Leitlinie

Informationssicherheit

Version:	1.0
Stand:	26.07.2023
Status:	Final
Klassifizierung:	öffentlich
Referenz:	[gem-LL-ISMS -extern]

Freigabe	Chief Security Officer	Geschäftsführer
Name	Holm Diening	Dr. M. Leyck Dieken
Unterschrift	 Digital unterschrieben von Holm Diening Datum: 2023.07.26 15:37:37 +02'00'	Markus Leyck Dieken Digital unterschrieben von Markus Leyck Dieken Datum: 2023.07.31 10:54:13 +02'00'

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

Inhaltsverzeichnis

1 Einordnung

1.1 Auftrag der gematik

Die Digitalisierung ist der nächste Quantensprung in der Entwicklung der Medizin. Die Erfassung, Verarbeitung und Nutzung medizinischer Daten beflügelt die Forschung, revolutioniert Therapien und sorgt dafür, dass wir immer gesünder, länger und besser leben. Diesen Prozess in Deutschland entschlossen voranzutreiben und konstruktiv mitzugestalten, ist Ziel, Aufgabe und Mission der gematik. Als nationale Agentur für digitale Medizin trägt die gematik die Gesamtverantwortung für die Telematikinfrastruktur (TI), die zentrale Plattform für digitale Anwendungen im deutschen Gesundheitswesen. Mit der Definition und Durchsetzung verbindlicher Standards für Dienste, Komponenten und Anwendungen in der TI gewährleistet die gematik, dass diese zentrale Infrastruktur sicher, leistungsfähig und nutzerfreundlich ist und bleibt.

Der Unternehmenserfolg der gematik beruht daher sowohl auf der sicheren Nutzung, Verarbeitung, Speicherung und Übertragung von Informationen des Unternehmens selbst aber insbesondere auch in der Fähigkeit, Vorgaben für das erforderliche Sicherheitsniveau der TI zu erstellen, zu überwachen, durchzusetzen und kontinuierlich weiter 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

Zweck der Leitlinie ist die Beschreibung der strategischen Ziele und übergeordneten Rahmenbedingungen zur Aufrechterhaltung der Informationssicherheit für die gematik und TI. Hierzu etabliert der Geschäftsführer

- ein Informationssicherheitsmanagementsystem auf Basis der internationalen Norm ISO/IEC 27001,
- fördert die Umsetzung der notwendigen Prozesse durch den Aufbau einer Informationssicherheitsorganisation,
- befähigt die Organisation durch geeignete Organisationsstrukturen und Prozesse, Informationssicherheit optimal in die Organisation, Projekte und Produkte der TI zu integrieren,
- unterstützt aktiv die sichere Entwicklung von Komponenten der TI durch die gematik selbst,
- beauftragt die Durchführung von Audits und technischen Prüfungen, zur Verifikation des erforderlichen Sicherheitsniveaus,
- hält die notwendigen Prozesse zur Steuerung der Anbieter aufrecht und
- stellt die dafür notwendigen Ressourcen bereit.

1.3 Geltungsbereich des ISMS

Das Informationssicherheitsmanagementsystem (ISMS) ist eine Aufstellung von Verfahren, Regeln, Gremien und Rollenbeschreibungen, 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 Mitarbeiterinnen und Mitarbeiter[i], die im Angestelltenverhältnis bei der gematik beschäftigt sind (einschließlich Führungskräften, Praktikanten, Auszubildenden, Trainees und Werksstudenten), insbesondere Personen oder Unternehmen, die im Rahmen von Werkverträgen oder auf sonstiger Vertragsgrundlage für die gematik tätig sind (Beauftragte).

2 Sicherheitsziele

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

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 sicherem 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.

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 effektiv 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 Festschreiben der Informationssicherheit als integralen Bestandteil der Unternehmensstrategie,
- den Aufbau und die kontinuierliche Verbesserung der Prozesse des Informationssicherheitsmanagements,
- 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 Spezifikation (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 Auswertung von sicherheitsrelevanten Meldungen externer Stakeholder,
- die kontinuierliche Detektion, Analyse und Behandlung von Bedrohungen, Risiken, Schwachstellen und Sicherheitsvorfällen,
- die Planung und Erprobung von Maßnahmen zur Vorsorge von Notfällen,
- die Einbindung externer und interner Stakeholder in das ISMS,
- der Gewährleistung 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 Mitarbeitern ein angemessenes Sicherheitsbewusstsein zu schaffen und aufrecht zu erhalten,
- die regelmäßigen Erfolgskontrollen bei der Prozessdurchführung und der Maßnahmenumsetzung zur Verbesserung der Informationssicherheit.

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 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 inkl. 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 den Richtlinien *Cyber Defense Center, Application Design & Audit* sowie *Sichere Softwareentwicklung* zu entnehmen.