus
- prüfen – und falls nötig anpassen – des definierten Soll-Niveaus in Abhängigkeit mit der jeweils aktuell geltenden Bedrohungslage für die Spitäler fmi AG

Die jährliche Betrachtung des Ist- und Soll-Niveaus wird zugleich als Kontroll- und Planungsinstrument für Massnahmen zur kontinuierlichen Verbesserung der Informationssicherheit verwendet.

2.3 Informationssicherheitsorganisation

Die Informationssicherheitsorganisation ermöglicht es der Spitäler fmi AG das angestrebte Informationssicherheitsniveau zu erreichen und aufrecht zu erhalten.
Die Delegation von Aufgaben ist möglich, die Verantwortung kann nicht delegiert werden.
Bei den Spitäler fmi AG wurden folgende Rollen benannt:

- Datenschutzverantwortliche:r (DSV). Die Hauptverantwortung liegt bei der /dem Vorsitzenden GL (CEO) oder der Geschäftsleitung (GL)
- Datenschutzberater:in (DSB)
- Externe:r Datenschutzbeauftragte:r (externe:r DSB)
- Informationssicherheitsverantwortliche:r (ISV)
- Informationssicherheitsbeauftragte:r (ISB)



Die Grafik bildet die entsprechenden Kommunikationswege der Rollen ab

[3] https://www.nist.gov/cyberframework
[4] http://de.wikipedia.org/wiki/Capability_Maturity_Model_Integration

Rolle	Aufgabe	Beziehung
DSV (Datenschutzverantwortliche:r)	Strategisch verantwortlich – trägt die Gesamtverantwortung.	Teil der GL, z. B. CEO
DSB (Datenschutzberater:in)	Operative Schnittstelle zu Fachbereichen, Koordination.	Berichtet an DSV
DSB (externe Datenschutzbeauftragte:r)	Rechtliche Beratung, Kontrolle der Einhaltung (DSG, DSGVO).	Unabhängig, berichtet direkt an DSV, ist aber beratend tätig
ISV (Informationssicherheitsverantwortliche:r)	Strategische Verantwortung für das ISMS	Teil der GL, z.B. CISO
ISB (Informationssicherheitsbeauftragte:r)	Aufbau, Betrieb, Weiterentwicklung des ISMS	Berichtet an ISV, ggf. auch an DSK bei Überschneidungen respektive an RiskOwner

2.3.1 Verwaltungsrat (VR)

Der Verwaltungsrat trägt die oberste Verantwortung für die Informationssicherheit.
Der Verwaltungsrat:

- Verantwortet die Ausgestaltung einer angemessenen und wirkungsvollen Informationssicherheit und agiert als höchste Kontrollinstanz zur Sicherstellung von Massnahmen der Informationssicherheit.
- Fordert ein akkurates Lage- und Risikobild und definiert das erforderliche Maturitätsniveau sowie die damit einhergehende Risikobereitschaft.
- Kontrolliert den Fortschritt und die Umsetzung der Massnahmen zur Aufrechterhaltung der Informationssicherheit.
- Stellt sicher, dass Wirtschaftlichkeit sowie Mittel und Ressourcen für Informationssicherheit mit den festgelegten Zielen in Einklang stehen.

2.3.2 Geschäftsleitung (GL)

Die Geschäftsleitung ist verantwortlich für die Sicherstellung der finanziellen und personellen Mittel für die Umsetzung der Informationssicherheitspolitik. Die Geschäftsleitung schafft die zur Umsetzung der Informationssicherheit notwendigen Rahmenbedingungen.
Daraus ergeben sich die folgenden Aufgaben:

- Ernennung der ISV und Datenschutzverantwortlichen Personen
- Sicherstellung der Unabhängigkeit von ISV und DSV im Rahmen ihrer Funktionen
- Vorleben der Sicherheitskultur und Förderung der Sensibilisierung der Mitarbeitenden
- Regelmässige Information über Sicherheitslage, aktuelle Bedrohungen und Risiken
- Freigabe der Vorgabendokumente (Stufe Konzepte, Weisungen und Richtlinien gemäss Kapitel 2.4)
- Sicherstellung der Berichterstattung an den Verwaltungsrat

2.3.3 Informationssicherheitsverantwortliche:r

Die/der ISV rapportiert direkt an die Geschäftsleitung oder den CEO und ist für die Umsetzung der Informationssicherheit und deren Ziele verantwortlich. Dazu gehören insbesondere folgende Aufgaben:

- Erarbeitung einer auf der Geschäftsstrategie ausgerichteten Informationssicherheitsstrategie und Steuerung der Umsetzung
- Erarbeitung von Weisungen, Vorgaben und Standards, regelmässige Prüfung der konformen Umsetzung und Sicherstellung der kontinuierlichen Optimierung
- Sicherstellung der jährlichen Beurteilung des Informationssicherheitsniveaus
- Sicherstellung, dass Informationssicherheitsereignisse erkannt und bearbeitet werden
- Bewertung der Verträglichkeit von Vorhaben in Bezug auf die Informationssicherheit
- Förderung der Sicherheitskultur
- Regelmässige Berichtserstattung an den DSV und die allfälligen Risikoeigner
- Koordination der Aufgaben innerhalb der Informationssicherheitsorganisation

2.3.4 Informationssicherheitsbeautragte:r (ISB intern)

Der / die ISB rapportiert an den ISV, respektive an die Risikoeigner und den/die DSV und nimmt folgende Aufgaben und Tätigkeiten wahr.

- Unterstützung ISV in ihren/seinen Aufgaben und Tätigkeiten
- Ausarbeitung und Anpassung des Informationssicherheits-Frameworks
- Begleitung und Beurteilung von IKT-Projekten in Bezug auf sicherheitsrelevante Aspekte
- Definition von Sicherheitszielen und -anforderungen für IKT-Systeme und Anwendungen
- Übernahme der Funktion als Ansprechpartner für sicherheitsrelevante Fragestellungen
- Stärkung des Bewusstseins (Awareness) der Mitarbeitenden der Spitäler fmi AG hinsichtlich Informationssicherheit

2.3.5 Datenschutzverantwortung

Datenschutz hat bei den Spitäler fmi AG einen hohen Stellenwert. Um den Schutz der im Rahmen der Geschäftstätigkeit bearbeiteten und gespeicherten Daten und Informationen sicherzustellen, sind in den Spitäler fmi AG verschiedene Rollen im Datenschutz definiert. Beim Datenschutz geht es nicht nur um den Schutz von allgemeinen Daten vor Schäden, sondern um den Schutz personenbezogener Daten vor Missbrauch. Geschützt werden muss dabei die Privatsphäre bzw. die Anonymität muss gewahrt bleiben. Datenschutz verlangt über die Datensicherheit hinaus den Ausschluss des Zugangs zu Daten durch unbefugte Dritte. Folgende Aufgaben und Tätigkeiten liegen in der Verantwortung der Datenschutzverantwortlichen Person:

- Hauptverantwortung für die Einhaltung der geltenden Datenschutzbestimmungen
- Sicherstellung einer angemessenen Organisation und Steuerung des Datenschutzes innerhalb der Spitäler fmi AG
- Festlegung von Rollen, Zuständigkeiten und Prozessen im Datenschutz
- Sicherstellung, dass für Anwendungen und Datensammlungen geeignete Informations- und Auskunftsstellen definiert sind
- Sicherstellung der datenschutzkonformen Bearbeitung personenbezogener Daten über den gesamten Lebenszyklus (insbesondere Bearbeitung, Bekanntgabe, Archivierung und Löschung)
- Sicherstellung der Wahrnehmung der Rechte betroffener Personen (insbesondere Auskunfts-, Berichtigungs- und Löschbegehren)
- Verantwortung für die Etablierung und Durchsetzung von Sensibilisierungs- und Schulungsmassnahmen im Bereich Datenschutz
- Sicherstellung der datenschutzkonformen Planung und Umsetzung von IT-Projekten sowie organisatorischen Vorhaben
- Verantwortung für die Überwachung der Einhaltung der datenschutzrechtlichen Vorgaben sowie der internen Weisungen der Spitäler fmi AG
- Regelmässige Berichterstattung an die Geschäftsleitung über den Stand des Datenschutzes, relevante Risiken und notwendige Massnahmen

2.3.6 Datenschutzberater:in

- Mitglied der Arbeitsgruppe Datenschutz, Sitzungsvorbereitung und Sitzungsleitung
- Regelung der Massnahmen für den Datenschutz und deren Kontrolle sowie Verantwortung für die Dokumentation der Schutzvorkehrungen
- Mitverantwortung für die Erfüllung der Datenschutzbestimmungen
- Informationsstelle für die im Verantwortungsbereich liegenden Anwendungen und Datensammlungen
- Mitverantwortung für die Bearbeitung (inklusive Bekannt- und Weitergabe), Archivierung oder Vernichtung der im Verantwortungsbereich liegenden Daten
- Mitverantwortung für die Sensibilisierung der Mitarbeitenden bezüglich Datenschutzes
- Beratung der Mitarbeitenden, Fachbereiche und Management in Fragen des Datenschutzes
- Ansprechperson für Betroffene (Auskunfts- und Löschbegehren)
- Berichten an die Arbeitsgruppe Datenschutz über den Stand des Datenschutzes
- Verantwortung für die Überwachung der Einhaltung des Datenschutzes und der Vorgaben der Spitäler fmi AG
- Begleitung und Beurteilung von IT-Projekten in Bezug auf datenschutzrelevante Aspekte
- Kontaktperson zur kantonalen Datenschutzaufsichtsstelle (DSA). Die Kommunikation mit der kantonalen Datenaufsichtstelle (DSA) läuft über die Direktion

2.3.7 Externe:r Datenschutzbeauftrage:r (DSB)

- Direkte Ansprechperson für Datenschutzberater:in in Datenschutzrechtlichen Fragen
- Erfüllung der gesetzlichen Anforderungen an die Tätigkeit eines DSB gemäss Art. 12b VDSG Kontrolle der Datenbearbeitung, mindestens jährlich und vor Ort
- Stichprobenweise Kontrolle der Einhaltung des Datenschutzes auf Basis des Inventars der Datensammlungen/Verarbeitungsverzeichnisses
- Führung und mindesten jährliche Aktualisierung des Inventars/Verarbeitungsverzeichnisses
- Beratung in datenschutzrechtlichen Themen
- Rapportierung gegenüber leitendem Organ
- Durchführung von Risikoanalysen im Bereich Datenschutz
- Überwachung der Schulungen und Kommunikationsmassnahmen im Bereich Datenschutz
- Erstellung resp. Aktualisierung interner Vorgaben im Bereich Datenschutz
- Begleiten und Beurteilung von IT-Projekten in Bezug auf datenschutzrelevante Aspekte
- Mitglied der Arbeitsgruppe Datenschutz erweitert (alle zwei Monate)
  Rapportiert mindestens Jährlich direkt and die GL, respektive den DSV

2.3.8 Umsetzung der Informationssicherheitsorganisation

Die Rollenträger müssen über das erforderliche Fachwissen verfügen und sich weiterbilden. Der Beizug von externem Fachwissen wird bei Bedarf durchgeführt.

Die Umsetzung wird durch folgende Gremien sichergestellt:

Arbeitsgruppe «Datenschutz Datensicherheit DSDS»

- Leitung
  - DSB
- Mitglieder
  - ISV
  - DSB (Datenschutzberater:in
  - QM (Leitung Qualitätsmanagement)
  - ISB
- Frequenz
  - monatlich / 10-12-mal jährlich
- Fokus
  - Datenschutz
  - Datensicherheit

Arbeitsgruppe DSDS inkl. Swiss Infosec

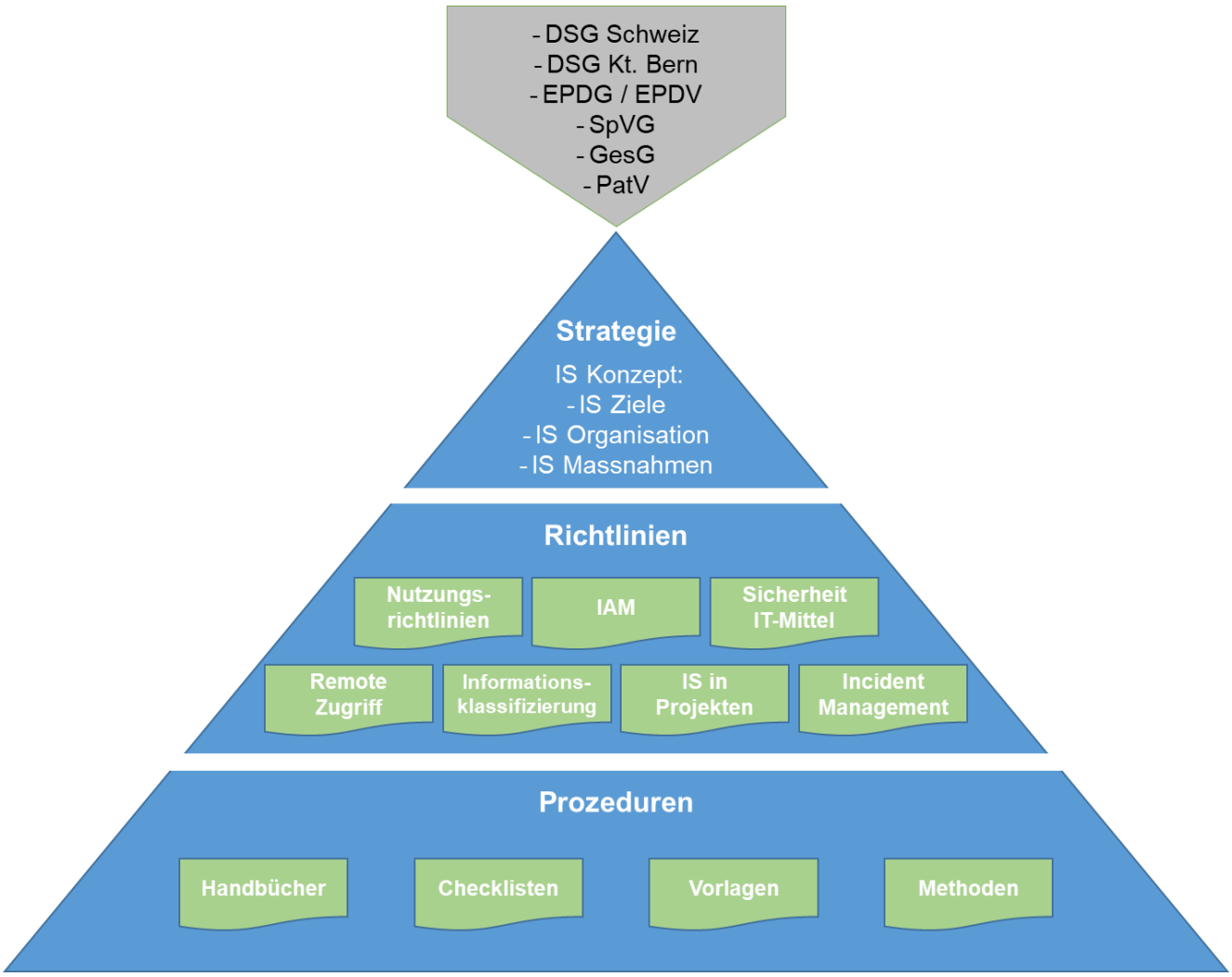
- Leitung
  - DSB
- Mitglieder
  - ISV
  - DSB extern
  - DSB
  - ISB
  - QM
- Frequenz zweimonatlich
- Fokus
  - Datenschutz
  - Datensicherheit

Arbeitsgruppe «Informationssicherheit»

- Leiter
  - ISV
- Mitglieder
  - ISV
  - ISB
  - Externer ISB/CISO
- Frequenz
  - Viermonatlich / 3x pro Jahr
- Fokus
  - Informationssicherheit
  - Risikomanagement (bezüglich Informationssicherheit)
  - Info GL / VR

2.4 Vorgaben und Richtlinienlandschaft

Die folgende Abbildung zeigt die Vorgaben und Richtlinienlandschaft der Spitäler fmi AG in Bezug auf die Informationssicherheit und deren Einordnung.



Die einzelnen Elemente der Vorgaben und Richtlinienlandschaft werden in der folgenden Tabelle beschrieben:

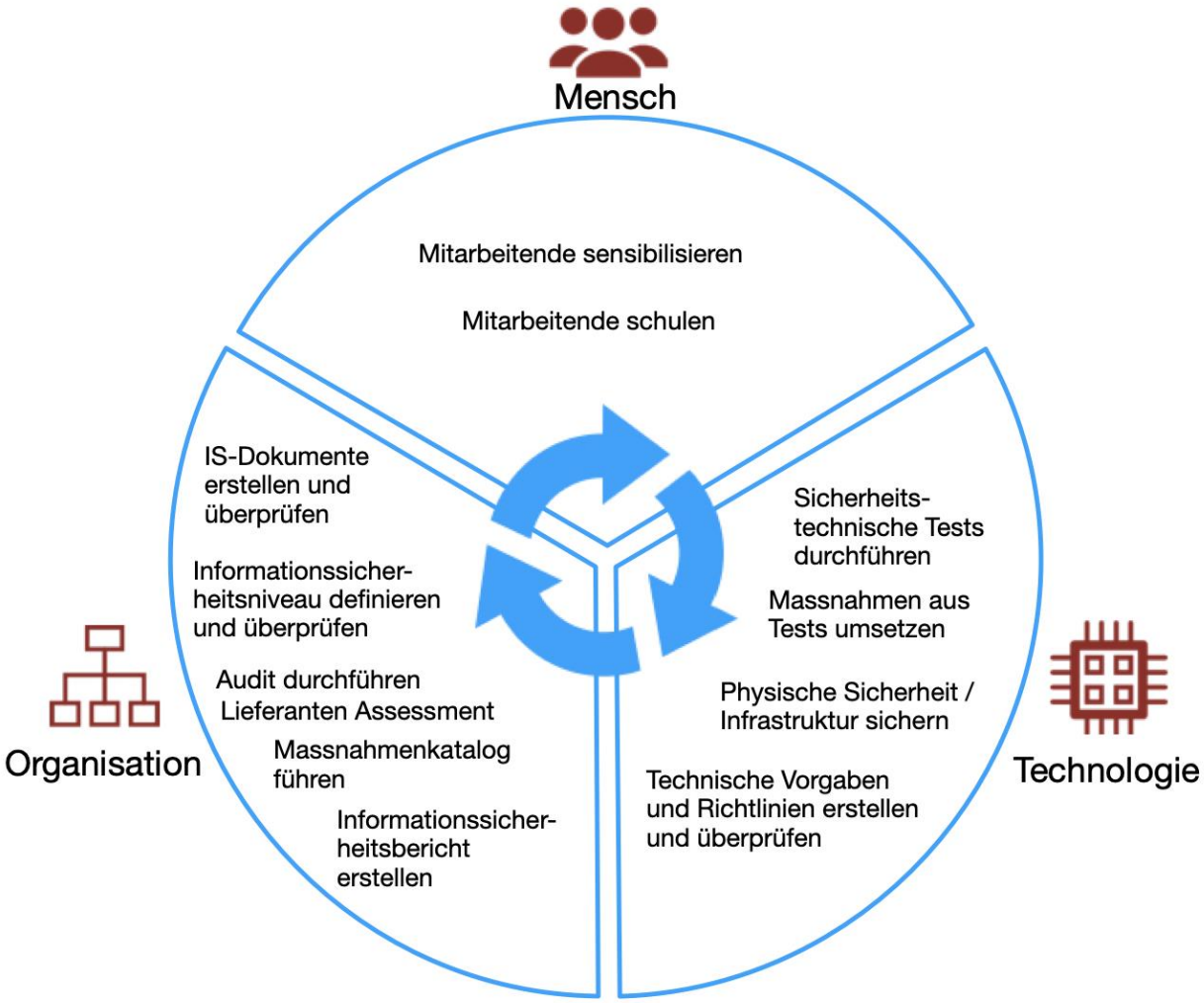
ID	Bezeichnung	Beschreibung
1	Gesetze / Normen	Es muss sichergestellt werden, dass das Informationssicherheitskonzept, die Richtlinien und Prozeduren den relevanten Gesetzen und Normen entsprechen. Diese sind unter anderem: ▪ Bundesgesetz über den Datenschutz (DSG / SR 235.1) ▪ nDSG / VDSG ab 09 2023 ▪ Kantonales Datenschutzgesetz (KDSG / 152.04) ▪ Bundesgesetz/-verordnung elektronisches Patientendossier (EPDG, EPDV / SR 816.1, SR 816.11) ▪ Spitalversorgungsgesetz (SpVG / 812.11) ▪ Gesundheitsgesetz (GesG / 811.01) ▪ Patientenrechtsverordnung (PatV / 811.011) ▪ Medizinprodukteverordnung (MepV / 812.213) ▪ Berufs- und Arztgeheimnis (Art. 321 StGB) ▪ KAIO-Weisung ICSGW (Kantonale Architektur und Informationssicherheits-Governance Weisung)

ID	Bezeichnung	Beschreibung
		▪ Kantonale Strategie Informationssicherheit Bern (KISB) ▪ Kantonales Gesundheitsgesetz (KGesG / 811.1 BE) ▪ Richtlinie zur Bearbeitung von Gesundheitsdaten im Kanton Bern (KDSG-Handreichung)
2	Strategie	Das Informationssicherheitskonzept (vorliegendes Dokument) definiert die Basis des Informationssicherheitsmanagements und legt damit den Grundstein für ein gemeinsames Verständnis und die fortlaufende Verbesserung des zugehörigen Regelwerks (Strategie / Richtlinien / Prozeduren). Das Informationssicherheitskonzept richtet sich dabei an den Rahmenbedingungen und Leitplanken der Spitäler fmi AG aus.
3	Richtlinien	Richtlinien übersetzen die Zielsetzung des Informationssicherheitskonzepts in konkrete und messbare Informationssicherheitsanforderungen. Richtlinien adressieren unter anderem folgende Themen im Rahmen der Informationssicherheit: ▪ Verantwortlichkeiten ▪ Management von Informationssicherheitsvorfällen ▪ Informationssicherheit in Projekten ▪ Klassifizierung und Handhabung von Daten ▪ E-Mail und Internet ▪ Handhabung IKT-Mitteln ▪ Endgeräteschutz ▪ Identifizierung, Authentifizierung und Autorisierung ▪ Netzwerke und Kommunikation ▪ Fernzugriffe
4	Prozeduren	Die Prozeduren stellen kurze und prägnante verbindliche Anweisungen und Hilfsmittel für die Mitarbeitenden der Spitäler fmi AG dar. Es werden dabei folgende drei Prozedurarten unterschieden: ▪ Handbücher sind Hilfsmittel, welche auf den sicheren Umgang und die sichere Nutzung von IKT-Mittel hinweisen. (Bsp. «Sicherer Umgang mit Passwörtern», «E-Mail Nutzung», «Internet Nutzung», «Sicherer Umgang mit mobilen Geräten») ▪ Checklisten sind verbindliche Anweisungen für die Mitarbeiter. Die Checklisten sollen sicherstellen, dass in bestimmten Bereichen und Abläufen ein definierter Standard eingehalten wird. (Bsp. «Checkliste Härtung Windows Server», «Mitarbeitende Ein- und Austrittsformular») ▪ Vorlagen sind Hilfsmittel; in der Regel handelt es sich um Dokumentationsvorlagen o. Templates. (Bsp. «Systemdokumentationsvorlage») ▪ Methoden schliesslich sind Hilfsmittel für das Vorgehen in Projekten

2.5 Aktionsbereiche

Die Ablauforganisation der Informationssicherheit der Spitäler fmi AG orientiert sich an den Aktionsbereichen Mensch, Technologie und Organisation.

Die Informationssicherheitsablauforganisation unterstützt die kontinuierliche Steigerung des Informationssicherheitsniveaus in Form eines iterativen Prozesses und zeigt, in welchem Aktionsbereich Schritte ausgeführt werden.



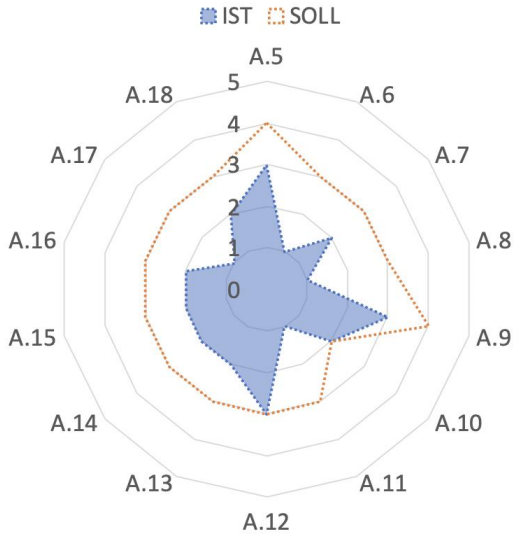
2.6 Schutzziele und Massnahmenumsetzung

Alle Daten und Informationen innerhalb der IKT-Infrastruktur und der Umsysteme der Spitäler fmi AG sowie alle analogen Daten müssen gemäss den gesetzlichen Vorgaben und Anforderungen respektive den Vorgaben und der Richtlinienlandschaft der Spitäler fmi AG geschützt werden.
Dies ist unter Berücksichtigung eines verhältnismässigen Einsatzes von Informatikmitteln, Personal und anderer Ressourcen risikobasiert zu bewerkstelligen.
Es gilt einen dem Schutzbedarf angemessenen Sicherheitsstand innerhalb der fmi zu erreichen und zu halten, sowie dabei die Wirtschaftlichkeitsfaktoren der Spitäler fmi AG zu gewährleisten.
Für die Umsetzung, Aufrechterhaltung und Weiterentwicklung der Massnahmen, die sich aus diesem Konzept und den dazugehörigen Regelwerken ergeben, sind ausreichend personelle und materielle Mittel zur Verfügung zu stellen.
Massnahmen, die sich aus diesem Konzept und den dazugehörigen Standards ableiten lassen, werden risiko-basiert priorisiert, terminiert und umgesetzt.

3 Anhang

3.1 Maturitätsniveau

Im Folgenden ist die initiale Bestimmung des Ist- und Soll-Zustands aus der erstmaligen Durchführung vom April 2019 dargestellt. Die aktuelle Standortbestimmung zur Informationssicherheit ist unter folgendem Verweis verfügbar: [Informatik Team - Dokumente Informationssicherheit - Nach Themenbereich]



A.5 Sicherheitsleitlinien
A.6 Organisation der Informationssicherheit
A.7 Personalsicherheit
A.8 Verwaltung der Werte (Assets)
A.9 Zugangssteuerung
A.10 Kryptographie
A.11 Physische und umgebungsbezogene Sicherheit
A.12 Betriebssicherheit
A.13 Kommunikationssicherheit
A.14 Anschaffung, Entwicklung und Instandhalten von Systemen
A.15 Lieferantenbeziehungen
A.16 Management von Informationssicherheitsvorfällen
A.17 Aufrechterhalten der Informationssicherheit (Business Continuity Management)
A.18 Compliance

Maturitäts-niveau	Beschreibung	Zusammenfassung	Kernbestandteile
5	Bestmöglich, Optimiert und geschäftsorientiert	• In den Audit- und Bewertungszyklus einbezogen • Steuerungskennzahlen gemessen und überwacht • Entwicklung und Anwendung von Prozesskennzahlen • Vollständige Kontrolle der Qualitätsrückführung	• Nachverfolgte Steuerungsinformationen und Status • Abgestimmt auf die Geschäftsprozesse • Sehr geringes Restrisikopotenzial • Erfüllung oder Übertreffen von betriebswirtschaftlichen Anforderungen
4	Verwaltet, gesteuert und vorhersehbar	• Kontrollmassnahmen, die geprüft und auf Konformität getestet wurden. • Festgelegte Kennzahlen und Schwellenwerte • Vorhandene und implementierte Normen • Schulung und Sensibilisierung vollständig abgeschlossen	• Effizientes Agieren im Rahmen des formalen Prozesses • Eingebettet in Gesamtprozesse • Geschäftsanforderungen berücksichtigt • Geringes Restrisikopotenzial • Effizienz in einem adäquaten Bereich
3	Proaktiv, definiert und implementiert	• Benutzer, die für die Bedienung und Überwachung geschult sind • Gleichmässige Umsetzung und Überwachung • Dokumentierte Normen • Regelmässige Evaluierungen	• Guter/Hervorragender Wirkungsgrad • Einbettung in den IT-Prozess • Weit verbreiteter und publizierter Regelungsstand • Moderates Restrisikopotenzial • Wirkungsgrad in einem adäquaten Bereich
2	Reproduzierbar, flexibel und mit Best Effort	• Verantwortlichkeit, die einer Rolle, Person oder einem Prozess zugeordnet ist • Inkonsistente Implementierung in verschiedenen Unternehmensbereichen • Dokumentiert durch Richtlinien und Leitfäden • Inkonsistente Beurteilung und/oder Überprüfung	• Angemessener Wirkungsgrad • Der aktuelle Zustand ist in der Regel nur wenigen bekannt. • Mässiges bis hohes Restrisikopotenzial • Wirksamkeit durch individuellen Einsatz/Fachwissen
1	Initial, undefiniert und ad-hoc	• Nicht offiziell einer Rolle, Person oder einem Prozess zugeordnet. • Teilweise realisiert. • Unzureichend dokumentiert. • Nicht überwacht oder geprüft.	• Schlechter Wirkungsgrad • Fragwürdige Verantwortlichkeitsstruktur • Zustand unklar/ ungenau • Hohes Restrisikopotenzial • Allgemein unbekannter Wirkungsgrad
0	Nicht identifiziert und nicht adressiert	• Steuerung nicht implementiert. • Unkenntnis der Existenz von Kontrollmechanismen	• Nicht in Betrieb • Undefinierte Anforderungskriterien

3.2 NIST Cyber Security Framework

Folgend wird das NIST Framework mit seinen fünf Phasen erläutert:

Phase	Beschreibung
Identifizieren	Entsprechend der relativen Bedeutung für die Geschäftsziele und die Risikostrategie des Unternehmens werden Mitarbeiter, Daten, Geräte, Systeme und Einrichtungen identifiziert und verwaltet. Zur Unterstützung von Entscheidungen über operationelle Risiken werden sodann Prioritäten, Einschränkungen und Risikotoleranzen festgelegt und verwendet. Erst durch das Verständnis des Geschäftskontextes, der Ressourcen, der kritischen Funktionen und der damit verbundenen Cybersicherheitsrisiken können die Spitäler fmi AG ihre Massnahmen definieren und priorisieren.
Schützen	Entwicklung und Umsetzung geeigneter Sicherheitsvorkehrungen, um die Bereitstellung kritischer Infrastrukturdienste zu gewährleisten. Die «Schützen»-Funktion unterstützten die Spitäler fmi AG in der Fähigkeit, die Wahrscheinlichkeit eines potenziellen Cybersicherheitsereignisses zu begrenzen oder einzudämmen.
Erkennen	Entwicklung und Umsetzung geeigneter Massnahmen zur Identifizierung des Auftretens eines Cybersicherheitsereignisses. Diese Funktion ermöglicht den Spitäler fmi AG die rechtzeitige Erkennung von Cybersicherheitsereignissen.
Reagieren	Entwicklung und Umsetzung der geeigneten Aktivitäten, um Massnahmen in Bezug auf ein erkanntes Cybersicherheitsereignis zu ergreifen. Die Funktion unterstützt die Spitäler fmi AG in der Fähigkeit, die Auswirkungen eines potenziellen Cyberereignisses zu begrenzen.
Wiederherstellen	Entwicklung und Durchführung geeigneter Massnahmen zur Aufrechterhaltung von Plänen für die Widerstandsfähigkeit und zur Wiederherstellung von Fähigkeiten oder Diensten, die durch ein Cybersicherheitsereignis beeinträchtigt wurden. Die Funktion unterstützt die rechtzeitige Wiederherstellung des normalen Betriebs, um die Auswirkungen eines Cybersicherheitsereignisses zu reduzieren.

4 Glossar

Begrifflichkeit	Definition
CISO	Chief Information Security Officer, der Begriff kann mit dem ISV gleichgesetzt werden
DSG	Abkürzung für das Schweizer Bundesgesetz über den Datenschutz. Es bezweckt den Schutz der Persönlichkeit und der Grundrechte von natürlichen und juristischen Personen, über die Daten bearbeitet werden
DSV	Abkürzung für datenschutzverantwortliche Person (siehe Kapitel 2.3.5)
EPD	Abkürzung für Elektronisches Patientendossier. Ein stellt eine Sammlung persönlicher Dokumente mit Informationen rund um Ihre Gesundheit dar
EPDG	Abkürzung für das Schweizer Bundesgesetz über das Elektronische Patientendossier. Das EPGD beschreibt technische, organisatorische und sicherheitsrelevante Rahmenbedingungen zum EPD
IKT	Abkürzung für Informations- und Kommunikationstechnik
Integrität	Integrität bedeutet, dass es nicht möglich sein darf, Daten unerkannt bzw. unbemerkt zu ändern
ISB	Abkürzung für eine Informationssicherheitsbeauftragte Person (siehe Kapitel 2.3.4)
ISDS	Informationssicherheit und Datenschutz
ISMS	Abkürzung für Informationssicherheitsmanagementsystem.
ISO/IEC 2700x	Die Normreihe ISO 27000 enthält viele Teilnormen zum Thema Informationssicherheitsmanagement.

Begrifflichkeit	Definition
	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
ISV	Abkürzung für Informationssicherheitsverantwortliche Person (siehe Kapitel 2.3.3)
IT-Infrastruktur	Abkürzung für Informationstechnik-Infrastruktur. IT-Infrastruktur umfasst alle Komponenten, welche zur automatisierten Informationsverarbeitung zur Verfügung stehen.
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