Leitlinie Informationssicherheit und Datenschutz

Informationssicherheitsmanagementsystem

Bearbeiter	K.-H. Borgheyink / J. Ritter
Verantwortliche Organisationseinheit	Vorstand Informationssicherheitsbeauftragter
Verteiler	Mitarbeiterinnen und Mitarbeiter der Kassenzahnärztlichen Vereinigung Westfalen-Lippe Eine Weitergabe an Dritte ist nur nach Freigabe durch den Vorstand erlaubt
Datum der letzten Bearbeitung/Freigabe	10.03.2025
Version	6.0
Vertraulichkeitsstufe	Öffentlich
Freigabestatus	Freigegeben

1 Inhaltsverzeichnis

1 Inhaltsverzeichnis 2
2 Generelle Informationen 3
2.1 Ziel und Zweck des Dokumentes 3
2.2 Geltungsbereich 3
2.3 Freigabe 3
2.4 Revision 3
3 Anwendung auf Normen 4
4 Einleitung 5
4.1 Heutiges Gefährdungspotenzial für vertrauliche Daten 5
4.2 Risiken für Daten der Organisation 5
5 Leitlinie der KZVWL zur Informationssicherheit 6
6 Berücksichtigung des Datenschutzes 7
7 Normative Grundlage und Sicherheitsziele 7
8 Geltungsbereich 8
9 Verpflichtung des Vorstands, Abteilungs- und Referatsleitern 9
10 Festlegung von Sicherheitszielen 9
11 Berücksichtigung des Klimawandels 10
12 Sicherheitsstrategie 11
13 Kontrolle durch Audits 12
14 Organisation des Informations- & Datenschutz-managements 13
15 Einbindung von Informationssicherheit & Datenschutz innerhalb der KZVWL 15
16 Kontinuierliche Verbesserung der Informations-sicherheit 16
17 Mitgeltende Unterlagen 17
18 Inkrafttreten 17
19 Dokumenteninformationen 18

2 Generelle Informationen

2.1 Ziel und Zweck des Dokumentes

Durch das Vorschreiten der Digitalisierung und die teils hohe Abhängigkeit im Bereich der Informationstechnologie hat der Vorstand der Kassenzahnärztlichen Vereinigung Westfalen-Lippe (im folgenden „KZVWL" genannt) erkannt, dass Informationssicherheit mehr und mehr Schlüssel zum Erfolg und absolut notwendig für funktionierende Prozesse und Verfahren geworden ist.

Dieses Dokument beschreibt allgemein verständlich, für welche Zwecke, mit welchen Mitteln und mit welchen Strukturen Informationssicherheit innerhalb der KZVWL durch das Informationssicherheitsmanagementsystem (ISMS) hergestellt werden soll. Diese Leitlinie initiiert den Informationssicherheitsprozess und ist das zentrale organisatorische Regelwerk des ISMS.

Dieses Dokument ist sowohl für alle Mitarbeiter der KZVWL als auch für externe Dienstleister sowie weitere Dritte mit Zugriff auf Informationswerte bestimmt.

Auf eine geschlechterspezifische begriffliche Trennung wird aus Vereinfachungsgründen bewusst verzichtet. Es wird in der Regel die geläufigere Form gewählt.

2.2 Geltungsbereich

Die hier getroffenen Regelungen gelten für das Informationssicherheitsmanagement-system (ISMS) der KZVWL.

2.3 Freigabe

Das vorliegende Dokument wird durch den Vorstand genehmigt und freigegeben.

2.4 Revision

Dieses Dokument sowie die daraus sich ergebenden Sicherheitsmaßnahmen unterliegen der Dokumentenlenkung [1].

3 Anwendung auf Normen

Auf dieses Dokument werden folgende Maßnahmen der ISO-Normen angewendet. Die definierten Maßnahmen in den ISO-Normen sind selbst als Arbeitshilfen zu bewerten, weil sie beschreiben was in den Dokumenten und Aufzeichnungen erwartet wird.

DIN ISO/ IEC 27001:2022

Maßnahme ISO27001:2022	Beschreibung
4.1	Verstehen der Organisation und ihres Kontextes
4.3	Festlegung des Anwendungsbereichs des Informationssicherheitsmanagementsystems
4.4	Informationssicherheitsmanagementsystem
5.1	Führung und Verpflichtung
5.2	Politik
5.3	Rollen, Verantwortlichkeiten und Befugnisse in der Organisation
6.2	Informationssicherheitsziele und Planung zu deren Erreichung
10.1	Fortlaufende Verbesserung
10.2	Nichtkonformität und Korrekturmaßnahmen
A.5.1	Informationssicherheitspolitik und -richtlinien
A.5.4	Verantwortlichkeiten der Leitung

4 Einleitung

4.1 Heutiges Gefährdungspotenzial für vertrauliche Daten

Ein ISMS wahrt die **Vertraulichkeit**, **Integrität** und **Verfügbarkeit** sowie die **Resilienz** (Widerstandsfähigkeit) von Informationen unter Anwendung eines Risikomanagementprozesses und verleiht interessierten Parteien das Vertrauen in eine angemessene Steuerung von Risiken.

Die Forderungen eines ISMS zur Informationssicherheit bestehen aufgrund verschiedener Regelungen:

- Verpflichtung der KZVWL zur Informationssicherheit;
- Gesetzliche Verpflichtung zum Schutz der personenbezogenen Daten auf der Basis der EU-DSGVO und des DSG-NRW;
- Gesetzliche Verpflichtung zum Schutz von Sozialdaten nach SGB;
- weitere gesetzliche Vorschriften oder Verordnungen;
- der Tatsache, dass die Folgen einer unangemessenen Informationssicherheit nicht auf die KZVWL begrenzt bleiben, sondern Folgen für die Beteiligten, darunter die Mitarbeiter und Mitglieder haben.

4.2 Risiken für Daten der Organisation

In gleichem Maße wie die Mitgliederdaten müssen auch Daten der KZVWL vor unbefugten Zugriffen oder ungewollten Übertragungen geschützt werden. Die stetig wachsende Vernetzung mit externen Stellen (z.B. Finanzamt, Banken, gesetzlichen Krankenkassen, Dienstleistern, etc.) erhöht die Risiken auch für Daten der KZVWL.

Daher gelten auch für Daten der KZVWL dieselben Grundregeln zur Absicherung wie für die Absicherung von Mitgliederdaten.

5 Leitlinie der KZVWL zur Informationssicherheit

Der Einsatz von moderner IT und Kommunikationstechnik ist wesentlich für die Aufgabenerfüllung der KZVWL. Als KZVWL werden unsere Prozesse in allen organisatorischen und kaufmännischen Bereichen maßgeblich durch die IT getragen.

Teile der Infrastruktur der KZVWL werden für die Aufrechterhaltung des Betriebes als kritisch eingestuft. Ein Ausfall von kritischen Systemen gefährdet den Geschäftsbetrieb.

Die Sicherheit der Informationsverarbeitung spielt daher eine Schlüsselrolle für unsere Aufgabenerfüllung.

Zur Erfüllung der Aufgaben der Körperschaft des öffentlichen Rechts nach SGB V müssen schutzbedürftige Mitgliederdaten verarbeitet werden. Auch im Rahmen der übrigen Geschäftsprozesse ist die Verarbeitung von vertraulichen Daten, wie zum Beispiel Personaldaten oder Geschäftsgeheimnissen erforderlich.

Die Vertraulichkeit von schutzbedürftigen Daten und wichtiger Geschäftsprozesse sind durch wirksame und angemessene technische und organisatorische Maßnahmen sicherzustellen.

Um dies zu gewährleisten wird von der KZVWL ein Informationssicherheitsmanagement-system betrieben und kontinuierlich weiterentwickelt. Das Informationssicherheits-managementsystem soll dazu beitragen, die gesetzlichen Anforderungen des Datenschutzes umzusetzen.

Die vorliegende Informationssicherheitsleitlinie definiert die Ziele der KZVWL im Bereich der Informationssicherheit unter Berücksichtigung der gesetzlichen Anforderungen.

Die zur Gewährleistung der Informationssicherheit und zur Umsetzung der gesetzlichen Anforderungen im Bereich des Datenschutzes erforderlichen Aufgaben und Pflichten gegenüber unseren Mitgliedern, Vertragspartnern, Dienstleistern, Behörden und sonstigen Dritten werden in dieser Leitlinie festgelegt. Diese Aufgaben und Pflichten können in Dienstvereinbarungen, Richtlinien, etc. weiter konkretisiert werden.

Ferner werden die Sicherheitsstrategie, die Sicherheitsorganisation und die Sicherheitsziele der KZVWL definiert.

Mit dieser Sicherheitsleitlinie bekennt sich der Vorstand der KZVWL zu seiner Verantwortung für die Informationssicherheit und für den Datenschutz.

Der Vorstand der KZVWL setzt gemeinsam mit der Vertreterversammlung ein deutliches Signal für die Stärkung des Standortes und der Arbeitsplätze in Westfalen-Lippe und

möchte auf zukünftige Anforderungen der Telematikinfrastruktur und gesetzliche Vorgaben vorbereitet sein.

Weitere Entwicklungen der Telematikinfrastruktur bieten neue Potentiale im Hinblick auf eine Umsetzung diverser Anwendungsmöglichkeiten für die Mitglieder und stellen diesbezüglich hohe Anforderungen an die Informationssicherheit.

Alle Mitarbeiter der KZVWL sind aufgefordert, im Rahmen ihrer dienstlichen Tätigkeit auf die Einhaltung der in dieser Leitlinie definierten Ziele hinzuwirken.

Dies gilt insbesondere für Abteilungs- und Referatsleiter, die dafür verantwortlich sind, sowohl durch ihr Vorbild als auch durch ihre Anleitung ihre Mitarbeiter bei der Umsetzung der Regelungen und der gesetzlichen Anforderungen zur Einhaltung der Informationssicherheit und des Datenschutzes zu unterstützen.

Die Gesamtverantwortung für die Informationssicherheit und den Datenschutz obliegt dem Vorstand, der dabei vom Informationssicherheitsbeauftragten (ISB) sowie vom Datenschutzbeauftragten (DSB) unterstützt und beraten wird.

6 Berücksichtigung des Datenschutzes

Die Anforderungen des Datenschutzes basierend auf der DSGVO decken sich teilweise mit den Anforderungen der Informationssicherheit im Sinne der einschlägigen Normen, wie der ISO/IEC 27001. Maßnahmen, die die Schutzziele der DSGVO gemäß Art. 32 Abs. 1 sicherstellen, entsprechen Maßnahmen, die auch von der Norm ISO/IEC 27001 gefordert werden.

Dementsprechend können durch die Integration von Datenschutz und Informationssicherheit sowohl auf der Ebene des Managementsystems als auch auf der Ebene der Umsetzung von konkreten Maßnahmen Synergien genutzt werden. Die normative Grundlage für die Informationssicherheit bildet die ISO/IEC 27001, die über den Anhang A in 5.34 die DSGVO miteinschließt.

7 Normative Grundlage und Sicherheitsziele

Für die Umsetzung von angemessenen Maßnahmen innerhalb eines Managementsystems wird die Norm ISO/IEC 27001 genutzt. Für den Nachweis der Umsetzung dient eine Zertifizierung auf der Basis dieser Norm.

Unter Berücksichtigung der Anforderungen der DSGVO gemäß Art. 32 Abs. 1 lit. b) ergeben sich folgende Sicherheitsziele, welche innerhalb des ISMS betrachtet werden:

Vertraulichkeit

Vertrauliche Informationen dürfen ausschließlich dem berechtigten Personenkreis zur Verfügung stehen. Dienstgeheimnisse müssen gewahrt bleiben.

Integrität

Die physische und logische Unversehrtheit von Systemen, Anwendungen und Informationen muss jederzeit gewahrt sein. Dies schließt auch die Verhinderung einer unberechtigten Erstellung, Veränderung oder Löschung von Informationen mit ein.

Verfügbarkeit

Systeme, Anwendungen und Informationen müssen den Berechtigten im Rahmen vertretbarer technischer Möglichkeiten stets wie vorgesehen zur Verfügung stehen.

Resilienz

IT-Systeme müssen widerstandsfähig gegen Gefahren aus dem Internet oder internen Netzwerken sein.

8 Geltungsbereich

Es ergibt sich folgender Geltungsbereich für das Informationssicherheits-managementsystem im Sinne Kapitel 4.3 ISO/IEC 27001:

„Interessenvertretung der Vertragszahnärzte und -ärztinnen, Prozesse zur Sicherstellung der ambulanten vertragszahnärztlichen Versorgung der gesetzlich Versicherten und die Organisation der vertragszahnärztlichen Versorgung sowie deren Management, als auch unterstützende Prozesse, Ressourcen und Mitarbeitende."

9 Verpflichtung des Vorstands, Abteilungs- und Referatsleitern

Mit dieser Leitlinie legt der Vorstand die Informationssicherheitspolitik und die Informationssicherheitsziele fest. Der Vorstand stellt sicher, dass die in dieser Leitlinie festgelegten Sicherheitsziele und die Umsetzung des Informationssicherheits-managementsystems mit der strategischen Ausrichtung der KZVWL vereinbar sind. Der Vorstand bestimmt die erforderlichen Ressourcen für den Aufbau, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung des Informationssicherheits-managementsystems und stellt diese bereit.

Mit Unterstützung aller Abteilungs- und Referatsleiter stellt der Vorstand sicher, dass die Anforderungen des Informationssicherheitsmanagementsystems in die Geschäftsprozesse der KZVWL integriert werden. Der Vorstand und alle Abteilungs- und Referatsleiter sind dafür verantwortlich, die Bedeutung eines wirksamen Informationssicherheits-managements sowie die Wichtigkeit der Erfüllung der gesetzlichen und normativen Anforderungen zur Informationssicherheit und zum Datenschutz zu vermitteln.

Mit Unterstützung des Informationssicherheitsbeauftragten (ISB), des Datenschutzbeauftragten (DSB) sowie aller Abteilungs- und Referatsleiter stellt der Vorstand sicher, dass das Informationssicherheitsmanagementsystem die beabsichtigten Ergebnisse erzielt und der Datenschutz innerhalb der Organisation sichergestellt wird.

Die Abteilungs- und Referatsleiter sind dafür verantwortlich, ihre Mitarbeiter und gegebenenfalls auch die Mitarbeiter von involvierten Dienstleistern anzuleiten und dabei zu unterstützen, zur Wirksamkeit des Informationssicherheitsmanagementsystems beizutragen und sicherzustellen, dass die gesetzlichen Anforderungen zum Datenschutz umgesetzt werden. Vorstand sowie Abteilungs- und Referatsleiter wirken darauf hin, dass die fortlaufende Verbesserung der Informationssicherheit gefördert wird.

10 Festlegung von Sicherheitszielen

Für die KZVWL werden die in Kapitel 7 festgelegten strategischen Sicherheitsziele wie folgt konkretisiert:

- Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Abteilungen,
- Minimierung der zu erwartenden Ausfallzeiten,
- zuverlässige Unterstützung der Geschäftsprozesse durch die IT,

- Realisierung sicherer und vertrauenswürdiger digitaler Verfahren,
- Sicherung der hohen, möglicherweise unwiederbringlichen Werte der verarbeiteten Informationen,
- Gewährleistung der aus rechtlichen Vorgaben resultierenden Anforderungen,
- Gewährleistung des informationellen Selbstbestimmungsrechts der Betroffenen bei der Verarbeitung personenbezogener Daten,
- Sicherstellung der Gesetzeskonformität,
- Aufrechterhaltung einer positiven Reputation,
- Wahrung der Dienstgeheimnisse sowie
- Reduzierung der im Schadensfall entstehenden Aufwände durch ausreichende Notfallvorsorge.

Bei der Erreichung dieser Ziele ist eine Verhältnismäßigkeit der eingesetzten Mittel zum Wert der schützenswerten Güter zu beachten.

11 Berücksichtigung des Klimawandels

Hinsichtlich des Klimawandels können diverse Einflüsse auf die KZVWL identifiziert werden, die in der Sicherheitsstrategie Berücksichtigung finden müssen.

Hierzu gehören

extreme Wetterbedingungen

Das bestehende Rechenzentrum wurde einer baulichen Überprüfung unterzogen, ob es einer Überschwemmung standhalten würde. Daraufhin wurde auf Beschluss der Vertreterversammlung (VV), ein Backuprechenzentrum gebaut, welches gegen Hochwasser geschützt ist.

Um die Verfügbarkeit der sich im Rechenzentrum befindlichen Hardware bei anhaltender Hitze gewährleisten zu können, wurde eine zusätzliche Klimaanlage als Backup installiert.

Lieferkettenrisiken

Um das Risiko der Versorgungssicherheit durch den Klimawandel zu minimieren, sollte bei der Vergabe von Dienstleistungen darauf geachtet werden, das Lieferanten und Dienstleister durch Nachweise wie z.B. DIN EN 50600 - Zertifizierung von Rechenzentren grundlegende Anforderungen erfüllen.

Reputation und Anforderungen interessierter Parteien

Um ihrer Verantwortung hinsichtlich Klima- und Umweltschutz gerecht zu werden, hält die KZVWL bestimmte energetische Standards bei Renovierungen und Baumaßnahmen ein. Diese werden bei Erfordernis mit den relevanten interessierten Parteien abgestimmt.

Die KZVWL wurde an das örtliche Fernwärmenetz angeschlossen, um eine effiziente und klimaschonende Alternative zum herkömmlichen Heizsystemen zu erhalten.

Die KZVWL plant die Installation einer Photovoltaikanlage, diese trägt direkt zum Klimaschutz bei, indem sie den CO2-Ausstoß reduziert und den Übergang zu einer nachhaltigeren und saubereren Energieversorgung fördert.

12Sicherheitsstrategie

Die Gewährleistung der Vertraulichkeit von Mitgliederdaten bzw. personenbezogenen Daten der besonderen Kategorien im Sinne von Art. 9 Abs. 1 DSGVO hat einen hohen Stellenwert für die KZVWL.

Bei der Planung und Umsetzung von Geschäftsprozessen werden die Vertraulichkeit, die Integrität, und die Authentizität der Daten sowie die Verfügbarkeit der Geschäftsprozesse und der dazu erforderlichen Systeme und Infrastruktur und die Belastbarkeit der Systeme sichergestellt.

Die Strategie basiert auf folgenden Maßnahmen:

- Kritische Systeme werden redundant betrieben
- Wir führen regelmäßige Datensicherungen nach einem definierten Datensicherungskonzept durch.
- Mit sicherheitsrelevanten Vorfällen gehen wir kontrolliert um.

- Für alle IT-Verfahren, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person inklusive Vertretung benannt.
- Durch ausreichende Unterweisung und Dokumentation wird gewährleistet, dass Vertreter ihre Aufgaben erfüllen können.
- Räumlichkeiten werden ausreichend vor unbefugten Zutritten geschützt.
- Es existiert ein Virenschutzkonzept für alle IT-Systeme.
- Ein Zugriff von außen wird durch geeignete Systeme gesichert.
- Potenziell gefährliche Websites und Anhänge werden blockiert.
- Es existiert ein Notfallkonzept, um schnell auf Vorfälle reagieren zu können und Systeme nach einer tolerierbaren Zeit wiederherzustellen.
- Der Zugriff auf personenbezogene Daten erfolgt nur über persönliche und passwortgeschützte Zugänge.
- Zugriffe werden nach dem Minimalprinzip gewährt.
- Personenbezogene Daten, die das Unternehmen verlassen, werden über sichere Wege übermittelt.
- Die Einhaltung der ISMS Vorgaben wird regelmäßig kontrolliert und auditiert.
- Mitarbeiter werden regelmäßig sensibilisiert und geschult.
- Unsere Mitarbeiter kennen und befolgen die Richtlinien und sonstigen Vorgaben des ISMS.
- IT-Mitarbeiter nehmen regelmäßig an fachlichen Weiterbildungen bzgl. IT-Systemen und Softwareentwicklung teil.
- Durch das Risikomanagement wird sichergestellt, dass Risiken identifiziert und mit angemessenem Aufwand durch geeignete und wirksame Maßnahmen reduziert werden.
- Implementierung einer leistungsstarken Firewall

13 Kontrolle durch Audits

Informationssicherheit erfordert permanente Anstrengungen (Sicherheitsstrategie) und ist folglich keine einmalige Aktivität. Verlässliche Informationssysteme erfordern kontinuierliche Aufmerksamkeit.

Nach der Implementierung wird auditiert, ob die Maßnahmen tatsächlich wie geplant durchgeführt werden (Audit). Eine regelmäßige Evaluierung ist erforderlich, um festzustellen, ob die gewählten Maßnahmen noch ausreichen oder an welcher Stelle Anpassungen erforderlich sind.

Unter der Verantwortung des Informationssicherheitsbeauftragten werden in den einzelnen Fachabteilungen Kontrollen zu folgenden Punkten durchgeführt:

- Vorhandensein angemessener Notfallpläne;
- Beachtung der festgestellten Basisanforderungen und Implementierung der erforderlichen zusätzlichen Sicherheitsmaßnahmen;
- Engagement des Vorstands sowie Abteilungs- und Referatsleiter für die dauerhafte Wirkung der Maßnahmen, beispielsweise durch Befragungen der Fachabteilungen, d.h. es ist die Einhaltung von Richtlinien zu überprüfen und auf Abweichungen hinzuweisen und darauf hinzuwirken, dass diese behoben werden.

Bei der Kontrolle festgestellte Mängel werden in Auditberichten dokumentiert. Ergänzend erfolgt ggf. eine Beratung über zu ergreifende Maßnahmen zur Behebung der Mängel.

14 Organisation des Informations- & Datenschutz-managements

Zur Erreichung der Informationssicherheitsziele hat die KZVWL eine Sicherheitsorganisation implementiert.

Der **Informationssicherheitsbeauftragte (ISB)** ist in Form einer Stabsstelle unmittelbar dem Vorstand unterstellt und berichtet im Rahmen seiner Funktion direkt an diesen. Er wird von allen Abteilungs- und Referatsleitern sowie seinem Stellvertreter bei der Erfüllung seiner Aufgaben unterstützt.

Die Rolle des **Datenschutzbeauftragten (DSB)** ist in Form einer Stabsstelle unmittelbar dem Vorstand unterstellt. Auch der DSB arbeitet weisungsfrei und berichtet direkt an den Vorstand.

Dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten werden die zur Erfüllung ihrer Aufgaben erforderlichen Ressourcen zur Verfügung gestellt.

Dazu gehört die regelmäßige Teilnahme an Fortbildungsmaßnahmen, angemessene Unterstützung bei der Durchführung von internen Auditierungen sowie die Unterstützung bei der Ausübung ihres Weisungsrechts im Kontext der Informationssicherheit bzw. des Datenschutzes.

Der ISB und der DSB unterstützen alle Abteilungs- und Referatsleiter und Mitarbeiter und gegebenenfalls auch Mitarbeiter von Dienstleistern bei der Umsetzung der Regelungen zur Einhaltung der Informationssicherheit und der gesetzlichen Anforderungen zum Datenschutz bei der KZVWL.

Um die Synergien zwischen dem Datenschutz- und dem Informationssicherheitsmanagement optimal zu nutzen und die Integration von Managementsystemen innerhalb der Organisation zu fördern, wird ein **ISMS-Team** eingerichtet.

Das ISMS-Team koordiniert übergreifende Maßnahmen in der Gesamtorganisation, trägt Informationen zusammen und führt Kontrollaufgaben durch.

Das ISMS-Team (Kernteam) setzt sich aus den folgenden Bereichen zusammen:

- Informationssicherheitsbeauftragter
- Stellvertreter des Informationssicherheitsbeauftragten
- Datenschutzbeauftragter

Anlassbezogen können weitere Teilnehmer hinzugezogen werden. Diese könnten beispielweise sein:

- Personalrat
- Innere Verwaltung / Beschaffungsstelle
- Personalabteilung
- IT - Abteilung
- Abteilungs- und Referatsleitungen
- Compliance-Managerin

Das ISMS-Team berichtet an den Vorstand.

Zu den Aufgaben des ISMS-Teams gehören insbesondere:

- Datenschutz- und Informationssicherheitsziele und -strategien zu bestimmen sowie die Leitlinie zur Informationssicherheit zu entwickeln,
- die Umsetzung der Sicherheitsleitlinie zu überprüfen,
- den Sicherheitsprozess zu initiieren, zu steuern und zu kontrollieren,
- bei der Erstellung des Sicherheitskonzepts mitzuwirken,
- zu überprüfen, ob die im Sicherheitskonzept geplanten Sicherheitsmaßnahmen wie beabsichtigt funktionieren sowie geeignet und wirksam sind,
- die Schulungs- und Sensibilisierungsprogramme für Informationssicherheit zu konzipieren,
- als Hauptansprechpartner bei Fragen, die den Datenschutz und die Informationssicherheit betreffen, zu beraten.
- Bewertung und Behandlung von Sicherheitsvorfällen die den Datenschutz und die Informationssicherheit betreffen.

Das Risikomanagement stellt sowohl für den Datenschutz im Sinne der DSGVO als auch für das Informationssicherheitsmanagement auf der Basis der Norm ISO/IEC 27001 ein wichtiges Hilfsmittel dar.

Die methodische Verantwortung für das Risikomanagement hat das ISMS-Team. Das Risikomanagement der Organisation soll soweit möglich einheitlich erfolgen. Dabei muss den besonderen Anforderungen des Datenschutzes und der Informationssicherheit Rechnung getragen werden.

Weitere Einzelheiten zu den Rollen und zum ISMS-Team werden im Management-Handbuch beschrieben.

15 Einbindung von Informationssicherheit & Datenschutz innerhalb der KZVWL

Der Informationssicherheitsbeauftragte muss frühzeitig in alle informationssicherheitsrelevanten Projekte und Beschaffungsmaßnahmen eingebunden werden, damit schon in der Planungsphase relevante Aspekte berücksichtigt werden können. Er berät und sensibilisiert zu Fragen der Informationssicherheit.

Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Ein Mitspracherecht haben der ISB und DSB bei allen Entscheidungen die ihren Verantwortungsbereich betreffen (z. B. bei der Initiierung von IT-Projekten, Beschaffung von informationsverarbeitenden Systemen, Änderungen von Geschäftsprozessen, Ausbildung von Mitarbeitern, etc.).

Alle Mitarbeiter der KZVWL haben sich in informationssicherheitsrelevanten Fragestellungen an die Empfehlungen des Informationssicherheitsbeauftragten zu orientieren.

Alle Mitarbeiter der KZVWL sind aufgefordert, tatsächliche und gegebenenfalls auch vermutete Abweichungen von den Vorgaben dieser Leitlinie oder anderer Regelungen die Informationssicherheit oder den Datenschutz betreffend an den Informationssicherheitsbeauftragten bzw. den Datenschutzbeauftragten zu melden. Meldungen an den Datenschutzbeauftragten werden vertraulich behandelt. Meldungen an den Informationssicherheitsbeauftragten können auf Wunsch des Meldenden und soweit dies im Rahmen der Ziele dieser Informationssicherheitsleitlinie möglich ist, gegebenenfalls vertraulich behandelt werden.

16 Kontinuierliche Verbesserung der Informations-sicherheit

Das Informationssicherheitsmanagementsystem wird regelmäßig auf seine Aktualität und Wirksamkeit geprüft. Daneben werden auch die Maßnahmen regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt.

Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und diese ständig auf dem aktuellen Stand der Technik und konform zu den jeweiligen gesetzlichen Regelungen und normativen Vorgaben zu halten.

17 Mitgeltende Unterlagen

[1] Richtlinie - Dokumentenlenkung

18 Inkrafttreten

Diese Leitlinie tritt mit sofortiger Wirkung in Kraft und ersetzt die bisherige Version vom **21.05.2024**.

Münster, den 10.03.2025

Dr. Holger Seib
Vorstandsvorsitzender

Michael Evelt
stv. Vorstandsvorsitzender

19 Dokumenteninformationen

Historie und Status

Status	Anmerkungen	Datum	Version	Durchgeführt von
Entwurf	Initiale Erstellung	02.02.2021	0.1	ISMS-Team
In Bearbeitung	Inhaltliche Anpassungen	12.02.2021	0.2	ISMS-Team
In Bearbeitung	Inhaltliche Anpassungen	08.03.2021	0.3	ISMS-Team
In Bearbeitung	Inhaltliche Anpassungen	15.03.2021	0.4	ISMS-Team
In Bearbeitung	Inhaltliche Anpassungen	16.04.2021	0.5	ISMS-Team
Freigabe	Freigegeben durch Vorstand	29.04.2021	1.0	Vorstand
In Bearbeitung	Review Unter „Durchgeführt von" wurden die Verantwortlichen angepasst	07.03.2022	1.1	ISMS-Team
Freigabe	6 Leitlinie der KZVWL zur Informations-sicherheit	02.02.2023	1.2	Vorstand
Freigabe	Freigegeben durch Vorstand	07.02.2023	2.0	Vorstand
In Bearbeitung	- 5.1 Heutiges Gefährdungspotenzial für vertrauliche Daten	07.08.2023	2.1	ISMS-Team
In Bearbeitung	- 9 Geltungsbereich konkretisiert	16.08.2023	2.2	ISMS-Team
Freigabe	Freigegeben durch Vorstand	23.08.2023	3.0	Vorstand
In Bearbeitung	- 9 Geltungsbereich Beschreibung angepasst - 11 Festlegung von Sicherheitszielen - 12 Sicherheitsstrategie - 15 Einbindung von Informationssicherheit & Datenschutz innerhalb der KZVWL	10.04.2024	3.1	ISMS-Team

In Bearbeitung	Beschreibung angepasst - 8 Normative Grundlage und Schutzziele - 14 Organisation des Informations- & Datenschutzmanagements - 17 Mitgeltende Unterlagen ergänzt	16.05.2024	3.2	ISMS-Team
Freigabe	Freigegeben durch Vorstand	21.05.2024	4.0	Vorstand
In Bearbeitung	Beschreibung angepasst - 3.1 Ziel und Zweck des Dokumentes - 9 Geltungsbereich (Standorte ergänzt)	09.07.2024	4.1	ISMS-Team
Freigabe	Freigegeben durch Vorstand	10.07.2024	5.0	Vorstand
In Bearbeitung	Beschreibung angepasst - 1. Klassifizierung gelöscht - 4. Anwendung auf Normen (Norm A.17.1.1, A.17.1.2, A18.1.1 gelöscht)	07.10.2024	5.1	ISMS-Team
in Bearbeitung	1 Dokumenteninformationen - Historie und Status wurde ans Ende des Dokuments verlegt 3 Anwendung auf Normen - Umstellung auf die neuen ISO27001:2022 Corntrols	11.01.2025	5.2	ISMS-Team
in Bearbeitung	5 Leitlinie der KZVWL zur Informationssicherheit - Ausschluss des Controls A.8.30 "Ausgegliederte Entwicklung" definiert 7 Normative Grundlage und Sicherheitsziele - Schutzziele ergänzt	05.02.2025	5.3	ISMS-Team

	8 Geltungsbereich - Beschreibung der Standorte und ausgeschlossenen Dienstleistungen gelöscht 11 Berücksichtigung des Klimawandels - Punkt ergänzt			
Freigabe	Freigabe durch Vorstand	10.03.2025	6.0	Vorstand