Medizinischer Dienst
Nordrhein

Informationssicherheitsrichtlinie des Medizinischen Dienstes Nordrhein

Vertraulichkeitsstufe: Öffentlich
Version: 1.0

Medizinischer Dienst Nordrhein

Inhaltsverzeichnis

Medizinischer Dienst Nordrhein

Dokumentenklassifizierung

Feld	Angabe
Dokumentenverantwortung	Informationssicherheitsbeauftragte
Geltungsbereich	Gesamtes Informationssicherheitsmanagementsystem des Medizinischen Dienstes Nordrhein (gemäß definiertem Anwendungsbereich)
Zielgruppe	Vorstand, Mitarbeitende, Auftragsverarbeiter, externe Dienstleister, Auftraggeber
Version	1.0
Gültig ab	Datum der Freigabe durch den Vorstand
Vertraulichkeitsstufe	Öffentlich

Glossar

Begriff / Abkürzung	Definition und Bedeutung im ISMS
Vertraulichkeit (Confidentiality)	Sicherstellung, dass Informationen nur denjenigen Personen, Prozessen oder Systemen zugänglich sind, die die entsprechende Berechtigung besitzen (Schutz vor unbefugter Preisgabe).
Integrität (Integrity)	Sicherstellung der Korrektheit, Vollständigkeit und Unversehrtheit von Daten und Systemen (Schutz vor unbefugter oder unbeabsichtigter Veränderung).
Verfügbarkeit (Availability)	Gewährleistung, dass autorisierte Benutzer bei Bedarf und im vereinbarten Zeitrahmen auf Daten, Dienste und IT-Systeme zugreifen können (Schutz vor Systemausfällen).
ISMS	Informationssicherheitsmanagementsystem: Ein systematischer Ansatz (basierend auf der ISO/IEC 27001) zur Steuerung, Überwachung und kontinuierlichen Verbesserung der Informationssicherheit im Unternehmen.
IT-Sicherheitsvorfall	Ein unerwartetes oder unerwünschtes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen oder IT-Systemen beeinträchtigt oder gefährdet.
Kontinuierliche Verbesserung (KVP)	Der stetige Prozess der Optimierung des ISMS (Plan-Do-Check-Act), um das Sicherheitsniveau laufend an neue Bedrohungslagen anzupassen.

1. Zweck und Geltungsbereich

Diese Richtlinie definiert die grundlegenden Ziele, Prinzipien und Verantwortlichkeiten der Informationssicherheit beim Medizinischen Dienst Nordrhein. Sie ist das grundlegende Dokument des Informationssicherheitsmanagementsystems und dokumentiert das nachhaltige Engagement der Organisation für den Schutz von Informationen.

2. Normative Grundlage

Diese Richtlinie basiert auf ISO/IEC 27001:2022 und bildet die Grundlage für das Informationssicherheitsmanagementsystem.

3. Stellenwert der Informationssicherheit

Informationssicherheit ist ein wesentlicher Bestandteil der Unternehmensführung. Sie gewährleistet den Schutz personenbezogener Daten, Sozialdaten und geschäftskritischer Informationen und ist Voraussetzung für Vertrauen, Qualität und Kontinuität der Aufgabenerfüllung im Gesundheitswesen.

Der Medizinische Dienst Nordrhein verpflichtet sich zur Erfüllung dieser Aufgaben und zur Ausrichtung des ISMS an folgenden Kernpunkten und Interessierte Parteien:

3.1. Relevante Anforderungen

Zur Gewährleistung eines angemessenen Informationssicherheitsniveaus sind insbesondere folgende Anforderungen zu berücksichtigen:

- **Schutz der Schutzziele**: Wahrung von Vertraulichkeit, Integrität und Verfügbarkeit von Sozialdaten, sensiblen Unternehmensdaten und personenbezogenen Daten.
- **Einhaltung von Vorgaben:** Erfüllung aller relevanten gesetzlichen, regulatorischen und vertraglichen Anforderungen (z. B. DSGVO).
- **Risikominimierung:** Vermeidung von finanziellen und reputationsbezogenen Schäden.
- **Geschäftskontinuität:** Sicherstellung der Prozesse durch Notfallvorsorge und Risikomanagement.

3.2. Interessierte Parteien

Die Erfordernisse und Erwartungen folgender Parteien möchte der Medizinische Dienst Nordrhein primär mit dem ISMS erfüllen:

- **Intern***:* Vorstand, Bereich IT, Informationssicherheitsbeauftragte, Datenschutzbeauftragte, Mitarbeitende, Organisationseinheiten, AG-ISMS.
- **Extern***:* Auftragsverarbeiter, Kooperationspartner, Kunden (z. B. Krankenkassen, Versicherte), Aufsichtsbehörden.

4. Risikobasierter Ansatz

Die Informationssicherheit basiert auf einem systematischen Prozess zur Erkennung und Bewertung von Risiken. Der Medizinische Dienst Nordrhein stellt durch diesen Ansatz sicher, dass Sicherheitsmaßnahmen verhältnismäßig und effektiv sind. Risiken werden regelmäßig bewertet, um auf Veränderungen der Bedrohungslage angemessen zu reagieren.

5. Ziele des Informationssicherheitsmanagementsystems

Das Informationssicherheitsmanagementsystem verfolgt insbesondere folgende Ziele:

- Erfüllung aller Anforderungen der ISO/IEC 27001:2022 sowie die erfolgreiche Zertifizierung und Aufrechterhaltung der Zertifizierung
- Einführung und regelmäßige Durchführung von Schulungs- und Sensibilisierungsmaßnahmen zur Stärkung der Informationssicherheitskompetenz aller Mitarbeitenden
- Etablierung eines kontinuierlichen Risikomanagementprozesses zur Identifikation und Behandlung von Bedrohungen, um das Gesamtrisiko auf ein akzeptables Maß (maximal „mittel“) zu reduzieren
- Vermeidung von Informationssicherheitsvorfällen sowie Reduzierung deren Auswirkungen

Diese Ziele sollen durch aktuelle, etablierte, allgemein anerkannte sowie wirksame technische und organisatorische Maßnahmen erreicht werden. Darüber hinaus besteht eine Verpflichtung zur Erfüllung der Anforderungen zur Informationssicherheit sowie eine Verpflichtung zur fortlaufenden Verbesserung des Informationssicherheitsmanagementsystem.

Die Zielerreichung wird anhand definierter Kennzahlen regelmäßig überprüft, bewertet und im Rahmen der kontinuierlichen Verbesserung des Informationssicherheitsmanagementsystems fortlaufend optimiert.

6. Verantwortlichkeiten

Vorstand

Er gibt die Rahmenbedingungen vor, stellt die erforderlichen Ressourcen bereit und überwacht die Wirksamkeit des ISMS. Zu diesem Zweck setzt der Vorstand diese Richtlinie in Kraft; ihre Einhaltung ist für alle Mitarbeiterinnen und Mitarbeiter sowie externe Partner verbindlich. Die praktische und operative Umsetzung aller Sicherheitsmaßnahmen wird an die Informationssicherheitsbeauftragte und den Bereichsleiter IT delegiert.

Informationssicherheitsbeauftragte

Die Informationssicherheitsbeauftragte ist vom Vorstand mit der praktischen Umsetzung, dem operativen Aufbau, Betrieb und der kontinuierlichen Weiterentwicklung des ISMS betraut. Sie besitzt die fachliche Richtlinienkompetenz für Informationssicherheit im Unternehmen. Die Informationssicherheitsbeauftragte koordiniert die Sicherheitsmaßnahmen, überwacht deren

Einhaltung im Alltag und berichtet regelmäßig sowie anlassbezogen direkt an den Vorstand, um dessen Überwachungsfunktion zu unterstützen.

Bereich IT

Der Bereich IT ist für den sicheren Betrieb der IT-Infrastrukturen sowie für die Umsetzung technischer Sicherheitsmaßnahmen verantwortlich. Die Bearbeitung von IT-Sicherheitsvorfällen erfolgt durch den Bereich IT in Zusammenarbeit mit der Informationssicherheitsbeauftragten. Die Informationssicherheitsbeauftragte wird frühzeitig eingebunden.

Arbeitsgruppe Informationssicherheitsmanagement

Die Arbeitsgruppe koordiniert die Weiterentwicklung der Informationssicherheit, bewertet Risiken und plant geeignete Maßnahmen. Die Informationssicherheitsbeauftragte und die Bereichsleitung IT bilden die Kernmitglieder dieser Arbeitsgruppe. Weitere Mitglieder werden von diesen beiden Personen je nach den spezifischen Anforderungen und Themen der jeweiligen Sitzung flexibel bestimmt und eingeladen.

Datenschutzbeauftragte

Die Datenschutzbeauftragten unterstützen die Einhaltung der datenschutzrechtlichen Anforderungen und beraten Organisationseinheiten und Mitarbeitende.

Mitarbeitende

Alle Mitarbeitenden sind verpflichtet, die Vorgaben dieser Richtlinie einzuhalten, sicherheitsrelevante Ereignisse unverzüglich zu melden sowie an informationssicherheitsrelevanten Schulungen teilzunehmen.

7. Verstöße

Verstöße gegen diese Richtlinie können arbeitsrechtliche Maßnahmen nach sich ziehen.

8. Gültigkeit und Dokumentenhandhabung

Dieses Dokument ist gültig ab dem Tag der Freigabe durch den Vorstand.
Die zuständige Person für dieses Dokument ist die Informationssicherheitsbeauftragte, die das Dokument mindestens einmal jährlich prüfen und gegebenenfalls aktualisieren muss.

9. Referenzdokumente

Die folgenden Dokumente werden referenziert:

- Anwendungsbereich des ISMS
- Verfahren zur Identifikation von Erfordernissen
- Verfahren zu Informationssicherheitszielen & KPIs
- Verfahren zur Korrekturmaßnahmen

10. Inkrafttreten

Die Richtlinie tritt mit dem Tag der Freigabe durch den Vorstand in Kraft.

	durch	Datum	Unterschrift
Verantwortlich:	Informationssicherheitsbeauftragte	29.06.2026	
freigegeben:	Vorstand	29.06.2026	