

Informationssicherheitsmanagementsystem (ISMS)

Universitätsklinikum Leipzig AÖR

Informationssicherheits- und Datenschutz- Grundsätze (IS/DS-Grundsätze)

Ersteller	Sascha Krause
Erstellende Organisationseinheit	Stabsstelle Informationssicherheit
Revision	002/01.2023
Status (Entwurf, Prüfung, Freigabe)	freigegeben
ID-Nummer des Dokuments	53138

Inhaltsverzeichnis

1	Einleitung.....	3
2	Geltungsbereich	3
3	Informationssicherheit	3
3.1	<i>Stellenwert der Informationssicherheit</i>	<i>3</i>
3.2	<i>Stellenwert des Datenschutzes</i>	<i>4</i>
3.3	<i>Ziele der Informationssicherheit und des Datenschutzes.....</i>	<i>4</i>
3.4	<i>Informationssicherheitsgrundsätze.....</i>	<i>5</i>
3.5	<i>Datenschutzgrundsätze.....</i>	<i>6</i>
4	Organisation der Informationssicherheit und des Datenschutzes	6
4.1	<i>Methodik für die Informationssicherheit.....</i>	<i>6</i>
4.2	<i>Integriertes Managementsystem</i>	<i>6</i>
4.3	<i>Rollen und Verantwortlichkeiten</i>	<i>7</i>
4.3.1	Vorstand.....	7
4.3.2	Informationssicherheitsbeauftragte (ISB)	7
4.3.3	Datenschutzbeauftragter (DSB)	7
4.4	<i>Organisation im Unternehmen</i>	<i>8</i>
4.4.1	Zusammenarbeit	8
4.4.2	Verantwortliche von Informationen	8
4.4.3	Dokumentationssysteme	8
4.4.4	Verpflichtungen und Schulungen der Mitarbeiter	8
4.4.5	Tochtergesellschaften und externe Vertragspartner	9
5	Kontinuierliche Verbesserung.....	9
6	Verstöße und deren Folgen.....	9
7	Ausnahmen und Abweichungen.....	9
8	Verhalten bei Informationssicherheitsvorfällen und Datenschutzpannen.....	9
9	Schlussbestimmungen	9
9.1	<i>Rechenschaftspflicht</i>	<i>9</i>
9.2	<i>Aktualisierung der Grundsätze</i>	<i>10</i>
10	Inkraftsetzung	10

1 Einleitung

Als kritischer Dienstleister im Bereich Gesundheitswesen nach §8a Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) und §6 BSI-Kritis-Verordnung (BSI-KritisV) ist das Universitätsklinikum Leipzig AöR - im weiteren als UKL bezeichnet - wichtiger Bestandteil der Gesundheitsversorgung, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.

Das UKL ist sich des gesellschaftlichen Auftrags für die Gesundheit der Bevölkerung bewusst und strebt in seinem Handeln stets nach einer ganzheitlichen und individuellen Betreuung der Patienten auf höchstem medizinischen Niveau. Um diese kontinuierlich zu ermöglichen, würdigt das UKL insbesondere auch den Stellenwert ihrer informationstechnischen Systeme, Komponenten und Prozesse, deren Sicherheit für die Funktionsfähigkeit der betriebenen kritischen Infrastruktur maßgeblich ist.

Darüber hinaus verarbeitet das UKL personenbezogene Daten (pbd), deren Handhabung nach Europäischer Datenschutzgrundverordnung (DSGVO), Bundesdatenschutzgesetz (BDSG) neue Fassung und Sächsischem Krankenhausgesetz (SächsKHG) gesetzlich geregelt ist.

Zum Schutz dieser Informationswerte setzt das UKL die Anforderung des §8a BSI-Gesetz nach der Norm ISO/IEC 27001:2013 unter Berücksichtigung des Branchenspezifischen Sicherheitsstandards (B3S) für die Gesundheitsversorgung im Krankenhaus sowie der DSGVO in einem integrierten Managementsystem (IMS), bestehend aus Informationssicherheitsmanagementsystem (ISMS) und Datenschutz-Managementsystem (DSMS) um. Beide zuvor benannten Bereiche organisieren im Zusammenhang mit diesem Gesamtsystem jeweils die Zertifizierungen und Prüfnachweise soweit gesetzlich zwingend und möglich. Das UKL verpflichtet sich, dieses Managementsystem aufrechtzuerhalten und ständig zu verbessern.

2 Geltungsbereich

Die vorliegende Richtlinie ist verbindlich für alle Mitarbeiter des UKL sowie externe Dritte, die an der Erbringung der kritischen Dienstleistung nach §6 (1) BSI-KritisV beteiligt sind.

Geltende gesetzliche Regelungen und vertragliche Vereinbarungen sind gegenüber Inhalten der vorliegenden Richtlinie vorrangig einzuhalten.

Die Richtlinie wird zur Umsetzung eines IMS (Aufbau und Betrieb eines ISMS und DSMS) in folgenden Gesellschaften angewendet:

- Universitätsklinikum Leipzig AöR
- MedVZ gGmbH

3 Informationssicherheit

3.1 Stellenwert der Informationssicherheit

Informationen sind grundlegende Faktoren für die störungsfreie Bereitstellung der kritischen Dienstleistung sowie für die Erreichung der Unternehmensziele und stellen Unternehmenswerte des UKL dar. Alle wesentlichen, strategischen und operativen Funktionen und Aufgaben zur Bereitstellung der kritischen Infrastruktur werden durch informationsverarbeitende Systeme maßgeblich unterstützt. Die Definition und Umsetzung der Ziele und Grundsätze der Informationssicherheit erfolgt daher anhand der gesellschaftlichen Bedeutung und der strategischen Ausrichtung des UKL.

Die Sicherung der Informationsverarbeitung für die betriebene kritische Dienstleistung nach dem Stand der Technik ist eine zentrale Anforderung der Informationssicherheit, damit das UKL gesetzeskonform als Betreiber agiert.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

Alle Beteiligten (Kunden, Dienstleister, Lieferanten, Partner, Gesellschafter, Aufsichtsräte etc.) müssen sich darauf verlassen können, dass das UKL die Sicherheitsverantwortung für die von ihnen verarbeiteten Informationen gewissenhaft wahrnimmt und Informationen vor missbräuchlicher Verwendung schützt.

3.2 Stellenwert des Datenschutzes

Für das UKL und seine Gesellschaften ist auch der Schutz der Rechte der Betroffenen bei der Verarbeitung personenbezogener Daten und die Sicherheit aller gespeicherten und verarbeiteten Informationen wesentlich. So sind beispielsweise folgende Informationen als besonders geschäftskritisch einzustufen:

- Personenbezogene Daten besonderer Kategorie (Gesundheitsdaten der Patienten)
- Sozialdaten der Patienten
- Personaldaten
- Unternehmensdaten mit Personenbezug

Zum Schutz des UKL sowie deren Patienten und aller Geschäftspartner sind pbD vor Missbrauch und Verlust der Integrität, der Vertraulichkeit, der Verfügbarkeit und der Authentizität zu bewahren.

Nicht nur die Korrektheit der Informationen (Integrität) muss gewahrt sein, sondern auch eine rechtliche Befugnis für die Speicherung und die Verwendung der Daten muss vorhanden sein (Rechtmäßigkeit).

Weiterhin sind die Geschäftsprozesse des UKL insbesondere von einer IT-gestützten Informationsverarbeitung abhängig. Die hiermit verbundenen Risiken müssen bewertet und durch geeignete Datenschutz- / Informationssicherheits-Maßnahmen angemessen behandelt werden. Aus Sicht des Datenschutzes ist insbesondere auch die Belastbarkeit der Systeme sicherzustellen.

3.3 Ziele der Informationssicherheit und des Datenschutzes

Die Zielsetzung des IMS ist, Informationen angemessen, wirksam und durchgängig vor möglichen Gefährdungen zu schützen, die bei Eintritt zu unerwünschten Schäden führen. Im Kontext des UKL bedeutet dies die Abwendung von Schäden, welche

- die medizinische Versorgung einschränken,
- sich negativ auf die Patientensicherheit und die Behandlungseffektivität auswirken oder
- das informationelle Selbstbestimmungsrecht des Einzelnen beeinträchtigen

Die Vermeidung von Schäden geschieht im Rahmen der normativen und gesetzlichen Anforderungen durch eine kontinuierliche und wirtschaftlich angemessene Steuerung der möglichen Risiken, die in Verbindung mit der Verarbeitung, dem Transport und der Speicherung von Informationen stehen.

Die im Folgenden beschriebenen Schutzziele stellen dabei Anforderungen an die Informationsverarbeitung insb. an informationstechnische Systeme, Komponenten und Prozesse des UKL und deren Gesellschaften dar, deren Aufrechterhaltung Grundvoraussetzung für die Erreichung der oben genannten IMS-Ziele ist. Die Schutzziele der Informationssicherheit sind:

- **Vertraulichkeit**

Vertraulichkeit bedeutet Schutz vor Offenlegung von Informationen ohne Erlaubnis des Eigentümers bzw. Betroffenen. Zugriff auf Informationen darf nur von berechtigten Personen erfolgen.

- **Integrität**

Integrität bedeutet Schutz vor Änderung von Informationen durch nicht berechnigte Personen und stellt die Richtigkeit, Konsistenz und Vollständigkeit von Informationen dar.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

- **Verfügbarkeit**

Verfügbarkeit bedeutet, dass Prozesse, Informationen, Funktionen und Informationssysteme immer dann verfügbar sind, wenn ein berechtigter Benutzer sie bearbeiten bzw. in Anspruch nehmen möchte. Verfügbar heißt in diesem Zusammenhang auch, dass der Zugriff auf Daten, Informationen, Funktionen und Betriebsmittel bedarfsgerecht gewährleistet ist.

Darüber hinaus verfolgt das IMS die Sicherstellung der folgenden, sich aus den Anforderungen des Datenschutzes ergebenden Schutzziele:

- **Authentizität**

Mit dem Begriff Authentizität wird die Eigenschaft bezeichnet, die gewährleistet, dass ein Kommunikationspartner- oder -system tatsächlich derjenige/dasjenige ist, der er/das vorgibt zu sein. Bei authentischen Informationen ist sichergestellt, dass sie von der angegebenen Quelle erstellt wurden.

- **Belastbarkeit der Systeme**

Die Belastbarkeit stellt auf die Widerstandsfähigkeit (Resilienz) der Systeme gegen unerwartete Störungen ab und damit die Aufrechterhaltung der Funktionsfähigkeit bei Verletzung der Schutzziele Integrität und/oder Verfügbarkeit.

Maßgeblich für die Erreichung der oben beschriebenen Ziele des ISM sind dabei alle fünf Schutzziele. Eine Differenzierung oder Priorisierung wird hier nicht vorgenommen.

3.4 Informationssicherheitsgrundsätze

Ein Fundament dieser Richtlinie bilden die folgenden Grundsätze der Informationssicherheit, an denen sich sämtliche Sicherheitsmaßnahmen und -vorgaben ausrichten und die für alle Mitarbeiter des UKL und deren Gesellschaften verbindlich sind.

- (1) Für Unternehmenswerte wie Informationen, IT-Systeme und IT-Anwendungen sind Verantwortliche benannt, die für die Sicherheit der jeweiligen Unternehmenswerte verantwortlich sind.
- (2) Risiken aus der Nutzung der Informationen und Informationssysteme sind frühzeitig zu identifizieren und auf ein akzeptiertes Restrisiko zu minimieren.
- (3) Kosten und Nutzen von Informationssicherheitsmaßnahmen stehen in einem angemessenen wirtschaftlichen Verhältnis.
- (4) Vorgaben und Maßnahmen orientieren sich an den Anforderungen des Branchenspezifischen Sicherheitsstandards (B3S) und Good Practices zur Informationssicherheit. MUSS-Anforderungen aus dem B3S werden unter Beachtung der formalen und wirtschaftlichen Rahmenbedingung umgesetzt.
- (5) Gesetzliche, regulatorische, vertragliche und sonstige Vorgaben für die Informationssicherheit sind zu identifizieren und durch angemessene Maßnahmen umzusetzen.
- (6) Zugriff, Zugang und Zutritt zu den Informationswerten sind auf das notwendige Maß zu beschränken.
- (7) Alle wesentlichen Aktivitäten und Ereignisse im Bereich Informationssicherheit müssen transparent und im erforderlichen Umfang nachvollziehbar sein. Verfahren für den Betrieb bzw. die Wiederherstellung des Betriebes der wesentlichen Informationssysteme sind zu dokumentieren. Sofern erforderlich, ist ein Notfallplan und ein Wiederanlaufplan zu erstellen und in das Notfallmanagement des UKL zu integrieren.
- (8) Für die an der Verarbeitung von Informationen beteiligten Mitarbeiter müssen angemessene Vorkehrungen zur Gewährleistung der Vertrauenswürdigkeit getroffen werden.
- (9) Die Mitarbeiter werden hinsichtlich des sicheren Umgangs mit Informationswerten informiert, geschult und sensibilisiert. Sie sind grundsätzlich verpflichtet, die entsprechenden Vorgaben umzusetzen.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

- (10) Die Wirksamkeit der Vorgaben und Maßnahmen zur Informationssicherheit werden kontinuierlich überprüft und verbessert.

3.5 Datenschutzgrundsätze

Das Hauptaugenmerk für den Datenschutz liegt auf der Verarbeitung von pbD. Daher ist ein zweites Fundament dieser Richtlinie der Schutz von personenbezogenen Daten im Allgemeinen und für das UKL in besonderer Weise der Schutz von Gesundheitsdaten (besondere Arten personenbezogener Daten).

Zum Schutz personenbezogener Daten sind darüber hinaus und zusätzlich zu den in Kapitel 3.4 genannten Grundsätzen auch folgende allgemeine Grundsätze für die Verarbeitung zu beachten:

- (1) **Rechtmäßigkeit:** pbD dürfen nur auf Basis einer Rechtsgrundlage oder legitimiert durch eine Einwilligung des Betroffenen verarbeitet werden.
- (2) **Treu und Glauben:** pbD werden nur so verarbeitet, wie es einem redlichen und ehrlichen Verhalten gebührt.
- (3) **Transparenz:** Die betroffene Person muss über die Verarbeitung informiert werden.
- (4) **Zweckbindung:** Die Datenverarbeitung darf nur für die eindeutig festgelegten und dem Betroffenen mitgeteilten Zwecke erfolgen.
- (5) **Datenminimierung:** Die Datenverarbeitung muss auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein.
- (6) **Richtigkeit:** Die verarbeiteten Daten müssen richtig sein.
- (7) **Speicherbegrenzung:** Die Daten dürfen nur so lange gespeichert werden, wie dies für den festgelegten Zweck erforderlich ist.
- (8) Im Sinne der Datenschutzgrundsätze sind analog zur Informationssicherheit technische und organisatorische Maßnahmen zu treffen, die eine missbräuchliche Datenverarbeitung verhindern.
- (9) Hinsichtlich der Einhaltung der Datenschutzgrundsätze besteht im Geltungsbereich dieser Richtlinie Rechenschaftspflicht.
- (10) Die Wirksamkeit der Vorgaben und Maßnahmen zum Datenschutz werden kontinuierlich überprüft und verbessert.

Auf die Vorgaben des Vorstandes wird verwiesen, diese sind im Datenschutz-Management-System beschrieben.

4 Organisation der Informationssicherheit und des Datenschutzes

4.1 Methodik für die Informationssicherheit

Das IMS des UKL wird auf Basis dieser Informationssicherheits- und Datenschutzrichtlinie, sowie weiteren Richtlinien und Sicherheitskonzepten geführt. Diese sind innerhalb der relevanten Geschäftsprozesse entsprechend der Zieldefinition (Scope) im ISMS/DSMS umzusetzen. Das Rahmenwerk der Managementsysteme ist im Detail in dem jeweiligen IS-Handbuch und im DS-Handbuch beschrieben.

4.2 Integriertes Managementsystem

Als Dienstleister im Bereich Gesundheitswesen und Verarbeiter von besonderen Arten personenbezogener Daten ist das UKL auf Basis des BSI-Gesetzes und der DSGVO gesetzlich verpflichtet, gleichartige technische und organisatorische Maßnahmen zum Schutz von Informationswerten und personenbezogenen Daten zu implementieren und stetig zu verbessern. Mit der Einführung eines IMS wählt das UKL einen Ansatz, der eine

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

nachhaltige und strukturierte Herangehensweise zur Umsetzung dieser Pflicht darstellt. Darüber hinaus ermöglicht die Integration von Informationssicherheit und Datenschutz in einem gemeinsamen Managementsystem eine Vermeidung von Doppelarbeit und Überschneidungen, nutzt Synergieeffekte und bildet eine ganzheitliche Sicht auf die Unternehmensprozesse.

4.3 Rollen und Verantwortlichkeiten

Der Informationssicherheitsbeauftragte (ISB) und der Datenschutzbeauftragte (DSB) steuern, kontrollieren und entwickeln in enger Zusammenarbeit das IMS im Auftrag des Vorstandes kontinuierlich weiter. Die Aufgaben aller Beteiligten im Rahmen des IMS sind im Detail im IS-Handbuch (Informationssicherheitsrollen) und im DS-Handbuch (Datenschutzrollen) der UKL beschrieben.

4.3.1 Vorstand

Der Vorstand unterstützt als gesamtverantwortliche Instanz die Einrichtung und den Betrieb des IMS und lässt die hierfür notwendigen Ressourcen zur Verfügung stellen und übt die Dienstaufsicht über die Stabstellen DS und IS aus. Dies beinhaltet neben der Verpflichtung zur Erfüllung der Anforderungen an die Informationssicherheit und den Datenschutz auch die fortlaufende Verbesserung des IMS. Um diesen Erwartungen gerecht zu werden, sieht der Vorstand die Umsetzung und Erhaltung des IMS als eine Verpflichtung im Rahmen der laufenden Geschäftsprozesse an.

4.3.2 Informationssicherheitsbeauftragte (ISB)

Der Informationssicherheitsbeauftragte (ISB) ist der zentrale Ansprechpartner für alle Fragen der Informationssicherheit im Geltungsbereich des Informationssicherheitsmanagements des UKL. Er wird vom Vorstand des UKL bestellt.

Die unternehmensweite Richtlinienkompetenz für Informationssicherheit wird durch den ISB wahrgenommen. Diese Richtlinienkompetenz bezieht sich insbesondere auf die Planung, Umsetzung, Überwachung und Weiterentwicklung der Informationssicherheit im Sinne eines kontinuierlichen Verbesserungsprozesses.

Er ist frühzeitig in Projekte einzubinden, damit schon in der Planungsphase sicherheitsrelevante Aspekte berücksichtigt werden. Die Mitarbeiter haben sich in sicherheitsrelevanten Fragestellungen an das geltende Regelwerk zur Informationssicherheit zu halten.

Der ISB berichtet dem Vorstand des UKL regelmäßig, mindestens einmal jährlich über den aktuellen Stand zur Planung, Umsetzung und Einhaltung der Grundsätze zur Informationssicherheit.

Der ISB ist durch die Mitarbeiter in seiner Arbeit zu unterstützen. Das UKL benennt zur Unterstützung des ISB verantwortliche Ansprechpartner für die Informationssicherheit.

4.3.3 Datenschutzbeauftragter (DSB)

Der DSB hat eine Beratungs- und Überwachungsfunktion hinsichtlich der Pflicht des Vorstandes jeder (daten-) verantwortlichen Stelle zur Erbringung des Nachweises, dass ausreichende Maßnahmen zur Sicherstellung des Datenschutzes ergriffen wurden. Der DSB ist dem Vorstand des UKL direkt unterstellt. Er ist bei Anwendung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei und zur Verschwiegenheit über die Identität des Betroffenen sowie über Umstände, die Rückschlüsse auf den Betroffenen zulassen, verpflichtet, soweit er nicht davon durch den Betroffenen befreit wird. Der DSB ist bei der Erfüllung seiner Aufgaben zu unterstützen und ihm sind insbesondere, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist, Hilfspersonal sowie Räume, Einrichtungen, Geräte und Mittel zur Verfügung zu stellen.

Der DSB hat auf die Einhaltung der DSGVO, des BDSG, des SächsDSGD datenschutzspezifischer Regelungen des Sozialgesetzbuches (SGB), des sächsischen Krankenhausgesetzes (SächsKhG), sowie anderer Vorschriften für den Datenschutz hinzuwirken.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

Bei neuen Systemen oder Prozessen ist der DSB frühzeitig in Projekte einzubinden, damit schon in der Planungsphase datenschutzrelevante Aspekte berücksichtigt werden können (privacy by design, privacy by default). Der DSB ist auch über wesentliche Änderungen von Systemen mit personenbezogenen Daten zu informieren.

Der DSB berichtet dem Vorstand des UKL einmal jährlich in seinem Datenschutzbericht. Im Abstand von zwei Jahren berichtet darüber hinaus der Vorstand dem Aufsichtsrat mit Unterstützung des DSB der letzten zwei Berichtsjahre.

Neben seinem Beratungsauftrag hat der DSB die ordnungsgemäße Anwendung der Informationsverarbeitung mit Bezug auf pbD zu überwachen. Er hat darauf hinzuwirken, dass ein Verzeichnis von Verarbeitungstätigkeiten geführt wird. Hat eine Verarbeitung, insbesondere bei Verwendung neuer Technologien, voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt das UKL als verantwortliche Stelle vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. Die verantwortliche Stelle muss bei der Durchführung einer Datenschutzfolgenabschätzung den Rat des DSB einholen. Das Nähere zur Datenschutzfolgenabschätzung ist im DS-Handbuch geregelt bzw. in der Verfahrensanweisung „Datenschutzfolgenabschätzung“.

4.4 Organisation im Unternehmen

4.4.1 Zusammenarbeit

Der ISB und der DSB unterstützen sich gegenseitig bei der Erfüllung ihrer Aufgaben.

Der ISB holt zur Durchführung seiner Aufgaben bei den zuständigen Fachbereichen bedarfsgerechte Unterstützung ein. Dies betrifft insbesondere:

- Anforderungs- und Risikomanagement von Geschäftsprozessen und Anwendungen
- Umsetzung, Überwachung und Verbesserung von Sicherheitsmaßnahmen
- Behandlung von Sicherheitsvorfällen und Notfällen
- Sensibilisierung und Schulung der Mitarbeiter

4.4.2 Verantwortliche von Informationen

Die Verantwortlichen von Informationen sind dafür zuständig, Anforderungen bezüglich Bestimmung, Bewertung, Verwendung und Schutz der Informationswerte zu definieren, diese den Verarbeitern zu kommunizieren und ihre Umsetzung zu überprüfen.

4.4.3 Dokumentationssysteme

Für die digitale Erfassung von Informationen werden zum Teil spezielle Datenbanksysteme eingesetzt.

Alle Dokumente des IMS werden einheitlich und zentral im UKL Dokumentenmanagementsystem Roxtra bereitgestellt und verwaltet.

4.4.4 Verpflichtungen und Schulungen der Mitarbeiter

Ein zentrales Element des IMS ist die schriftliche Selbstverpflichtung eines jeden Mitarbeiters, sich über die geltenden Vorgaben zu Datenschutz und Informationssicherheit in der Informationsverarbeitung in Kenntnis zu setzen und diese strikt einzuhalten. Auch externe Dritte, die berechtigten Zugang zu UKL-Systemen und -Daten haben sowie Dienstleister und deren Erfüllungsgehilfen sind entsprechend zu informieren und auf die Einhaltung zu verpflichten. Für die entsprechenden vertraglichen Regelungen ist die beschaffende Stelle verantwortlich.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

Es ist von entscheidender Bedeutung für die Wirksamkeit des Datenschutzes und der Informationssicherheit, dass jeder Mitarbeiter aktiv daran mitwirkt, das erforderliche Sicherheits- und Datenschutzniveau zu gewährleisten. Dies beinhaltet neben der Einhaltung von Richtlinien und Maßnahmen auch die permanente Aufmerksamkeit bzgl. möglicher Bedrohungen und Vorfälle. Darüber hinaus sollen Verbesserungsmöglichkeiten zeitnah kommuniziert werden.

Die Mitarbeiter müssen regelmäßig, mindestens einmal jährlich an internen Schulungen zum Datenschutz und zur Informationssicherheit und der korrekten, sicheren Nutzung der IT-Services teilnehmen.

4.4.5 Tochtergesellschaften und externe Vertragspartner

Jedes Unternehmen, jede externe Stelle und jeder beteiligte Dritte, der mit dem des UKL eine datenschutz- oder informationssicherheitsrelevante Geschäftsbeziehung unterhält, verpflichtet sich zur Einhaltung der Grundsätze zum Datenschutz und zur Informationssicherheit und benennt regelhaft einen Datenschutz- / Informationssicherheits-Ansprechpartner. Die Einhaltung dieser Verpflichtung wird durch entsprechende vertragliche Vereinbarungen sowie Audits gewährleistet.

5 Kontinuierliche Verbesserung

Zur kontinuierlichen Bewertung und Verbesserung des IMS und seiner Prozesse ist die Einführung eines Auditprogramms erforderlich. Dieses bietet die Möglichkeit, Abweichungen von den Zielen der Informationssicherheit und des Datenschutzes zu identifizieren und zeitnah zu bewerten.

6 Verstöße und deren Folgen

Alle Mitarbeiterinnen und Mitarbeiter der UKL sind verpflichtet, die vorliegenden Grundsätze und zugeordneten Richtlinien einzuhalten. Über Vorfälle unter Missachtung dieser Grundsätze hat der zuständige Bereich B4 - Personal und Recht zu entscheiden.

7 Ausnahmen und Abweichungen

Abweichungen von diesen Grundsätzen sind nur in Ausnahmefällen bei zeitlich begrenzten und/oder außergewöhnlichen Umständen möglich. Diese müssen vom zuständigen Fachbereich der UKL im Vorfeld schriftlich an Informationssicherheitsbeauftragten und/oder den Datenschutzbeauftragten gemeldet und von diesen genehmigt werden.

8 Verhalten bei Informationssicherheitsvorfällen und Datenschutzpannen

Bei Informationssicherheitsvorfällen oder Verletzungen von Bestimmungen des Datenschutzes oder bei Datenpannen ist nach den jeweiligen Arbeitsanweisungen der Informationssicherheit oder des Datenschutzes zu verfahren.

9 Schlussbestimmungen

9.1 Rechenschaftspflicht

Die Einhaltung der Vorgaben dieser Richtlinie in Bezug auf die Informationsverarbeitung muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Maßnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

Ersteller: Krause, Sascha	Prüfer: IS Management Board	Freigeber: Vorstand UKL / Geschäftsführung MedVZ	Revision: 002/01.2023
Erstellende Organisationseinheit: Stabsstelle Informationssicherheit			ID Nummer: 53138

9.2 Aktualisierung der Grundsätze

Im Rahmen der Fortentwicklung des Informationssicherheits- und Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Richtlinie jährlich auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

Änderungen an diesen Grundsätzen sind genehmigungspflichtig. Die Beschäftigten und leitenden Angestellten sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

10 Inkraftsetzung

Durch die Unterzeichnung dieser Grundsätze bzw. durch deren digitale Freigabe im DMS (Roxtra) durch den Vorstand des UKL sowie der Geschäftsführung der MedVZ ist diese ab sofort gültig und in allen enthaltenden Punkten ausnahmslos anzuwenden.