edia.con gemeinnützige GmbH

Leitlinie zur Informationssicherheit

Diese Leitlinie definiert die Ziele und Grundprinzipien der Informationssicherheit sowie die primären Rollen und Verantwortlichkeiten.

Diese Leitlinie gilt für die gesamte edia.con-Gruppe und tritt am 01.06.2018 in Kraft.

Diese Version ersetzt alle vorherigen Versionen.

Version	01
Dokumentenstatus:	Version 1
Datum	08.05.2018
Dokumentationsverantwortlicher	Biche, Markus Informationssicherheitsbeauftragter edia.con

Inhaltsverzeichnis

1 Einleitung und Geltungsbereich

Informationen zählen zu den primären Vermögenswerten der edia.con-Gruppe. Informationen über Untersuchungen, Behandlungen, Diagnosen, Prozesse, Patienten, Lieferanten, Partner und Mitarbeiter sind entscheidend für die erfolgreiche Behandlung und Gesundung der Patienten und tragen wesentlich zum Unternehmenserfolg der Gruppe bei. Daher ist der Schutz und die Sicherung dieser Informationen für die Organisation von entscheidender Bedeutung, in vielen Fällen gesetzlich erforderlich und ein wesentliches Element der Unternehmensführung der edia.con-Gruppe.

Diese Leitlinie stellt die Grundlage für den Rahmen der Informationssicherheitsanforderungen der edia.con-Gruppe dar.

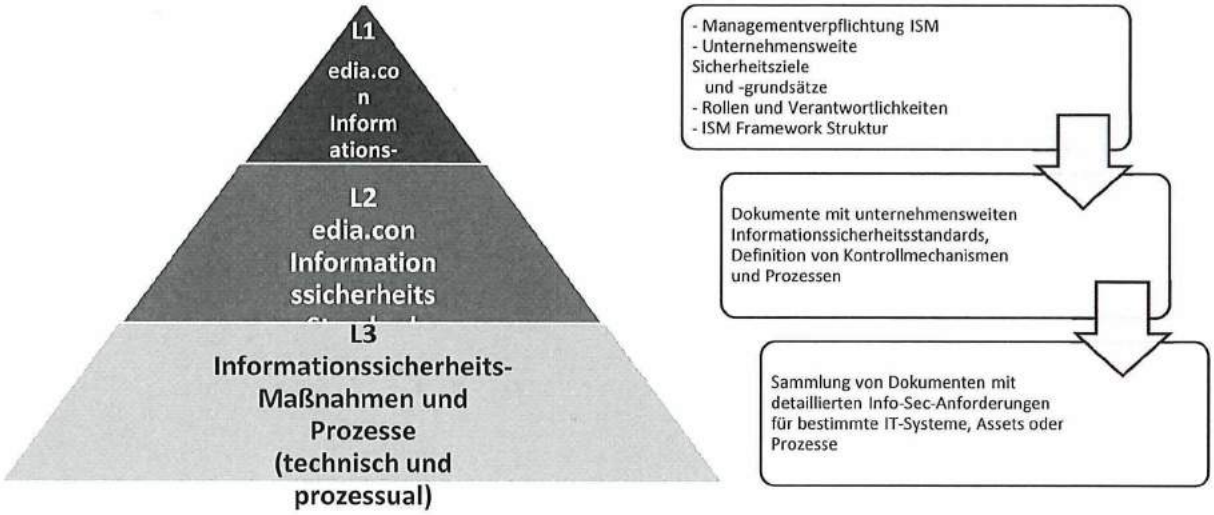
Diese Leitlinie gilt für alle Mitarbeiter der edia.con-Gruppe, verbundene Unternehmen und alle anderen Personen oder Unternehmen wie externe Partner, Lieferanten, niedergelassene Praxen oder Belegärzte, die Zugang zu Informationen der Gruppe haben oder dafür verantwortlich sind. Es liegt in der Verantwortung aller Parteien, Informationssicherheitsmaßnahmen zu unterstützen und die Anforderungen an die Informationssicherheit zu erfüllen.

2 Wesentliche Grundlagen und Ziele der Informationssicherheit

Das edia.con-Informationssicherheitsmanagement (edia.con-ISM) vermindert die Informationssicherheitsrisiken durch die Analyse von Bedrohungen der Informationssicherheit und bietet einen angemessenen Schutz durch die Umsetzung von technischen, organisatorischen und personellen Maßnahmen. Die Maßnahmen werden durch das vorab analysierte Risiko begründet.
Ziel der Informationssicherheit ist es, die folgenden drei Schutzziele zu gewährleisten:
Vertraulichkeit - Sicherstellung, dass Informationen nur für diejenigen zugänglich sind, bei denen die Notwendigkeiten und Befugnisse vorliegen
Integrität - Sicherung der Genauigkeit und Vollständigkeit der Informations- und Verarbeitungsmethoden, d.h. die Information ist echt, überprüfbar und die Übermittlung von Informationen kann nachgewiesen werden - alle Arten von Nutzern können für ihre Handlungen zur Rechenschaft gezogen werden
Verfügbarkeit - Sicherstellung, dass autorisierte Benutzer bei Bedarf auf die Informationen und zugehörigen IT-Einrichtungen und Services zugreifen können.

Die Informationssicherheitsanforderungen werden in einem globalen Information Security Management Framework gemäß ISO/IEC 27000 Serie (z. B. Informationsklassifizierung und Handhabung, Anforderungen an Passwörter, technische Anforderungen) integriert.
Informationssicherheitsregelungen, Prozesse und Methoden müssen mit dem Datenschutz und Betriebsschutz (Werkschutz), sowie mit dem Risiko-, Krisen-, und Qualitätsmanagement in Einklang gebracht werden.
Informationssicherheitsprozesse der edia.con sollen in Übereinstimmung mit den Grundsätzen dieser Leitlinien und den im edia.con-ISM festgelegten Anforderungen konzipiert und organisiert werden, um eine effiziente und konsistente Umsetzung in der gesamten edia.con-Gruppe zu gewährleisten.
Die Implementierung der ISM-Anforderungen ist in der gesamten edia.con-Gruppe zwingend erforderlich. Externe Parteien, die auf edia.con-Informationen zugreifen oder diese verarbeiten, müssen an die Anforderungen des edia.con-ISM durch vertragliche Bestimmungen gebunden sein.
Das edia.con-ISM besteht aus einem verbindlichen Regelwerk, welches Schutzziele, Sicherheits-Maßnahmen (Controls), Sicherheits-Standards sowie Implementierungsspezifikationen vorgibt, um Systeme und Prozesse sicher und vertrauenswürdig zu betreiben.

Das edia.con-ISM folgt einem 3-Schichten-Modell, bestehend aus der edia.con Informationssicherheitsleitlinie (L1), den edia.con-Informationssicherheitsstandards (L2) und aus technischen Informationssicherheits-Maßnahmen und Prozessen (L3).



1 edia.con-ISM Schichten-Modell (Framework Layer)

Der Informationssicherheits-Lenkungsausschuss ist verantwortlich für die Pflege und Überwachung der Anwendung der Informationssicherheitsdokumente in Layer 1 und definiert die Grundbestandteile, Richtwerte und wichtigen Sicherheitsmaßnahmen für die Layer 2 Dokumente.

Layer 2 und 3 Dokumente, miteingeschlossen technische und prozessuale Informationssicherheitsmechanismen werden durch das Linien Management oder nach Bedarf auch durch Sachverständigengruppen entwickelt und gepflegt.

Verweis intern:

Unternehmenstruktur der edia.con

Verweis extern:

ISO/IEC 27001:2013

OSSTMM 3.0

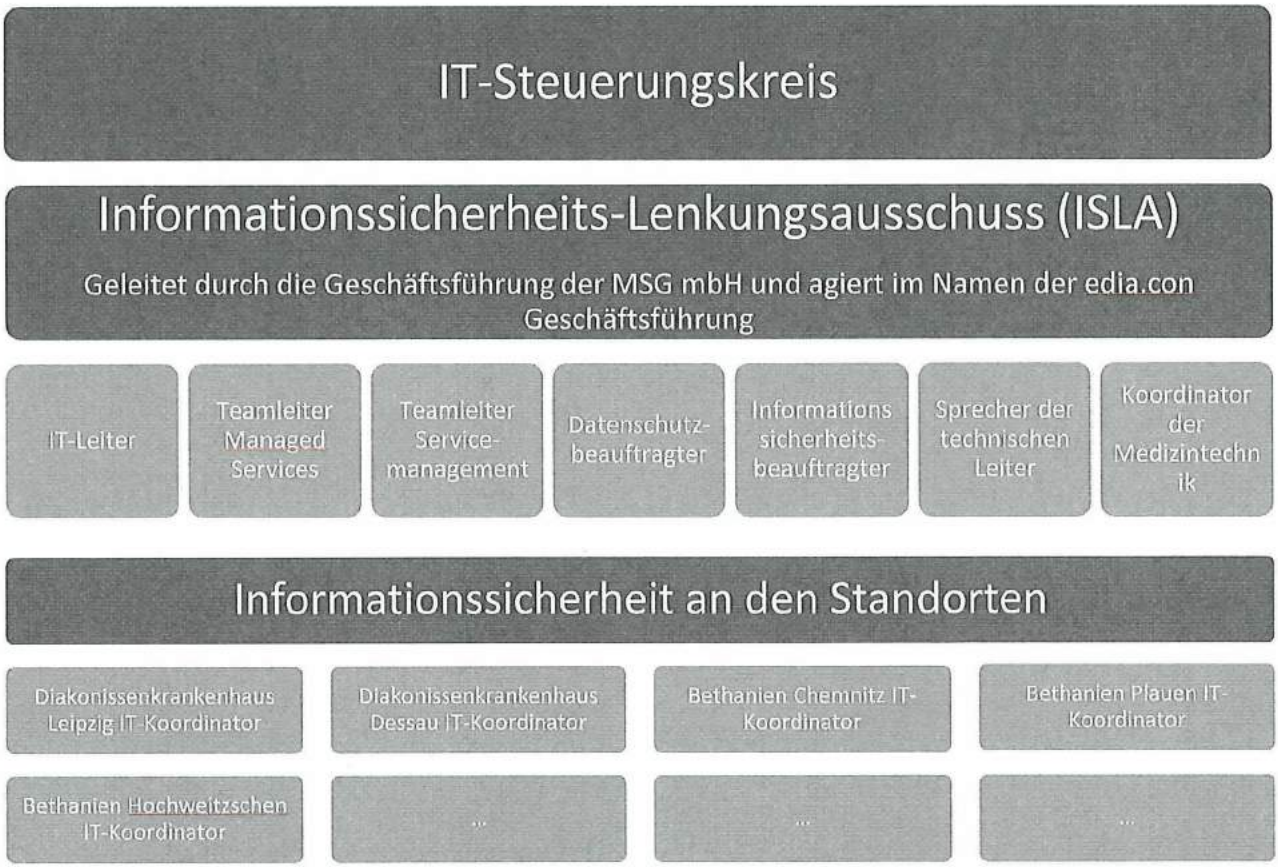
3 Primäre Rollen und Verantwortlichkeiten der Informationssicherheit

Für eine erfolgreiche Steuerung und Betrieb des edia.con-ISM sind klare Rollen, deren Zuordnung und Verantwortlichkeiten definiert.

Informationssicherheits-Lenkungsausschuss (ISLA)

Der ISLA wird von der Geschäftsführung der MSG mbH geleitet und agiert im Namen der edia.con Geschäftsführung.

Der ISLA besteht aus der Geschäftsführung der MSG mbH, dem IT-Leiter, dem Informationssicherheitsbeauftragten, dem Datenschutzbeauftragten und den Teamleitern IT-Servicemanagement und Managed Service, sowie dem Sprecher der technischen Leiter und der Koordinator der Medizintechnik. Darüber hinaus wird der ISLA durch den bereits etablierten Qualitäts- und Risikomanagementprozess begleitet.



Die Aufgaben des ISLA sind:

- Definition und Pflege der Informationssicherheits-Strategie und des Informationssicherheitsmanagementsystems
- Definition von Informationssicherheitsanforderungen, um relevante Informationssicherheitsrisiken zu mindern
- Zuweisen von Informationssicherheitsaufgaben
- Unterstützung der Geschäftsbereiche zur kontinuierlichen Verbesserung der Informationssicherheit in ihren Abteilungen
- Statusüberwachung der Informationssicherheit und Berichterstattung an die Geschäftsführung der edia.con im IT-Steuerungskreis
- Durchführung entsprechender Berichtsverfahren gemäß der Definition durch den ISLA
- Anleiten der Geschäftsbereiche, damit der sichere Umgang mit Informationen gewährleistet ist.

edia.con Informationssicherheitsbeauftragter

Der Informationssicherheitsbeauftragte informiert über sicherheitsrelevante Gesetze, Richtlinien und Rechtsprechung. Der Informationssicherheitsbeauftragte ist für die Informationssicherheitsleitlinie zuständig und überwacht deren Einhaltung. Der Informationssicherheitsbeauftragte führt regelmäßige Informationssicherheitsaudits durch. Diese Funktion koordiniert auch die Entwicklung und Umsetzung von Informationssicherheitsbestimmungen, definiert Prozesse, Methoden und Werkzeuge und überprüft deren Umsetzung.

Verweis intern:

Vertrag_Informationssicherheitsbeauftrager
Bestellung_Informationssicherheitsbeauftragter

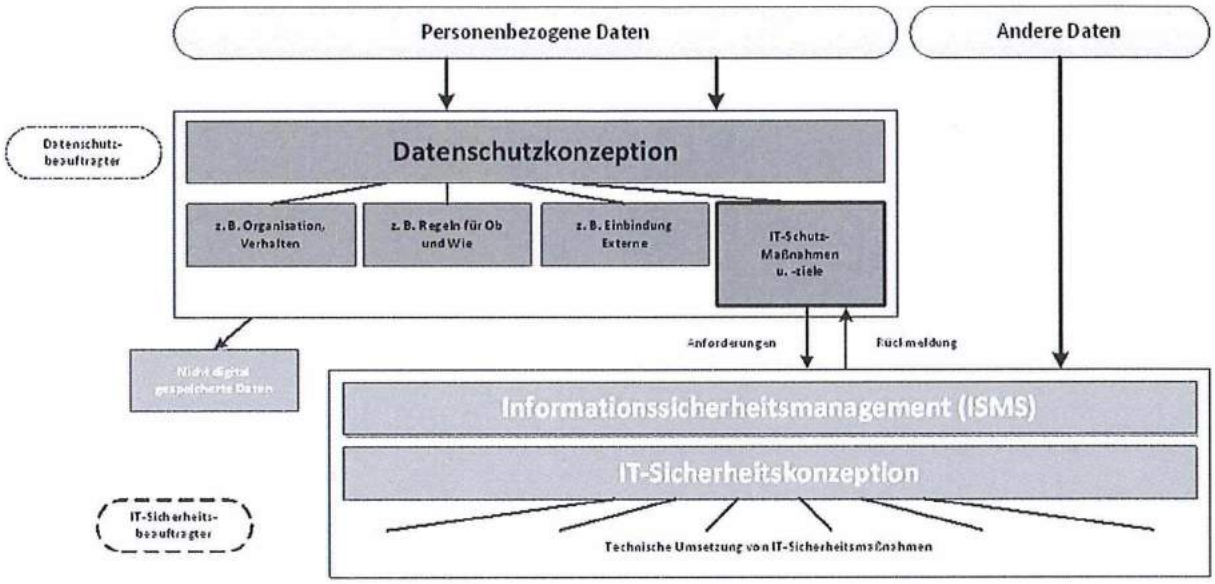
Verweis extern:

edia.con Datenschutzbeauftragter

Der edia.con Datenschutzbeauftragte überwacht die Einhaltung kirchlicher, nationaler und internationaler Datenschutzgesetze und -vorschriften. Der Datenschutzbeauftragte ist für die Datenschutzrichtlinien zuständig und überwacht deren Einhaltung. Der Datenschutzbeauftragte führt Datenschutzkontrollen und Audits durch. Die technischen und organisatorischen Maßnahmen der Informationssicherheit müssen den gesetzlichen Anforderungen des Datenschutzgesetzes entsprechen.

Es ist ein Datenschutzbeauftragter bestellt.

Die Abgrenzung zwischen Datenschutz und Informationssicherheit in der edia.con-Gruppe ist klar definiert und kann der folgenden Grafik entnommen werden:



Verweis intern
Tbd
Verweis extern
EU-DSGVO
BDSG-Neu
LKHG-Neu
DSG-EKD
OH-KIS, Weitere

Betriebsschutz (Werkschutz) der edia.con

Der Betriebsschutz ist verantwortlich für den physischen Schutz von Informationen. Dies betrifft vor allem Informationen, die nicht elektronisch abgewickelt werden. Der Betriebsschutz legt die allgemeinen Vorschriften für die Absicherung von Informationen auf dem Campus fest. Der Betriebsschutz wird bei der Untersuchung von Informationssicherheitsverletzungen, in Verbindung mit dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten unterstützend tätig.

Medizintechnik

Die Medizintechnik ist verantwortlich für die Sicherheit der Patienten, Anwender und Dritte die mit Medizingeräten oder deren Zubehör in Verbindung kommen, so dass physische Verletzungen oder Schädigungen der menschlichen Gesundheit ausgeschlossen werden können (Safety). Die Medizintechnik ist verantwortlich für die Daten-und Systemsicherheit von Medizingeräten, sowie des dazugehörigen medizinischen IT-Netzwerks. Sie achtet auf Vertraulichkeit und

Integrität von Informationen auf allen medizintechnischen Geräten, sowie deren Übertragungswegen (Daten-und Systemsicherheit). Die Verfügbarkeit von Daten und Systemen muss jederzeit gewährleistet sein (Effektivität). Die Medizintechnik legt die allgemeinen Vorschriften für die Absicherung von Informationen auf Medizingeräten und deren Übertragungswegen fest. Unterstützend kann hierzu die internationale Norm IEC 80001-1:2010 eingesetzt werden.

Es wird ein Medizintechnik-Risikobeauftragter von der edia.con-Geschäftsführung benannt, dessen Aufgabe die Etablierung und der Betrieb eines IT-Risikomanagements gemäß den Anforderungen der IEC 80001 ist.

Verweis intern
Tbd
Verweis extern
ISO 27799:2008
IEC 80001

Informationssicherheitskoordinator (InfoSiko)

In Zusammenarbeit mit dem ISLA und unterstützt vom edia.con Informationssicherheitsbeauftragten müssen die Standorte einen InfoSiko ernennen. Der InfoSiko ist verantwortlich für die Umsetzung und Verbesserung der Informationssicherheit an den jeweiligen Standorten.

Die Verantwortlichkeiten des InfoSiko sind wie folgt:

- Einrichtung eines lokalen Informationssicherheits-Forums, um Ziele und Richtlinien der zentral entwickelten Informationssicherheitsanforderungen umzusetzen und anzuwenden.
- Verbesserung der Informationssicherheit in einer strukturierten und systematischen Weise, proportional zu den Geschäftsrisiken und in Zusammenarbeit mit anderen Abteilungen
- Der InfoSiko führt kontinuierliche Hintergrundaktivität von Informationssicherheits-Spot-Checks, Tests und Selbsteinschätzungen durch, um Feedback über die Wirksamkeit von aktuellen Sicherheitsmaßnahmen und Prozessen gemäß ISLA-Anforderungen zu geben.
- Förderung des allgemeinen Bewusstseins für Informationssicherheit.

Mitarbeiter der edia.con-Gruppe

Der Mitarbeiter spielt eine wichtige Rolle, um die Informationssicherheit in seinem jeweiligen Verantwortungsbereich zu wahren. Dies geschieht durch die Einhaltung der Anforderungen der Informationssicherheit im Sinne des Information Security Managements.

Um sicherzustellen, dass keine Einzelperson - unbeabsichtigt oder vorsätzlich – Daten ohne Genehmigung oder Nachweis erlangen oder manipulieren kann, erfolgt die Trennung von miteinander im Konflikt stehenden Aufgaben und Verantwortlichkeiten.

Verweis intern:

tbd

Verweis extern:

ISO/IEC 27001:2013 Annex A 6.1

4 Wesentliche Elemente und Sicherheitsmaßnahmen

Die Grundbestandteile, Richtwerte und die wichtigen Sicherheitsmaßnahmen für das edia.con-ISM werden vom ISLA definiert und von den Leitungs- oder Sachverständigengruppen weiter dokumentiert und gepflegt.

4.1 Security Channels

Das edia.con Information Security Management gilt für folgende Security Channels:

Security Channel	Beschreibung
Faktor Mensch/ Prozess Sicherheit	Umfasst das menschliche Element der Kommunikation, wobei die Interaktion entweder physikalisch oder psychologisch ist, z.B. Betrug, Phishing, Social Engineering.
Physische Sicherheit	Umfasst die äußeren Gefahren oder Ereignisse wie z.B. Vandalismus, Sabotage, Diebstahl, Naturkatastrophen, Feuer, Terrorismus
Wireless	Besteht aus allen elektronischen Kommunikationen und Signalen, deren Ausstrahlung nicht kabelgebunden ist
Telekommunikation	Umfasst alle Telekommunikationsnetze, digital oder analog, bei denen die Interaktion über bestehende Telefon- oder telefonähnliche Netzleitungen erfolgt.
Daten Netzwerk	Besteht aus allen elektronischen Systemen und Datennetzen, in denen Interaktionen über bestehende Kabel- und Kabelnetze erfolgen

In Fällen, in denen Informationen unbekannten Interaktionen und Bedrohungen durch den Geschäftsbetrieb ausgesetzt werden, sind Sicherheitsmaßnahmen (Security Controls) ein Mittel, um die Auswirkungen der Bedrohungen und deren potentiellen Folgen entgegenzuwirken oder zu minimieren.

Als Grundlage für die Auswahl der Sicherheitsmaßnahmen dient die vom Bundesamt für Sicherheit in der Informationstechnik erstellte Studie „Durchführungskonzept für Penetrationstests". In dieser Studie wird auf das Open Source Security Methodology Manual verwiesen, welches die nachfolgenden zehn Sicherheitsmaßnahmen beinhaltet. Um die Namenkonvention zu wahren, verzichten wir auf eine Übersetzung der zehn Sicherheitsmaßnahmen. Allerdings geben wir einen Übersetzungsvorschlag.

Authentication – ist eine Kombination aus Identifikation und Berechtigung.

Indemnification – sind rechtliche Aussagen zur Schadensvorbeugung zwischen dem Informationsinhaber und den interagierenden Parteien. Die Schadensvorbeugungen können durch Warnungen über Schadensersatzforderungen, Gesetze oder Versicherungen geregelt sein.

Resilience (Widerstandsfähigkeit) – stellt sicher, dass bei Ausfall oder bei Auftreten von Limitierungen in den Information Assets bzw. bei den Sicherheitsmaßnahmen die Schutzziele weiterhin gewahrt werden.

Subjugation (Erzwingen von Sicherheitsmaßnahmen) – ist eine Maßnahme die sicherstellt, dass Interaktionen nur nach definierten Prozessen stattfinden. Der Informationsinhaber legt fest, wie die Interaktion abgesichert wird. Somit hat der Interagierende keine Entscheidung über sein Vorgehen und die Absicherung der Interaktion.

Continuity (Verfügbarkeit) – sind Maßnahmen um Interaktionen mit und zwischen den Information Assets im Falle von Ausfall oder Unterbrechung weiterhin aufrechtzuerhalten.

Non-repudiation (Unleugbarkeit) – sind Maßnahmen zur Sicherstellung von Unleugbarkeit der Interagierenden.

Confidentiality (Schutz der Information) – sind Maßnahmen, um die Information vor Offenlegung und Kenntnisnahme zu schützen.

Privacy (Schutz der Aktion) – sind Maßnahmen, um zu verbergen wie auf Informationen zugegriffen, diese angezeigt oder ausgetauscht werden.

Integrity (Veränderungskontrolle) – sind Maßnahmen, um sicherzustellen, dass Veränderungen von Informationen und Prozessen dokumentiert und den entsprechenden interagierenden Parteien mitgeteilt werden.

Alarm – sind Maßnahmen zur Alarmierung, dass ein festgelegtes Ereignis eingetreten ist.

Der Schutz von Informationen wird durch die Umsetzung einer Reihe von geeigneten Maßnahmen erreicht, dazu gehören Maßnahmen zu Richtlinien, Prozessen, Verfahren, Organisationsstrukturen sowie Software- und Hardwarefunktionen.

4.2 Management und Steuerungsbereiche

Entsprechend der ISO/IEC 27001:2013 sind folgende Management- und Steuerungsbereiche Gegenstand für die Definition, Umsetzung und Verbesserung des edia.con-ISM.

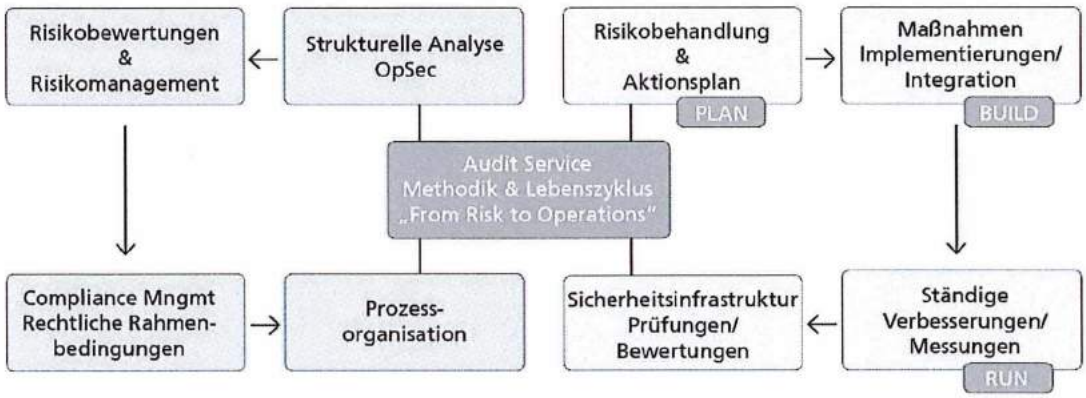
4.2.1 Informationssicherheit Lebenszyklus, Informationssicherheit in Projekten

Kontinuierliche Verbesserung der Informationssicherheit ist für jeden Service zu berücksichtigen, unabhängig von der Art der Services, um sicherzustellen, dass Informations-Sicherheitsrisiken identifiziert und adressiert werden. Dies gilt allgemein auch für jedes neue Projekt, unabhängig von seiner Ausprägung, z.B. Ein Projekt für einen Geschäftsprozess (z.B. Aufnahmeprozess, Behandlungsprozess), IT-Prozess, Facility Management Prozess und andere unterstützende Prozesse.

Es muss sichergestellt werden, dass die Informationssicherheit ein integraler Bestandteil der Informationssysteme über ihren gesamten Lebenszyklus ist.

Informationssicherheitsmaßnahmen im Entwicklungslebenszyklus der Informationssysteme ermöglichen den Schutz von Informationen gemäß deren Schutzbedarf.

Ein Informationssicherheits-Lebenszyklus wird durch organisatorische und technische Maßnahmen gepflegt und ist Teil des kontinuierlichen Verbesserungsprozesses, wie im nachfolgenden Abbild (∞) beschrieben.



Als Teil des edia.con-ISM-Lebenszyklus werden die Sicherheitsanforderungen der Informationen kontinuierlich analysiert. Dazu werden verschiedene Methoden verwendet, wie etwa die Einhaltung von Compliance-Anforderungen aus Richtlinien und Vorschriften, Risikomodellierung, Vorfallbehandlung oder die Verwendung von Benchmarks. Die Ergebnisse der Analyse werden von allen Beteiligten dokumentiert und überprüft. Informationssicherheitsanforderungen

und -Maßnahmen spiegeln den Geschäftswert der analysierten Informationen und die potenziellen negativen Geschäftsauswirkungen wider, die sich aus dem Mangel an angemessener Sicherheit ergeben könnten. Die Identifizierung und das Management von Informationssicherheitsanforderungen und damit verbundenen Prozessen sollten immer in frühen Stadien von Informationssystemprojekten integriert werden. Um effektivere und kostengünstigere Lösungen zu erreichen, wird von Anfang an eine frühzeitige Betrachtung der Anforderungen an die Informationssicherheit durchgeführt (z. B. bei der Entwurfsphase).

Verweis intern:
tbd
Verweis extern:
ISO/IEC 27001:2013 Annex A 6.1.3, Annex A 6.1.5
OSSTMM 3.0 §1.2 + §2.2

4.2.2 Informationssicherheit Risiko Management

Der Informationssicherheit-Risiko-Management Prozess wird durch die Sicherheitslinienfunktionen definiert und kontinuierlich verbessert um sicherzustellen, dass eine angemessene Risikobehandlung erfolgt, durch welche die Ergebnisse aus den Risikoanalysen in die Organisation der Informationssicherheit einfließen.
Der Informationssicherheits-Risiko-Management-Prozess ist in den edia.con-Risiko-Management-Prozess integriert und durch die Betriebsführung implementiert. Risikoverantwortliche sind verpflichtet, eine Entscheidung darüber zu treffen, wie identifizierte Risiken behandelt werden müssen.

Verweis intern:
tbd
Verweis extern:
ISO/IEC 27005:2011 Information Security Risk Management

4.2.3 Informationssicherheit im Zusammenhang mit Patientendaten

Die edia.con verwaltet sensible Informationen über personenbezogene Daten, insbesondere über den Gesundheitszustand ihrer Patienten und Bewohner.
Bei der edia.con hängt die Privatsphäre der behandelten Personen von der Wahrung der Vertraulichkeit persönlicher Gesundheitsinformationen ab. Gesundheitsinformationen müssen gegen unberechtigten Zugang, Veränderung und unberechtigte Weitergabe geschützt werden. Darüber hinaus müssen Maßnahmen zur Wahrung der Datenintegrität ergriffen werden. Es darf nicht möglich sein, die Integrität von Zugriffskontrolldaten, Audit-Trails und anderen Systemdaten so zu verändern, dass Vertraulichkeitsverletzungen stattfinden können oder diese nicht nachgewiesen werden. Gelingt dies nicht, kann dies zur Krankheit, Verletzung oder sogar zum

Tod führen. Ebenso ist eine hohe Verfügbarkeit der medizinischen Systeme elementar, da Behandlungen oft zeitkritisch sind. Ausfälle anderer, nicht-medizinischer IT-Systeme können dazu führen, dass die in medizinischen Systemen enthaltenen wichtigen Informationen nicht zur Verfügung stehen.

Verweis intern

tbd

Verweis extern

ISO/IEC 27799:2008 5.1 Ziele für die Sicherheit von Gesundheitsinformationen

Die Patienten sollen sich vertrauensvoll an die Einrichtungen der edia.con zum Zweck einer Untersuchung oder Behandlung wenden können ohne fürchten zu müssen, dass die Informationen, die sie zum Zweck der Behandlung über sich offenlegen, zu ihrem Schaden oder Nachteil genutzt werden. Daten über den Gesundheitszustand sind äußerst sensible Daten mit starkem Bezug zur Privat- und Intimsphäre. Sie geben Auskunft über seelische und körperliche Leiden, Eigenschaften und Dispositionen; sie haben über die Persönlichkeit des Menschen eine hohe Aussagekraft.

Um zu vermeiden, dass ungenaue oder unsichere Daten zu Patientengefährdungen, Datenschutzverletzungen oder Rechtsstreitigkeiten bei der edia.con führen, begründet der sehr hohe Schutzbedarf die Steuerung und Verbesserung der Sicherheitsmaßnahmen nach den höchsten Standards der Informationssicherheit, des Datenschutzes und der Datengenauigkeit. Um Integrität und Vertraulichkeit zu gewährleisten, müssen Daten und Transportwege entsprechend geschützt sein.

Der Lebenszyklus der Information muss die Schaffung, Verarbeitung, Speicherung, Übertragung, Löschung und Zerstörung beinhalten.

Es werden Vorkehrungen getroffen, um sicherzustellen, dass Mitarbeiter und Unternehmer sich ihrer Verantwortlichkeiten im Hinblick auf die Informationssicherheit bewusst sind. Darüber hinaus werden periodische Sicherheitsbewusstseinsschulungen durchgeführt, die den edia.con Mitarbeitern und Dienstleistern die Möglichkeit bieten, Patienten-Informationen durch eine sicherheitsbewusste Einstellung besser zu schützen.

4.2.4 Informationssicherheit im Zusammenhang mit der Personalabteilung

Es werden Vorkehrungen getroffen, um sicherzustellen, dass Mitarbeiter und Dienstleister ihre Verantwortlichkeiten im Hinblick auf die Informationssicherheit verstehen.

Die Personalabteilung behandelt sensible Informationen, indem sie die Einstellung und Entlassung von Mitarbeitern und Auftragnehmern und die Veränderungen im Beschäftigungsstatus verwaltet.
Der Lebenszyklus der Information muss die Schaffung, Verarbeitung, Speicherung, Übertragung, Löschung und Zerstörung beinhalten. Die Dokumentation muss in den entsprechenden oder vorhandenen Beständen gepflegt werden.
Periodische Sicherheitsbewusstseinsschulungen ermöglichen edia.con Mitarbeiter und Dienstleister die Möglichkeit, edia.con-Informationen durch eine sicherheitsbewusste Einstellung besser zu schützen.
Um zu vermeiden, dass ungenaue oder unsichere Daten zu Datenschutzverletzungen, Rechtsstreitigkeiten oder Feststellungen aus Audits n der Personalabteilung führen, erfordert der Schutzbedarf die Steuerung und Verbesserung der Sicherheitsmaßnahmen nach den höchsten Standards der Informationssicherheit, des Datenschutzes und der Datengenauigkeit.
Verweis intern:
tbd
Verweis extern:
ISO/IEC 27001:2013 Appendix A 7

4.2.5 Informationssicherheit im Zusammenhang mit Information Assets

Im Rahmen des strukturellen Risikomanagements werden alle Information Assets, kontinuierlich identifiziert und nach ihrem Schutzbedarf klassifiziert. Der Lebenszyklus der Information muss die Schaffung, Verarbeitung, Speicherung, Übertragung, Löschung und Zerstörung beinhalten. Die Dokumentation muss in den entsprechenden oder vorhandenen Beständen gepflegt werden. Der Asset Bestand muss genau, aktuell, konsistent und mit anderen Beständen abgestimmt sein. Für jedes der identifizierten Information Asset wird der Eigentümer festgelegt und eine Informationsklassifizierung durchgeführt.
Verweis intern:
tbd
Verweis extern:
ISO/IEC 27001:2013 Appendix A 8

4.2.6 Informationssicherheit im Zusammenhang mit Zugangs- und Zugriffskontrollen

Der Zugang zu Informationen und den Einrichtungen zur Informationsverarbeitung wird auf der Grundlage von Geschäfts- und Sicherheitsanforderungen gesteuert und wird in der Regel nur

auf Bedarfsgrundlage gewährt. Unbefugter Zugriff wird durch entsprechenden Maßnahmen verhindert. Zugriffskontrollen sind sowohl organisatorisch oder technisch, als auch physisch und werden gemeinsam betrachtet. Benutzer und Dienstleister erhalten eine klare Aussage über die Geschäftsanforderungen, die durch Zugangskontrollen erfüllt werden sollen.

Verweis intern:
tbd
Verweis extern:
ISO/IEC 27001:2013 Appendix A 9

4.2.7 Physische Sicherheit

Zum Schutz von Informationen und Einrichtungen zur Informationsverarbeitung vor unbefugtem Zugriff und Beschädigungen sind entsprechende Sicherheitsmaßnahmen implementiert. Das edia.con Equipment muss vor Verlust, Beschädigung, Diebstahl oder Beeinträchtigungen geschützt werden. Sicherheits-Perimeter werden definiert und verwendet, um Bereiche zu schützen, die entweder empfindliche oder kritische Informationen enthalten. Der Betriebsschutz sollte geeignete Regelungen definieren und diese kontinuierlich verbessern. Informationssicherheitsverfahren und -Maßnahmen werden verabschiedet, um zukünftige Risiken durch neue Informationstechnologie, z.B. mobile Geräte zu managen.

Verweis intern
Tbd
Verweis extern
ISO/IEC 27001:2013 Appendix A11

4.2.8 Operationelle Sicherheit

Der korrekte und sichere Betrieb von Einrichtungen zur Informationsverarbeitung stellt den Schutz der Software-Integrität sicher, garantiert die Vertraulichkeit von Informationen und die Integrität elektronischer Kommunikation.
Informationen und Einrichtungen zur Informationsverarbeitung müssen vor bösartiger Soft- und Hardware geschützt sein.
Maßnahmen zum Schutz vor Datenverlust werden umgesetzt. Relevante Ereignisse werden aufgezeichnet. Im Falle von Vorkommnissen werden entsprechenden Nachweise im Rahmen der geltenden Rechtsvorschriften erstellt.
Die Integrität der Informations-Systeme und Informationen muss zwingend gewährleistet sein. Das Ausnutzen technischer Schwachstellen muss verhindert werden.
Die dazu gehörenden Dokumentationsprozesse wie z. B. die Behandlung von E-Mail und Medien sowie die Organisation der IT Räume werden in das operative Geschäft integriert.

Kryptographie Maßnahmen werden auf Basis der Risikoanalyse und des Schutzbedürfnisses der Informationen ordnungsgemäß und effektiv eingerichtet. Die Vertraulichkeit, die Authentizität und die Integrität der Information muss gewährleistet sein. Das erforderliche Schutzniveau wird unter Berücksichtigung der Art, der Stärke und der Qualität des erforderlichen Verschlüsselungsalgorithmus festgelegt. Ein kryptographisches Key Management wird definiert, etabliert und gepflegt, einschließlich Methoden zum Umgang mit dem Schutz von kryptographischen Schlüsseln und der Wiederherstellung von verschlüsselten Informationen bei verlorenen, kompromittierten oder beschädigten Schlüsseln.

Verweis intern:
TBD
Verweis extern:
ISO/IEC 27001:213 Appendix A10, A12

4.2.9 Perimeter Sicherheit

Informationen sind vor unbefugtem Zugriff, Veränderung oder Verlust während der Übertragung nach ihrer Klassifizierung geschützt (z.B. verschlüsselt). Unternehmensnetzwerke und ihre unterstützende Einrichtungen zur Informationsverarbeitung sind entsprechend den Anforderungen an die Informationssicherheit abgesichert. Die Betriebsverantwortungen für alle Netzwerke sind zugeordnet. Sicherheitsmaßnahmen, Service Levels und administrative Anforderungen aller Netzwerkdienste werden identifiziert und in Netzwerk Service Level Agreements einbezogen, unabhängig davon, ob diese Dienste im eigenen Haus bereitgestellt oder ausgelagert werden.

Verweis intern
Tbd
Verweis extern
ISO/IEC 27001:2013 Appendix A13

4.2.10 Informationssicherheit Incident Management (Vorfalls Behandlung)

Ein konsequentes und effektives Konzept für die Verwaltung von Informationssicherheitsvorfällen, einschließlich der Kommunikation zu Sicherheitsereignissen und Schwachstellen, wird in der gesamten edia.con Gruppe etabliert. Verantwortlichkeiten und Prozesse sorgen für eine schnelle, effektive und ordnungsgemäße Reaktion auf Informationssicherheitsvorfälle.
Arbeitnehmer und Auftragnehmer kennen die Vorgehensweise und Ansprechpartner für die Meldung von Informationssicherheitsereignissen. In Fällen von Informationssicherheitsvorfällen

sind sich alle Mitarbeiter und Auftragnehmer ihrer Verantwortung bewusst und geben Informationen über Sicherheitsvorfälle so schnell wie möglich an die richtigen Stellen weiter. Typische Informationssicherheitsvorfälle sind Verstöße gegen die Integrität, Vertraulichkeit oder Verfügbarkeit von Informationen. Weitere mögliche Vorfälle sind das Auftreten von menschlichen Fehlern, Verstöße gegen Compliance-Regelungen, Verletzungen der physischen Sicherheit, unkontrollierte Systemänderungen, Funktionsstörungen von Software oder Hardware und Zugriffsverletzungen.

Verweis intern
Tbd
Verweis extern
ISO/IEC 27001:2013 Appendix A16

4.2.11 Informationssicherheitsaspekte beim Management zur Aufrechterhaltung des Krankenhausbetriebs

Die Kontinuität der Informationssicherheit ist in das Management zur Aufrechterhaltung des Einrichtungen der edia.con zu integrieren.
Der Informationssicherheitsbeauftragte ermittelt die Anforderungen an die Informationssicherheit und die Kontinuität des Informationssicherheitsmanagements bei widrigen Umständen. Hilfestellungen leisten hierzu Analyse-Prozesse wie z.B. eine Business Impact Analyse. Der IT-Leiter regelt das IT Service Continuity Management, um eine ausreichende Verfügbarkeit zu gewährleisten.

Verweis intern
Tbd
Verweis extern
ISO/IEC 27001:2013 Appendix A17

4.2.12 Aspekte der Informationssicherheit zur Compliance

Zur Vermeidung von Verstößen gegen gesetzliche, behördliche oder vertragliche Verpflichtungen im Zusammenhang mit Informationssicherheit wird ein Compliance Management für Informationssicherheit eingerichtet.
Die Geschäftsführung ist verantwortlich für die Anwendung der geltenden Gesetze, die Auswirkungen auf die Informationssicherheit haben, von z. B. personenbezogene Daten, geistiges Eigentum, Tech- und Industrie-Standards, Bug-Bounties & Hacking. Die Geschäftsleitung wird

dazu vom Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten beraten. Als gemeinnützige GmbH im Gesundheitswesen betrachtet die edia.con Gesetzgebung und Compliance im Zusammenhang mit Informationssicherheit der Evangelischen Kirche, in Deutschland und in der Europäischen Union.

Verweis intern
Tbd
Verweis extern
OSSTMM 3.0 §12, §1.6
ISO/IEC 27001:2013 Appendix A18

4.2.13 Informationssicherheitsaspekte zu Externen und mit Outsourcing-Partnern

Mit externen Partnern, die Zugang zu edia.con Informationen haben, werden Informationssicherheitsanforderungen und -Maßnahmen zur Minderung der Risiken definiert. Diese werden durch den internen Lieferantenkontakt rechtsverbindlich vereinbart und dokumentiert.
Der interne Lieferantenkontakt muss sicherstellen, dass die Services durch externe Parteien regelmäßig überwacht und auf Informationssicherheit überprüft werden. Der interne Lieferantenkontakt muss ebenfalls sicherstellen, dass Informationssicherheitsrisiken, die sich aus Änderungen der Erbringung von Dienstleistungen ergeben, ebenso in den Informationssicherheitsprozess aufgenommen werden.

Ein standardisierter Prozess- und Lebenszyklus für die Verwaltung der Anforderungen an die Lieferanten-Sicherheit wird festgelegt und die Mindestanforderungen an die Informationssicherheit und die Art des Zugangs sind Teil des Lieferantenvertrages, basierend auf einem entsprechenden Risikoprofil. Der Kontakt mit den Behörden wird nach den Vorschriften der zuständigen Unternehmensfunktionen durchgeführt.

Verweis intern
Tbd
Verweis extern
OSSTMM 3.0 §4

5 Messung/Monitoring

Die Überwachung der Einhaltung der Anforderungen an die Informationssicherheit wird gewährleistet durch:

- Selbständige Informationssicherheitschecks der Geschäftsbereiche
- Laufende Assessment-Programme des Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten
- Informationssicherheitsstatusberichte, die halbjährlich von allen Geschäftsbereichen dem Info-SiBe zur Verfügung gestellt werden, mit dem Ziel wichtige Potenziale zur Verbesserung der Informationssicherheit zu identifizieren.

Verweis intern

Tbd

Verweis extern

OSSTMM 3.0 §4

ISO/IEC 27004:2009 Information Security Management

6 Beratung und Support

Informationssicherheit betrifft jeden Mitarbeiter, jeden Auftragnehmer und Lieferanten. Jede Person ist verantwortlich für die Informationen der edia.con-Gruppe die sie verarbeitet.

Bei Fragen zur Informationssicherheit können die Mitarbeiter den zuständigen Informationssicherheitsbeauftragten bei Bedarf auch vertraulich kontaktieren. Eine Liste der jeweiligen Informationssicherheitsbeauftragten/koordinatoren finden Sie in der QM-Prozesslandkarte.

7 Angewandte Dokumente

Im Nachfolgenden finden Sie die Liste der Dokumente auf die in dieser Leitlinie referenziert wird.

Verweise intern:
Vertrag_Informationssicherheitsbeauftrager
Bestellung_Informationssicherheitsbeauftragter

... Tbd

Verweise extern:
ISO/IEC 27001:2013 Information Security Management
ISO/IEC 27004:2009 Information Security Measurement
ISO/IEC 27005:2011 Information Security Risk Management
ISO/IEC 27799:2008 Medizinische Informatik – Sicherheitsmanagement im Gesundheitswesen
OSSTMM 3.0
IEC 80001:2010 Risikomanagement für medizinische IT-Netzwerke
EU-DSGVO
BDSG-Neu
DSG-EKD
LKHG-Neu
OH-KIS, Weitere

8 Glossar

Acronym	Beschreibung
BDSG	Bundesdatenschutzgesetz
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland
EU-DSGVO	EU-Datenschutz-Grundverordnung
IEC	Internationale Elektrotechnische Organisation
Information Asset	Inhaltlich bedeutender Teil einer Abbildung, eines Textes oder eines Musters
InfoSibe	Informationssicherheitsbeauftragter
InfoSiko	Informationssicherheitskoordinator
ISLA	Informationssicherheit Lenkungsausschuss
ISMS	Information Security Management System
ISO	Internationale Organisation für Normung
LKHG	Landeskrankenhausgesetz
MSG mbH	Management- und Servicegesellschaft für soziale Einrichtungen mbH (Ein Unternehmen der edia.con-Gruppe)
OH-KIS	Orientierungshilfe-Krankenhausinformationssystem
OSSTMM	Open Source Security Testing Methodology Manual
SLA	Service Level Agreements
∞	Kontinuierliche Unendlichkeit (liegende Acht)

9 Inkrafttreten

Die vorstehende Leitlinie zur Informationssicherheit tritt mit Wirkung zum 01.06.2018 in Kraft.

Leipzig, den

Hubertus Jaeger
Geschäftsführer edia.con

Pastor Frank Eibisch
Geschäftsführer edia.con

Cornelia Schricker
Geschäftsführerin MSG mbH

Lars Forchheim
Leiter IT und Organisation

Markus Biche
Informationssicherheits-
beauftragter