Leitlinie

Informationssicherheit

Version:	1.3.0
Stand:	20.11.2026
Status:	Final
Klassifizierung:	extern
Referenz:	[gem-LL-ISMS-extern]

Freigabe	Chief Security Officer	Geschäftsführung	
Name	Holm Diening	Dr. Florian Hartge	Brenya Adjei
Unterschrift	Digital unterschrieben von Holm Diening Datum: 2026.11.24 10:58:44 +01'00'	sign-me Signiert von FLORIAN HARTGE am 24.11.2026	Datum: 2026.11.25 10:15:01 +01'00'

Dokumenteninformationen

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	26.07.23	alle	Erste finale Version der zusammengeführten Leitlinie Informationssicherheit und Leitlinie betriebliche Sicherheit TI	S. Labinski
1.1.0	07.11.24	alle	Überarbeitung und Aktualisierung der Leitlinie und der Grafiken	F. Lindemann
1.2.0	21.11.25	alle	Überarbeitung und Aktualisierung der Leitlinie und der Grafiken	F. Lindemann
1.3.0	20.11.26	alle	Überarbeitung und Aktualisierung der Leitlinie und der Grafiken	F. Lindemann

© gematik – extern

Inhaltsverzeichnis

Dokumenteninformationen 2

Inhaltsverzeichnis 3

1 Einordnung 4

1.1 Auftrag der gematik 4

1.2 Zweck der Leitlinie 4

1.3 Geltungsbereich des ISMS 5

2 Sicherheitsziele 6

Anhang A Anwendungsbereich der ISO 27001 Zertifizierung 8

© gematik – extern

1 Einordnung

1.1 Auftrag der gematik

Die Digitalisierung prägt die aktuelle Entwicklung der Medizin. Die Erfassung, Verarbeitung und Nutzung medizinischer Daten beschleunigt die Forschung, revolutioniert Therapien und kann zu einer nachhaltigen Verbesserung der Versorgung beitragen. Diesen Prozess in Deutschland entschlossen voranzutreiben und konstruktiv mitzugestalten, ist Ziel und gesetzlicher Auftrag der gematik. Als Digitalagentur Gesundheit trägt die gematik die Gesamtverantwortung für die Telematikinfrastruktur (TI) als zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Durch verbindliche Standards für Dienste, Komponenten und Anwendungen sorgt die gematik dafür, dass die TI sicher, stabil, interoperabel und nutzerfreundlich betrieben und weiterentwickelt wird.

Der Erfolg der gematik beruht daher auf der sicheren Nutzung, Verarbeitung, Speicherung und Übertragung von Informationen des Unternehmens, aber insbesondere der Fähigkeit, Vorgaben für das erforderliche Sicherheitsniveau der TI zu erstellen, zu überwachen, durchzusetzen und kontinuierlich zu verbessern.

Die Verlässlichkeit der eingesetzten Produkte und Verfahren sowie eine hohe Verfügbarkeit der Daten und Informationen sichern die Leistungsfähigkeit, das Vertrauen von Geschäftspartnern sowie unser Ansehen in der Öffentlichkeit. Die gematik ist sich aufgrund ihres gesetzlichen Auftrages und der Erwartung von Nutzern der TI ihrer besonderen Verantwortung für die Informationssicherheit bewusst.

1.2 Zweck der Leitlinie

Diese Leitlinie beschreibt strategische Ziele und Rahmenbedingungen zur Aufrechterhaltung und kontinuierlichen Verbesserung der Informationssicherheit für die gematik und TI. Hierzu etabliert die Geschäftsführung

- ein Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001,
- fördert den Aufbau einer leistungsfähigen Informationssicherheitsorganisation,
- befähigt die Organisation, Informationssicherheit wirksam in Aufbau- und Ablauforganisation, Projekte und TI-Produkte zu integrieren,
- unterstützt aktiv die sichere Eigenentwicklung von Komponenten der TI,
- beauftragt Audits und technische Prüfungen zur Verifikation des erforderlichen Sicherheitsniveaus,
- stellt die Steuerung von Anbietern und Dienstleistern über geeignete Prozesse sicher
- und stellt hierfür notwendigen Ressourcen bereit.

© gematik – extern

1.3 Geltungsbereich des ISMS

Das Informationssicherheitsmanagementsystem (ISMS) umfasst Prinzipien, Prozesse, Rollen und Gremien, um das angestrebte Sicherheitsniveau in der gematik zu definieren, umzusetzen, zu kontrollieren und fortlaufend an die aktuellen Bedürfnisse anzupassen und zu verbessern.

Das ISMS umfasst die interne Informationsverarbeitung der gematik und hierbei insbesondere alle Wertschöpfungsprozesse der gematik, die direkt dem Unternehmenszweck der gematik gemäß § 311 SGB V dienen. Neben der Gewährleistung der Informationssicherheit für Informationen und die Informationsverarbeitung (z.B. Anwendungen, IT-Systeme, Netze, Infrastruktur), die direkt im Verantwortungsbereich der gematik als Unternehmen liegen, gilt dies auch für die Verarbeitung von Daten durch Personen oder Unternehmen, die im Rahmen von Werkverträgen oder auf sonstiger Vertragsgrundlage durch die gematik beauftragt wurden. Die Informationssicherheit schließt, neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten, auch die Sicherheit von nicht elektronisch verarbeiteten Informationen (z.B. Aufzeichnungen in Papierform oder das gesprochene Wort) ein.

Diese Leitlinie gilt verbindlich für alle Beschäftigten der gematik (einschließlich Führungskräften, Praktikantinnen/Praktikanten, Auszubildenden, Trainees, Werkstudentinnen/Werksstudenten) sowie für beauftragte Personen und Unternehmen.

© gematik – extern

2 Sicherheitsziele

In der gematik werden in nahezu allen Unternehmensbereichen schützenswerte Informationen verarbeitet. Der Erfolg der gematik hängt vom schnellen, sicheren und aktuellen Zugriff auf diese Informationen sowie dem vertrauensvollen Umgang damit ab.

Der sichere Umgang mit schützenswerten Informationen bildet die Basis für die Wahrnehmung der gesetzlichen Aufgaben der gematik gemäß § 311 SGB V zur Bereitstellung von sicheren Komponenten der TI und deren sicheren und stabilen Betrieb.

Der Schutz von medizinischen Informationen der Versicherten im Verantwortungsbereich der TI hat für die gematik höchste Priorität und stellt einen wesentlichen Faktor für die Akzeptanz digitaler Anwendungen im deutschen Gesundheitswesen dar. Gleichzeitig dient die Informationssicherheit der Patientensicherheit und der medizinischen Versorgung, indem Vertraulichkeit, Integrität und Verfügbarkeit von versorgungsrelevanten Informationen gewährleistet werden.

Um diesem Anspruch gerecht zu werden, definiert die gematik unter Berücksichtigung der Erwartungshaltung der relevanten Stakeholder die folgenden Sicherheitsziele:

- Schützenswerte Informationen der TI und der gematik müssen wirksam vor unberechtigtem Zugriff geschützt werden (**Vertraulichkeit**).
- Die Unverfälschtheit (**Integrität**) von Informationen innerhalb der TI und der gematik muss gewährleistet werden.
- Die erforderliche **Verfügbarkeit** von Informationen und Anwendungen der TI sowie der Geschäftsprozesse der gematik muss sichergestellt werden.

Diese Ziele sollen im Rahmen des ISMS insbesondere erreicht werden durch:

- das Verankern der Informationssicherheit als integralen Bestandteil der Unternehmensstrategie,
- den Aufbau und die kontinuierliche Verbesserung der Prozesse des Informationssicherheitsmanagements,
- die enge Zusammenarbeit zwischen den Bereichen Sicherheit und Operations sowie der Integration des TI-Servicemanagements in den zertifizierten Geltungsbereich,
- die unmittelbare Einbindung von Experten der Informationssicherheit in das Portfolio der TI und deren Produkte sowie Programme und Projekte der gematik,
- die Erstellung von Vorgaben (gematik internes Regelwerk) und Spezifikationen (TI) sowie die Umsetzung geeigneter übergreifender Sicherheitsmaßnahmen,
- die Etablierung und Aufrechterhaltung von sicheren Entwicklungsprozessen über den gesamten Secure Software Development Life Cycle (SSDLC) für die Eigenentwicklung von Komponenten der TI bzw. gematik,
- die systematische Auswertung von sicherheitsrelevanten Meldungen externer Stakeholder,
- die kontinuierliche Erkennung, Analyse und Behandlung von Bedrohungen, Risiken, Schwachstellen und Sicherheitsvorfällen,
- die Planung, Testung und Pflege von Notfall- und Wiederherstellungsmaßnahmen;

© gematik – extern

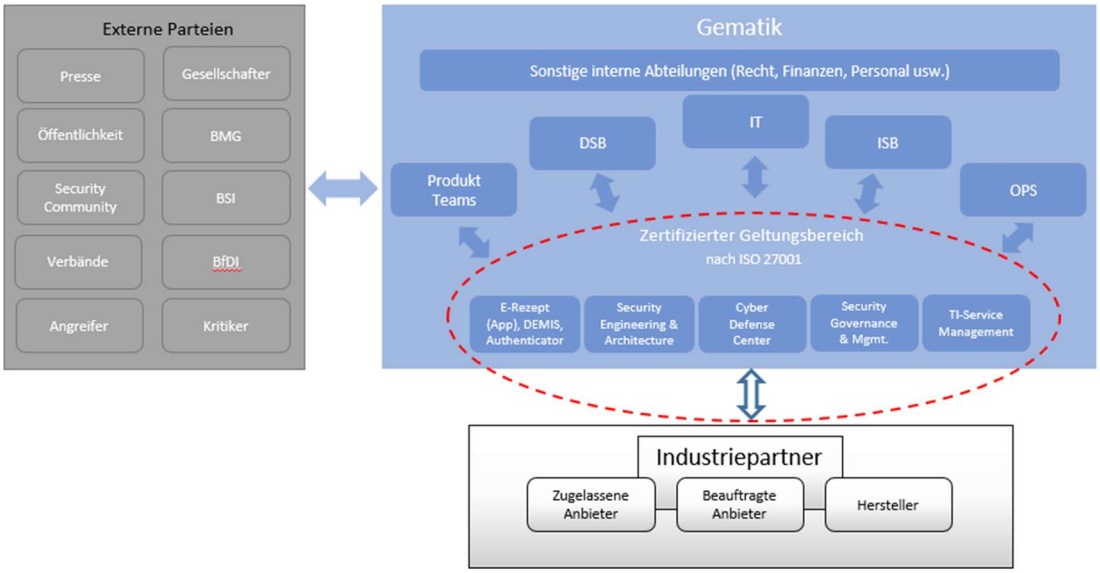
- die wirksame Einbindung externer und interner Stakeholder in das ISMS,
- die Sicherstellung des operativen Betriebs, unabhängig davon, ob der Betrieb im eigenen Unternehmen erfolgt oder ausgelagert ist,
- die regelmäßige Durchführung von Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit, um bei Führungskräften und Mitarbeitenden ein angemessenes Sicherheitsbewusstsein zu schaffen und aufrecht zu erhalten,
- die regelmäßigen Erfolgskontrollen bei der Prozessdurchführung und der Maßnahmenumsetzung zur Verbesserung der Informationssicherheit.

© gematik – extern

Anhang A Anwendungsbereich der ISO 27001 Zertifizierung

Die gematik spezifiziert Anforderungen an Dienste und Komponenten der Telematikinfrastruktur insbesondere auch im Kontext der Informationssicherheit. Zusätzlich übernimmt die gematik in begrenztem Umfang auch die Entwicklung eigener Komponenten. Der Anwendungsbereich der ISO/IEC 27001-Zertifizierung umfasst die anbieter- und herstellerübergreifende Überwachung des sicheren Betriebs der Telematikinfrastruktur mit seinen Diensten und Komponenten gemäß dem gesetzlichen Auftrag der gematik § 311 SGB V Absatz 1c, einschließlich der Überwachung der für den Betrieb erforderlichen Unterstützungsprozesse sowie die sicheren Entwicklungsprozesse von eigenentwickelten Komponenten und deren Bereitstellung innerhalb der Telematikinfrastruktur gemäß SGB V Kapitel 11.

Die nachfolgende Grafik visualisiert den Geltungsbereich (roter gestrichelter Kreis) sowie deren Schnittstellen. Eine Detaillierung der Stakeholder und Beschreibungen der Schnittstellen sind der Richtlinie und Arbeitsanweisung Betriebliche Sicherheit sowie dem Kommunikationskonzept zu entnehmen.



© gematik – extern