Richtlinie

INFORMATIONSSICHERHEITSRICHTLINIE

RICHTLINIE ZUM INFORMATIONSSCHUTZ

Version	8.0
Klassifikation	öffentlich/public
Status	Genehmigt
Letzte Änderung	08.11.2024
Verantwortung	ISMS

akquinet
Outsourcing & Services
Werner-Otto-Straße 6
22179 Hamburg

Vorlagenversion 7.0

0. Dokumenteninformation

0.1. Zuständigkeiten

Rolle	Firma/Abteilung	Zuständigkeit
Bearbeiter	AKQUINET / ISMS	Erstellung und Pflege
Genehmiger	AKQUINET / Geschäftsführung	Prüfung und Freigabe

Tabelle 1: Zuständigkeiten

0.2. Änderungshistorie

Dieses Dokument ersetzt das Dokument <Informationssicherheitsleitlinie.docm> (Informationssicherheitsrichtlinie) mit der Version <8.0> vom <12.11.2018>. Das vorhergehende Dokument wurde archiviert. Die Versionierung des neuen Dokumentes beginnt mit *Version 0.1*. Bei Bedarf kann Einsicht in das alte Dokument sowie vorherige Versionen über dokumentenverwaltung-oss@akquinet.de beantragt werden.

Die Änderungshistorie wird in der Dokumentenverwaltung gepflegt.

Änderungen zur Vorversion sind in der Datei durch Ansicht der Überarbeitungsfunktion sichtbar zu machen bzw. können über die Vergleichsfunktion in MS Word nachvollzogen werden.

0.3. Verteiler

- Geschäftsführer
- Mitarbeiter
- IS-Manager
- Öffentlichkeit

0.4. Vereinbarung zum Dokument

Die in diesem Dokument enthaltenen Informationen und Ergebnisse einschließlich der enthaltenen Anlagen sind urheberrechtlich geschützt. Eine Verwendung außerhalb des akquinet Unternehmensverbundes ist nur nach vorheriger Zustimmung zulässig.

Ferner gilt dies für die Übernahme der vorgeschlagenen Vorgehensweise, die Einsichtnahme Dritter, sowie die Vervielfältigung, Bearbeitungen, Übersetzungen, Mikroverfilmung und die Einspeicherung und Verarbeitung in elektronischen, nachrichtentechnischen oder optischen Systemen.

Ausgenommen von dieser Vereinbarung sind allgemein bekannte Informationen und Literatur, welche zum Erstellen der Bestandsaufnahme herangezogen wurden.

0.5. Inhalt und Umfang dieses Dokumentes

- Dieses Dokument bildet die Informationssicherheitsleitlinie des ISMS

0.6. Mitgeltende Dokumente

Dokumentenname	Beschreibung
oss-rtl—interessierte Parteien (seit dem 02.10.2020 Inhalt der Informationsicherheitsrichtlinie	Interessierte Parteien und deren Anforderungen
oss-rtl—ISMS-Scope (seit dem 02.10.2020 Inhalt der Informationsicherheitsrichtlinie	Anwendungsbereich des ISMS

Tabelle 2: Mitgeltende Dokumente

Inhaltsverzeichnis

1. Informationsicherheitsrichtlinie (IS-Richtlinie)

1.1. Zweck und Bedeutung der IS-Richtlinie

Die Sicherstellung der Informationssicherheit sowie Verfügbarkeit von Kundendaten ist ein wesentliches Vertrauensmerkmal für die Zusammenarbeit mit Kunden, für die die akquinet Services in ihren Rechenzentren erbringt. Die sichere Verarbeitung von Informationen und Bereitstellung von IT-Systemen mit Schutz vor Fremdzugriff und unautorisierten Veränderungen (Datenintegrität), sowie Verfügbarkeit, Vertraulichkeit und Schutz vor Datenverlust, ist zur Sicherstellung eines reibungslosen Ablaufes der IT-gestützten Geschäftsprozesse unserer Kunden unerlässlich. Damit dies gewährleistet werden kann betreibt akquinet ein Informationssicherheits-Managementsystem (ISMS).

Die Informationssicherheitsrichtlinie ist das Fundament des ISMS und beinhaltet grundlegende Vorgaben und Leitsätze sowie den Anwendungsbereich des Managementsystems. Dieses Dokument bildet darüber hinaus eine Schnittmenge mit der Datenschutzrichtlinie und erweitert diese an verschiedenen Stellen. Innerhalb des Anwendungsbereichs des ISMS besitzt die Informationssicherheitsrichtlinie unbegrenzt Gültigkeit.

1.2. Informationssicherheitspolitik

Es ist unser Ziel, die Geschäftsfähigkeit unserer Kunden durch verfügbare IT-Systeme in den Rechenzentren der akquinet sicher zu stellen und durch Vermeidung von Sicherheitsvorfällen und Reduzierung von Bedrohungen, ein potenzielles Schadensrisiko dieser zu minimieren. Der Schutz von Informationen und Systemen ist damit von besonderer Wichtigkeit. Als IT-Dienstleister verpflichten wir uns daher, neben unseren Eigensystemen auch Fremdsysteme unserer Kunden entsprechend zu schützen. Die Integrität, Verfügbarkeit und Vertraulichkeit werden dabei stets im Rahmen vertraglicher Verpflichtungen gewährleistet.

Schadensfälle mit hohen finanziellen Auswirkungen müssen verhindert werden. Risikominimierende Sicherheitsmaßnahmen müssen dabei in einem wirtschaftlich vertretbaren Verhältnis zum Wert der schützenswerten Informationen und IT-Systemen stehen. Sicherheitsmaßnahmen können sich auch auf unsere Kunden auswirken, sodass Mitwirkungsleistungen vertraglich geregelt werden müssen.

Zur Umsetzung der Sicherheitsmaßnahmen hat das Management die Aufgabe ausreichend Ressourcen zur Verfügung zu stellen. Jeder Mitarbeiter ist außerdem dafür verantwortlich, dass die Sicherheitsanforderungen in ihrem Bereich umgesetzt und eingehalten werden.

Gesetzliche Verpflichtungen müssen beachtet werden. Als Dienstleister werden wir daher die für uns relevanten Gesetze und Bestimmungen einhalten. Unsere Kunden unterstützen wir beim Nachweis gegenüber ihren Kontrollinstanzen, um deren Anforderungen an die von uns erbrachten Dienstleistungen zu erfüllen.

Das Management wird mit dieser Richtlinie verpflichtet nach den hier genannten Vorgaben und Leitsätzen zu handeln und das ISMS bestmöglich zu unterstützen (siehe auch 1.7).

1.3. Kontext der Organisation - intern & extern [NormRef.:4.1]

Extern: Gesellschaften der akquinet Gruppe akquinet outsourcing gGmbH, akquinet business service GmbH und akquinet hosting services GmbH erbringen IT-Services im Bereich Housing, Infrastructure as a Service, Managed Services, Hosting und Full Outsourcing. Nach außen tritt die Akquinet Gruppe in der Regel als akquinet GmbH auf. Die Unternehmensgruppe ist in diesem Kontext an langfristigen und vertrauensvollen Kundenbeziehungen interessiert, da die angebotenen Lösungen sehr sensible und schutzbedürftige Daten verarbeiten und deren Sicherheit für Kunden geschäftskritisch ist.

Intern: Unternehmen der akquinet Gruppe erbringen vielfältige Lösungen im IT-Umfeld. Hierfür greifen die Unternehmen auf Dienste, die durch die im externen Kontext genannten Gesellschaften erbracht werden, zurück. Dies entspricht dem Wesenskern der akquinet Gruppe – Zusammenarbeit unter spezialisierten Organisationen, um ein größeres Ganzes schaffen zu können.

1.4. Interessierte Parteien [NormRef.:4.2]

Die nachfolgende Tabelle führt die wesentlichen Interessierten Parteien auf und benennt deren Anforderungen, um ein angemessenes Schutzniveau der relevanten Informationen zu erreichen. Die Anforderungen der interessierten Parteien werden in der Arbeit des ISMS und insbesondere bei der Erstellung des Managementberichtes berücksichtigt.

Kontext	Interessierte Partei	Anforderung
Extern	Kunden	Kunden sind in Ihrem Geschäftsumfeld auf die von akquinet zugesagte Sicherheit als kritischen Erfolgsfaktor im Rahmen ihrer eigenen Leistungserbringung angewiesen (häufig Vorbedingung / Unterstützung für weitergehende interne Auditierung / Zertifizierung ist Auswahlkriterium). Dadurch erwarten Kunden, dass das Schutzniveau hinsichtlich der Vertraulichkeit, Verfügbarkeit und Integrität, der durch akquinet verarbeiteten Daten stets unter Berücksichtigung der Implementierungskosten und unterschiedlicher Eintrittswahrscheinlichkeiten sowie Schwere der Risiken gewahrt bleibt. Hierzu gehören insbesondere jedoch nicht ausschließlich: • hohe Verfügbarkeit sowie Widerstandsfähigkeit der Dienste und der RZ-Infrastruktur inkl. regelmäßiger Wartung und Durchführung von Redundanztests, • sicherer und kontrollierter Zutritt zu den Rechenzentren und Gebäuden von akquinet, • kontinuierliche Überwachung von sowie zeitnahe Reaktion auf Sicherheitsereignisse und strukturierter Umgang mit Sicherheits- und Datenschutzvorfällen, • Anwendung einer risikobasierten Vorgehensweise zur Verwaltung von Zugriffen und Berechtigungen, zur Durchführung von nachvollziehbaren Änderungen an Systemen und zum Umgang mit technischen Schwachstellen. • Schaffung einer sicherheitsbewussten Organisation inkl. Richtlinien und Prozesse zur strukturierten Bewältigung von Risiken im Bereich der Informationssicherheit und des Datenschutzes sowie zur Beachtung der Geheimhaltungspflicht und der relevanten gesetzlichen Anforderungen.
Intern	Gesellschaften der akquinet Gruppe	Unternehmen der akquinet Gruppe erbringen vielfältige Lösungen im IT-Umfeld. Hierfür greifen die Unternehmen auf Dienste, die durch die im externen Kontext genannten Gesellschaften erbracht werden, zurück. In dieser Beziehung deckt sich die Erwartungshaltung der internen Gesellschaften der akquinet Gruppe mit den weiter o.g. Erwartungen der Kunden. Grundvoraussetzung für die Zusammenarbeit zwischen allen Beteiligten ist allerdings die Beachtung der Mindestvorgaben, die im Rahmen des DSMS für alle Gesellschaften der akquinet Gruppe bindend sind. Außerdem spielt die Vertragssicherheit, pünktlicher Geldeingang und korrekte inter-company Abrechnung sowie Leistungsabgrenzung eine wichtige Rolle.
Intern	Eigentümer (Beirat / Investoren)	Die Eigentümer sind insbesondere an der wirtschaftlichen Stabilität und Weiterentwicklung des Unternehmens interessiert. Sicherheit der Rechenzentren wird dabei als ein wesentliches Qualitäts- und Differenzierungsmerkmal am Markt erachtet. Mögliche Sicherheitsvorfälle können den Unternehmenswert gefährden. Schäden und Strafen das Ergebnis beeinträchtigen. Für besonders wichtig werden folgende Punkte erachtet:

		• Förderung der Integration von Menschen mit Handicap zur Wahrung des Gesellschaftsauftrages • Einhaltung der gesetzlichen Vorgaben • Vermeidung möglicher Sicherheits- und Compliance-Risiken
Intern	Mitarbeiter	Mitarbeiter benötigen Informationen sowie Handlungsvorgaben und sind an Handlungssicherheit interessiert. Darüber hinaus spielen folgende Aspekte eine wichtige Rolle in der Zusammenarbeit: • Guter Umgang, Verlässlichkeit und Stabilität des Unternehmens • Vertragssicherheit, pünktliche Gehaltszahlung, korrekte Abführung von Abgaben • Sicherheit am Arbeitsplatz • Vertraulichkeit der personenbezogenen Daten
Extern	Lieferanten	Lieferanten müssen über ISMS-Anforderungen informiert sein, da sie nur so diese Anforderungen erfüllen können. Zwischen den beiden Parteien bestehen außerdem folgende Anforderungen hinsichtlich der Zusammenarbeit: • Abnahmesicherheit, fairer Umgang • Einhaltung von vertraglichen Bestimmungen wie z.B. Lizenzbestimmungen oder Zahlungszielen • Kenntnis und Einhaltung der IS-relevanten Vorgaben und Richtlinien
Intern	Geschäftsführung	Die Geschäftsführung hat die Verantwortung für die Identifizierung und Behandlung von Risiken und die Einhaltung der daraus abgeleiteten Richtlinien sowie technischen und organisatorischen Maßnahmen. Des Weiteren ist die Geschäftsführung daran interessiert eine vertrauensvolle Arbeitsatmosphäre und sichere Arbeitsumgebung zu schaffen sowie ein hohes Sicherheits- und Compliance-Niveau zu erreichen. Auch die Vermittlung von Werten und Ethik spielt eine wichtige Rolle.
Extern	Aufsichtsbehörden (Datenschutz)	Die Aufsichtsbehörden kontrollieren die Einhaltung von Regularien und geben Orientierungshilfen heraus. Darüber hinaus wird erwartet, dass das Unternehmen • die datenschutzrechtlichen Vorgaben kennt, befolgt sowie • technische und organisatorische Maßnahmen ergreift, um ein angemessenes Sicherheitsniveau abhängig vom Stand der Technik, den Implementierungskosten und der Art, dem Umfang und dem Zweck der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen zu gewährleisten.
Extern	Öffentlichkeit	Die Öffentlichkeit ist an innovativen Produkten und Dienstleistungen sowie Nachhaltigkeit und Wirtschaftlichkeit interessiert. Auch die Entwicklung und Einhaltung eines Umweltbewusstseins im unternehmerischen Kontext spielt zunehmend eine wichtige Rolle. Im Vordergrund stehen außerdem die Aktivitäten im Rahmen des Gesellschaftsauftrages zur Förderung der Integration von Menschen mit Handicap. Bei der Behandlung von Sicherheitsvorfällen oder im Rahmen des Business Continuity Managements kann es ebenfalls

		notwendig sein die Öffentlichkeit zu informieren. Auch hinsichtlich der Compliance mit DSGVO müssen hierbei gesetzliche Datenschutzanforderungen Beachtung finden.
Extern	Angreifer	Angreifer versuchen gezielt und absichtlich auf IT-Systeme zuzugreifen, um an bestimmte Informationen zu gelangen, die nicht für Angreifer bestimmt sind, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gefährden, für das Unternehmen schädliche Aktionen auszulösen oder Ressourcen für eigene Zwecke zu nutzen (Black Hat-Hacker). Hieraus resultiert die Notwendigkeit Informationen über aktuelle Bedrohungen der Informationssicherheit und beteiligte Akteure zu sammeln und auszuwerten, um Erkenntnisse hinsichtlich der Risiken gewinnen und daraus Gegenmaßnahmen ableiten zu können. Darüber hinaus gibt es Angreifer, die ihre Fähigkeiten zur Offenlegung von Sicherheitslücken nutzen, um Organisationen vor anderen Angreifern zu schützen und die Öffentlichkeit über mögliche Gefahren aufzuklären (White Hat-Hacker, Sicherheitsforscher, PenTester). Solche Personen erwarten von der Organisation einen möglichst offenen und transparenten Umgang mit Sicherheitslücken sowie eine möglichst realistische Einschätzung der Gefahrensituation und eine unverzügliche Reaktion mit korrigierenden und/oder präventiven Maßnahmen.
Extern	Versicherer	Versicherer haben ein Interesse daran, dass das versicherte Unternehmen möglichst strukturiert mit Risiken umgeht und diese sowohl auf der organisatorischen als auch auf der technischen Ebene auf ein akzeptables Maß dauerhaft reduziert werden.
Extern	Finanzierer/Banken	Finanzierer / Banken sind an der Beständigkeit, wirtschaftlichen Stabilität und Weiterentwicklung des Unternehmens interessiert. Die Bewertung erfolgt maßgeblich mit Hilfe der wirtschaftlichen KPIs und Prozesskennzahlen der Organisation.

Tabelle 3: interessierte Parteien (allgemein)

Darüber hinaus sind folgende interessierte Parteien für spezifische Dienste (eHealth Dienste) von Bedeutung:

Kontext	Interessierte Partei	Anforderung
Intern	Geschäftsführung HSE	Die akquinet hse Geschäftsführung erwartet, dass • über eHealth Dienstleistungen übermittelte Daten vertraulich bleiben; • alle Daten über Anwender vertraulich bleiben (Nutzungsverhalten); • dass die eHealth Dienstleistungen und der Support verfügbar sind. *Bemerkung: Der Kundenkreis selbst kann nicht vertraulich bleiben, denn dieser wird bei der gematik über einen Directory Service innerhalb der TI öffentlich gemacht.*
Extern	Leistungsempfänger (Anwender und Kunden)	Anwender und Kunden erwarten, dass • die Patientendaten vertraulich bleiben; • dass ihre eigenen Nutzungsdaten vertraulich bleiben; • dass niemand unter ihrer Identität unberechtigterweise eHealth Dienstleistungen nutzen kann;

		• das gesendete Daten nicht unterwegs verfälscht werden; • dass die eHealth Dienstleistungen und der Support verfügbar sind. *Bemerkung: Der Kundenkreis selbst kann nicht vertraulich bleiben, denn dieser wird bei der gematik über einen Directory Service innerhalb der TI öffentlich gemacht.*
Extern	Gematik	Die gematik erwartet von akquinet hse als Anbieterin von eHealth Dienstleistungen, dass Informationssicherheit nach ISO 27001 umgesetzt, gesteuert und gelebt wird. Bedeutet: Vertraulichkeit (Nutzerdaten, Logs und Emails bleiben geheim, Emails sind nur vom korrekten Empfänger abrufbar); Integrität: Absender sind korrekt (können nicht unter verfälschten Identitäten senden), Daten in den Emails kommen genauso an wie sie abgesendet worden sind; Verfügbarkeit sowohl des Supports als auch der eHealth Dienstleistungen. Datenschutz: gem. DSGVO, gesteuert über ein Datenschutzmanagementsystem.
Extern	Patienten (nur mittelbar, da Patienten keine Nutzer von eHealth Dienstleistungen sind)	Patienten erwarten, dass ihre personenbezogenen Daten • vertraulich bleiben, d.h. nur dem Absender und Empfänger bekannt sind; • unverfälscht bleiben, d.h. genauso dem Empfänger zugestellt werden, wie der Absender sie abgesandt hat; • zu jeder Zeit zur Verfügung stehen, so dass der Absender sie jederzeit senden und Empfänger sie jeder erhalten kann.
Extern	Partner	Partnerunternehmen, die mit akquinet hse gemeinsam eHealth Dienstleistungen anbieten, erwarten, dass akquinet hse ihnen genaue Vorgaben macht bzgl. des Levels an Datenschutz und Informationssicherheit, die sie sicherstellen sollen.

Tabelle 4: interessierte Parteien für spezifische Dienste (eHealth Dienste)

1.5. Anwendungsbereich des ISMS [NormRef.:4.3]

Der Anwendungsbereich des ISMS bildet die Grundlage für die Ermittlung der Werte, die einen Bedarf an Informationssicherheit besitzen. Als IT-Dienstleister verpflichtet sich akquinet, auch kundeneigene Assets, die im Anwendungsbereich des ISMS sind, zu schützen. Die Qualität des Schutzes soll durch das etablierte Informationssicherheits-Managementsystem (ISMS) geprüft und gewährleistet werden.

Das ISMS sichert die Services Housing und Managed Hosting unter der Prämisse der Informationssicherheit und damit, dass Integrität, Verfügbarkeit und Vertraulichkeit stets gewahrt bleiben. Unter Housing wird die Unterbringung physischer Systeme (Server, etc.) von Kunden, im Rechenzentrum HH der akquinet verstanden. Beim Managed Hosting handelt es sich um den Betrieb der IT-Infrastruktur, der Plattform, des Managed OS und der Middleware sowie der Netzwerkinfrastruktur für die Kunden der akquinet unterstützt durch die Supporting Services. Siehe hierzu die schematische Darstellung in Tabelle 6.

Das ISMS bezieht sich ausschließlich auf die o.g. Services, die an den Rechenzentrumsstandorten RZ-AKQ-HAM-01, RZ-AKQ-HAM-02 und RZ-AKQ-NOR-01 erbracht werden. Der Standort Itzehoe unterliegt nicht dem Geltungsbereich des ISMS.

Übersicht ISMS-relevanter Gesellschaften der akquinet Gruppe:

Unternehmen	Aufgaben im ISMS-Kontext	Services
akquinet GmbH	Entspricht den Vorgaben des ISMS für die im Anwendungsbereich relevanten Prozesse und gibt den Handlungsrahmen für die Akquinet Gesellschaften vor.	Finanz- und Rechnungswesen, Einkauf & Admin, Marketing, Presse & Öffentlichkeitsarbeit, Org-IT, Personal
akquinet outsourcing gGmbH	Hält die ISO 27001 Zertifizierung, betriebt das ISMS und bestimmt maßgeblich die einzuhaltenden Prozesse und Richtlinien	Housing, Managed Services, Hosting und Full Outsourcing
akquinet business service GmbH	Setzt die Vorgaben des ISMS um und nutzt die zentralen Prozesse	
akquinet hosting services GmbH	Setzt die Vorgaben des ISMS um und nutzt die zentralen Prozesse	
akquinet health service GmbH*	Überträgt die Verantwortung für den Betrieb des ISMS im servicespezifischen Kontext eHealth Dienste an die akquinet outsourcing gGmbH	Lösungen das Gesundheitswesen (eHealth Dienste z.B. KIM, Basis Consumer)
akquinet nx2 GmbH*	Entspricht den Vorgaben des ISMS	Betrieb eHealth Dienste

Tabelle 5 - Übersicht ISMS-relevanter Gesellschaften der akquinet Gruppe

** Die mit dem Stern gekennzeichneten Gesellschaften befinden sich zwar im Anwendungsbereich des ISMS und unterliegen den Vorgaben. Dieser servicespezifische Teilbereich des ISMS muss jedoch gemäß den Vorgaben der Gematik nicht zertifiziert sein und wird aus diesem Grund von der Zertifizierung ausgenommen.*

Übersicht ISMS-relevanter Dienste

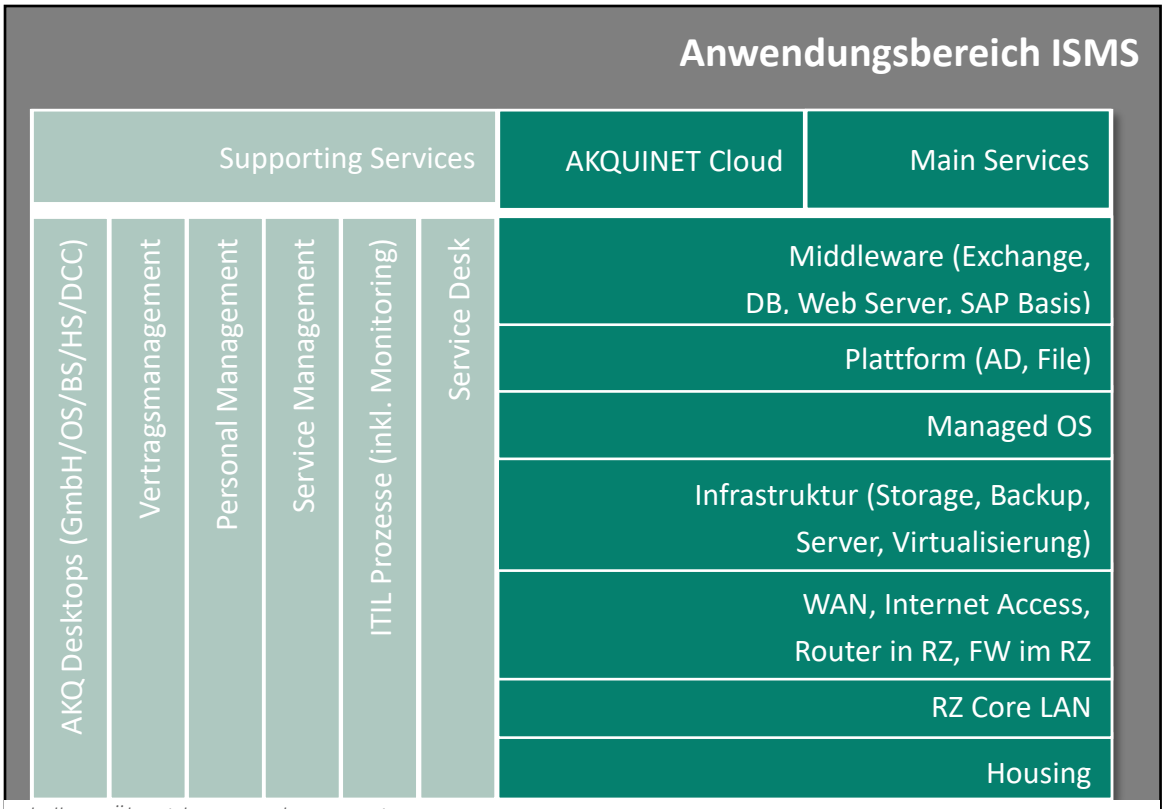

Tabelle 6 - Übersicht ISMS-relevanter Dienste

Erläuterung der Main Services:

Main Service	Beschreibung des Services
Middleware	AKQUINET betreibt für sich selbst und für Kunden Middleware Lösungen wie MS Exchange Mailserver, Datenbank Management Systeme, Web Server und SAP. Diese stellen entweder selbst einen Service dar oder dienen als Basis bzw. Schnittstelle für weitere Applikationen.
Plattform	Plattformsysteme wie Active Directory (AD) und File- sowie Print Services stellen zentrale Verwaltung und Authentifizierung von Benutzern (AD) sowie zentrale Office Services zur Verfügung.
Managed OS	Managed Operating System (OS) stellt die Betriebssystem Grundlage auf Serversystemen sicher. Dies ist u.a. die Basis für Plattform- und Middleware Systeme
Infrastruktur	Im Service Bereich Infrastruktur stellen zentrale Storage Systeme und Server Virtualisierung die Basis für den Systembetrieb im Rechenzentrum. Diese werden ergänzt um zentrale Backup Systeme. Die Mehrzahl der Systeme im Bereich Infrastruktur sind über Kunden geshared.
WAN, Internet Access, Router in RZ, FW im RZ	Die sichere Anbindung der Kunden an die Rechenzentren der AKQUINET ist Aufgabe des Services WAN. Hierzu wird die Anbindung mit verschiedensten Technologien (wie MPLS oder SD WAN) hergestellt. Der breitbandige und über mehrere Provider (die in den Rechenzentren terminieren) abgesicherte Zugang ins Internet stellt hierbei eine weitere Netzwerkschnittstelle für unser Kunden.
RZ Core LAN	Das RZ Core LAN stellt die grundsätzliche Verbindung zwischen den verschiedenen Rechenzentrumsstandorten sowie das Netzwerk innerhalb der Rechenzentren dar. Dies ist Basis für die abgesicherte Netzwerksegmentierung und die Darstellung der Kundennetzte.
Housing	Dieser Service stellt den Kunden Fläche sowie Racks & Einhausung in den Rechenzentrums IT Räumen zur Verfügung, auf der die Unterbringung eigener physischer Systeme (Server, etc.) vom Kunden möglich ist. Zu diesem Service gehört die Gebäudesicherheit, die energieeffiziente Kühlung sowie die abgesicherte Versorgung von IT-Strom.

AKQUINET Cloud	Beschreibung des Services
Akquinet Private Cloud	AKQUINET bietet ihren Kunden Private Cloud Dienste an. Die dazugehörige Infrastruktur wird in eigenen Rechenzentren betrieben. Der Kunde verwaltet dabei über das Self Service Portal vollumfänglich die virtuellen Ressourcen. Das detaillierte Reporting liefert die tagesgenaue Abrechnung der tatsächlich genutzten Ressourcen.

1.6. Informationssicherheits-Managementsystem [Norm-Ref.:4.4]

Das ISMS wird gemäß den Vorgaben des internationalen Standards ISO 27001 umgesetzt. Die normativen Anforderungen werden in die Organisation und die betrieblichen Prozesse vollumfänglich implementiert. Ausnahmen werden sofern relevant grundsätzlich im Statement of the Applicability festgehalten. Weitere Informationen zu ISMS-Prozessen sind dem ISMS-Handbuch zu entnehmen. Servicespezifische Teile des ISMS können transparent in das Haupt-ISMS integriert und müssen separat dokumentiert werden.

1.7. Managementverpflichtung [NormRef.:5.1]

Die Geschäftsführung der akquinet outsourcing gGmbH hat beschlossen, ein ISMS auf Basis der ISO 27001 für den hier definierten Anwendungsbereich umzusetzen. Dies bedeutet, dass die Managementebene für die Umsetzung folgender Aufgaben verantwortlich ist:

- Unterstützung der kontinuierlichen Verbesserung und Weiterentwicklung des etablierten ISMS bzw. Förderung der Informationssicherheit im Unternehmen
- Erarbeitung und Kommunikation einer Sicherheitspolitik
- Benennung des Anwendungsbereichs des ISMS
- Erarbeitung und Kommunizieren von Richtlinien zur Gewährleistung der Informationssicherheit
- Erstellung einer Methode zum Management von Risiken und zur Akzeptanz von Restrisiken
- Schaffung von Awareness für die Bedeutung und den Nutzen eines angemessenen Informationssicherheitsniveaus bzw. des ISMS
- Schaffung von Awareness und Motivation für die Notwendigkeit zur Einhaltung der Sicherheitsrichtlinien
- Schaffung von Awareness und Motivation, über Schwachstellen und Sicherheitsvorfälle zu informieren und Verbesserungen vorzuschlagen
- Bereitstellung ausreichender Ressourcen für Einrichtung und Betrieb des ISMS sowie der Sicherheitsmaßnahmen
- Durchführung von Audits und Management-Reviews im Rahmen des ISMS
- Verpflichtung von Mitarbeiter auf das Informationssicherheits-Managementsystem (ISMS)
- Bereitstellung der notwendigen Informationen zum ISMS und Datenschutz für jeden Mitarbeiter

Die Vorgaben des ISMS sind Vertragsbestandteile in definierten Kundensituationen, weshalb die Aufrechterhaltung des ISMS mittelbar zur Wertschöpfung beiträgt.

Die akquinet outsourcing gGmbH benennt einen Information Security Manager (IS-Manager), der für die Organisation und Pflege des ISMS und Sicherheitsprozesses verantwortlich ist. Unbeschadet davon bleibt die Gesamtverantwortung jedoch bei der Managementebene. Um diese Verantwortung effizient wahrnehmen zu können, wird sie stetig mit den essenziellen Informationen rund um das ISMS durch den IS-Manager versorgt. Der Informationsfluss geschieht mindestens im Rahmen eines Regeltermins. Zu den wichtigen Informationen für das Management zählen:

- Sicherheitsanforderungen, die sich aus geänderten und anwendbaren Gesetzen ergeben
- Sicherheitsanforderungen die sich aus vertraglichen Verpflichtungen von Kunden ableiten lassen
- Risiken und deren Auswirkungen
- Aufgetretene Schwachstellen oder Sicherheitsvorfälle
- Auswirkungen von tatsächlichen oder potenziellen Sicherheitsvorfällen auf kritische Geschäftsprozesse
- Potenzielle Gefährdungen aus veränderten Rahmenbedingungen und zukünftigen Entwicklungen
- Brauchbare Vorgehensweisen zur Informationssicherheit aus allgemeinen oder branchenüblichen Standards, vergleichbaren Organisationen, Arbeitsgruppen

Grenzen der Sicherheit:

- Es gibt keine 100%ige Sicherheit, sondern nur ein akzeptiertes Restrisiko, das innerhalb des Risikomanagements ermittelt wird. Das Management wird über die Restrisiken informiert und trägt diese.
- Sicherheitsmaßnahmen verursachen Aufwände. Diese werden denen der Folgen eines Security Incidents für eine Kosten-Nutzen Abschätzung gegenübergestellt. Die Senkung der Risiken geschieht in der Regel mit vertretbarem personellem, zeitlichem und finanziellem Aufwand.
- Es können Verkettungen von Vorfällen auftreten, die niemand vorhersagen kann und die ein höheres Schadenspotenzial als das akzeptierte Restrisiko nach sich ziehen. Das Management ist sich diesem bewusst.

1.8. Verpflichtung der Mitarbeiter

Alle Mitarbeiter müssen sich der Bedeutung von Informationssicherheit bewusst sein. Das Management unterstützt die Umsetzung des Bewusstseins in ihrem organisatorischen Bereich. Jeder Mitarbeiter soll aktiv in das Konzept „Informationssicherheit“ eingebunden sein, Verbesserungspotential melden und umsetzen können.

Mitarbeiter des Unternehmens sind verpflichtet, die einschlägigen Gesetze (z. B. Strafgesetzbuch, Handelsgesetzbuch, Sozialgesetzbuch, Gesetze und Regelungen zum Datenschutz) und vertraglichen Regelungen einzuhalten. Negative finanzielle

und immaterielle Folgen für das Unternehmen sowie für die Mitarbeiter durch Gesetzesverstöße sind zu vermeiden. Maßnahmen zur Gewährleistung von Informationssicherheit werden im Einklang mit der Datenschutzgrundverordnung und dem Bundesdatenschutzgesetz umgesetzt. Die besonders schützenswerten personenbezogenen Daten des Integrationsbetriebes werden gemäß den Vorgaben des Datenschutzes und des Sozialgesetzbuches behandelt.

Mitarbeiter haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen der ISMS-Richtlinien zum Schutz von Informationen zu halten. Sicherheitslücken, -ereignisse und -vorfälle sind dem Information Security Manager zu melden und werden von diesem an zentraler Stelle aufgenommen und aufbereitet. Jeder Mitarbeiter ist angehalten, in seinem Aufgabenbereich den Informationsschutz zu gewährleisten und diese in Abstimmung mit dem Information Security Manager zu verbessern. Bei Unklarheiten, zur Meldung von Sicherheitsvorfällen oder sonstigen Anliegen bezüglich der Informationssicherheit kann die folgende E-Mail-Adresse verwendet werden: isms@akquinet.de

1.9. Detailziele der Informationssicherheit [NormRef.:5.2]

Abgeleitet aus der Informationssicherheitspolitik ist die Gewährleistung von Vertraulichkeit und Informationssicherheit eine wesentliche Säule unseres unternehmerischen Erfolgs. Darum führen wir ein ISMS mit folgenden Aktionspunkten:

- Erarbeitung, Weiterentwicklung und Kommunikation einer Sicherheitspolitik
- Benennung und Überprüfung des Anwendungsbereichs
- Erarbeitung und Kommunizieren von Richtlinien zur Gewährleistung der Informationssicherheit
- Erstellung einer Methode zum Management von Risiken und zur Akzeptanz von Restrisiken
- Schaffung von Awareness für die Bedeutung und den Nutzen eines angemessenen Informationssicherheitsniveaus bzw. des ISMS
- Schaffung von Awareness und Motivation für die Notwendigkeit zur Einhaltung der Sicherheitsrichtlinien
- Schaffung von Awareness und Motivation, über Schwachstellen und Sicherheitsvorfälle zu informieren und Verbesserungen vorzuschlagen
- Bereitstellung ausreichender Ressourcen für Einrichtung und Betrieb des ISMS sowie der Sicherheitsmaßnahmen
- Durchführung von Audits und Management-Reviews im Rahmen des ISMS

Konkrete IS-Ziele und Maßnahmen werden jährlich zwischen der Geschäftsführung und dem IS-Manager vereinbart und umgesetzt. Im Rahmen des kontinuierlichen Verbesserungsprozesses werden diese regelmäßig auf Angemessenheit und Wirksamkeit überprüft und bewertet. Hierzu gehören insbesondere Prüfkriterien aus den Bereichen Governance, Risk Management und Compliance, sowie eine Betrachtung möglicher Chancen zur Erhöhung der Informationssicherheit und zur Risikovermeidung.

1.10. Rollen, Verantwortlichkeiten und Kompetenzen [NormRef.:5.3]

Die nachfolgend aufgeführten Rollen sind maßgeblich für den Betrieb des ISMS. Ergänzt werden diese durch betriebliche Rollen, die unter Umständen Teilaufgaben im Sinne des ISMS wahrnehmen und die IS-Ziele damit ebenfalls unterstützen. Die Beschreibung dieser betrieblichen Rollen ist der betriebs- und service-spezifischen Dokumentation zu entnehmen.

Zur Erreichung der Maßnahmenziele wird ein IS-Manager ernannt. Dieser ist verantwortlich dafür, dass für Informationssicherheit relevante Richtlinien erstellt, genehmigt und umgesetzt werden. Die Entwicklung und Umsetzung von Informationssicherheit werden maßgeblich von dieser Stelle gesteuert. Der IS- Manager untersteht der Geschäftsführung und steht dieser beratend zur Seite.

Miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche werden, sofern es organisatorisch möglich ist, voneinander getrennt vergeben. Hierbei werden weiter unten definierte Grundsätze und Vorgaben beachtet. Absichernde Maßnahmen werden implementiert, sofern im Konflikt stehende Rollen einer Person zugewiesen werden.

Kompetenzlevel	Anforderungen hinsichtlich des Wissens und der Fähigkeiten
[E] Einsteiger	Verstehen und wissen
[P] Praktiker	Verstehen, wissen und anwenden können
[X] Experte	Verstehen, wissen, anwenden, analysieren, verbessern und adaptieren können

Rolle	Beschreibung	Kenntnisse IS-/DS-spezifischer Gesetze	Interne Richtlinien	Kenntnisse Betriebssicherheit	Kenntnisse Risiko Management	Fachkunde Datenschutz	Kenntnisse der ISO 27x-Normreihe	Kenntnisse ISO 27001 und ISO 27002
Geschäftsführung (GF)	Die Geschäftsführung trägt die Gesamtverantwortung für das Unternehmen. Im Kontext des Risiko Managements prüft die Geschäftsführung die ermittelten Risiken und definiert die Optionen der Risikobehandlung. Die Geschäftsführung genehmigt außerdem ISMS Richtlinien und relevante Dokumente und sorgt dafür, dass entsprechende Ressourcen zur Umsetzung von Gegenmaßnahmen bereitgestellt werden.	P	E	E	P	P	X	P
IS-Manager (IS-Manager/ISM)	Der IS-Manager ist für die Sicherheitsprozesse verantwortlich und fungiert als zentraler Ansprechpartner für Fragen zur Informationssicherheit und IT-Sicherheitsvorfällen. Er ist der Prozessverantwortliche und steht der GF beratend zur Seite, ist aber **nicht** weisungsbefugt gegenüber Fachbereichen. Die Aufgaben sind im Bestellungsschreiben formuliert. Diese sind z.B.: ▪ Erstellung einer Informationssicherheitsrichtlinie und Strategien zur Umsetzung ▪ Bereitstellung von Standards, Prozesse, Verfahren, Baselines, Leitlinien und Risikobewertungen ▪ Unterstützung und Koordination bei der Bearbeitung v. Sicherheitsvorfällen ▪ Weitere Aufgaben sind dem Bestellungsschreiben zu entnehmen.	X	E	E	X	P	X	X
Datenschutzbeauftragter (DSB)	Der Datenschutzbeauftragte ist die vom Vorstand / GF bestellte Person, die den datenschutzrechtlich korrekten bzw. gesetzeskonformen Umgang mit personenbezogenen Daten überwacht und die verantwortlichen Stellen bei der Einhaltung der Datenschutzbestimmungen berät und unterstützt. Weitere Aufgaben sind der Ernennungsurkunde zu entnehmen.	P	-	X	E	E	X	X
IT-Sicherheitskoordinator (ITSEC-Koordinator)	Der ITSEC-Koordinator unterstützt den IS-Manager in operativen Tätigkeiten und koordiniert die Aktivitäten bei der Erstellung von Sicherheitskonzepten für akquinet-eigene Zwecke und im Kundenauftrag. Er unterstützt bei Audits und nimmt die Kundenkommunikation und operative Bearbeitung von IT-Sicherheitsvorfällen und Notfällen in Vertretung des IS-Manager wahr. Die Aufgaben sind im Bestellungsschreiben formuliert. Diese sind z. B.: ▪ Fachbereichsspezifische Kommunikation und Awareness bzgl. IS ▪ Pflege / Revision der ISMS Dokumente ▪ Unterstützung bei Dokumentation von Fachbereichen	E	-	E	P	X	P	E

	▪ Unterstützung in anderen Projekten ▪ Auswertung und Bearbeitung von Security Events / Incidents ▪ Allgemeine Kommunikation bzgl. IS-Anliegen für Stakeholder							
Informationssicherheits- / Datenschutzkoordinator (IS-/DS-Koordinator KIM)	Der IS-/DS-Koordinator KIM übernimmt folgende Aufgaben: ▪ Durchführung von Audits gem. Auditprozess (intern, aber insb. bei den Partnerfirmen); ▪ Unterstützung beim Risikomanagement; ▪ Anleitung von Personen innerhalb der Organisationen des Partnernetzwerks zu den Erfordernissen (einzuhalten Richtlinien, Prozessen, Nachweisen); ▪ Erstellen von Input und Verbesserungsvorschlägen für das Management-Review; ▪ Umsetzen oder Delegieren der beschlossenen Verbesserungsvorschläge. ▪ Abstimmung mit dem IS-Manager der akquinet outsourcing gGmbH und Umsetzung der Anforderungen aus dem Haupt-ISMS ▪ Erstellen von Input zu Datenschutzberichten gem. Anforderungen der Gematik; ▪ Erstellen von Input und Verbesserungsvorschlägen für das Management-Review; ▪ Umsetzen oder Delegieren der beschlossenen Verbesserungsvorschläge; ▪ Unterstützung und Durchführung von Datenschutzfolgenabschätzungen; ▪ Freigaben von Verarbeitungen; ▪ Behandlung von Datenschutzvorfällen; ▪ Kommunikation zu den Datenschutzbeauftragten (DSB) der Organisationen im Partnernetzwerk ▪ Abstimmung mit dem DSB der akquinet GmbH und Umsetzung der Anforderungen aus dem zentralen DSMS; ▪ Kommunikation zu Datenschutzaufsichtsbehörden am Ort von akquinet hse; ▪ Kommunikation zur Gematik; ▪ Audits sowohl intern als auch extern.	E	-	P	P	P	P	E

Service-Verantwortlicher (SV)	Der SV verantwortet die kundenübergreifende Gestaltung und Betreibbarkeit seines Services. ▪ Technischer Fokus ▪ Kundenunabhängig pro Service, Innensicht auf den Service ▪ Verantwortlich für die Betreibbarkeit seines Services (auch im Zusammenspiel mit über- oder untergeordneten Services) ▪ Definition der technischen Ausprägung des Services ▪ Verantwortlich für den Service-Lifecycle (Patch-, Releasemanagement, Capacitymanagement (Forecast)) ▪ Prüfung auf Schwachstellen bei Services und Aufzeigen von technischen Änderungsbedarfen und Optimierungsmöglichkeiten ▪ Erstellung und Pflege des Service-Betriebshandbuchs und Serviceinhalte im Servicekatalog ▪ Kommunikation Service-relevanter Informationen (inkl. notwendiger Einweisungen von Kollegen) ▪ Überwacht die Einheitlichkeit seines Services in den Implementierungen ▪ Technische Steuerung der kundenübergreifender Entstörung bei kritischen / schwerwiegenden Störungen ▪ Primärer Kandidat als Problem Owner für Services-Problems	E	-	E	P	X	P	E
Operatives Management (Cluster-Leiter, Teamleiter u. Prozessverantwortliche)	Das operative Management unterstützt die Informationssicherheit innerhalb der Organisation, indem es eine klare Ausrichtung vorgibt, das Engagement demonstriert, Aufgaben explizit formuliert und die Verantwortlichkeiten für Informationssicherheit anerkennt und die Asset Owner benennt. Das operative Management ist für die Freigabe von Ressourcen zum Erhalt des Informationssicherheitslevels und der kontinuierlichen Verbesserung des Prozessframeworks als Ganzes verantwortlich. Unter operativem Management werden alle Geschäftsführer, Teamleiter und Prozessverantwortliche verstanden.	E	-	E	E	P	P	P
Mitarbeiter	Mitarbeiter sind für die Erhaltung der Informationssicherheit in den Abteilungen unter Einhaltung von Richtlinien verantwortlich. Verbesserungsvorschläge oder Security Incidents / Security Events werden durch sie gemeldet.	-	-	E	-	E	E	E
IS-Managementteam (ISMT)	Das ISMT setzt sich aus dem ITSEC-Koordinator, dem ISP-Koordinator und dem DSB unter Leitung des IS-Manager zusammen. Bei Bedarf werden weitere Mitarbeiter geladen. Im Kontext des Risiko Managements stellt das ISMT interne Auditoren bereit, um zu prüfen, ob die Risikomanagement Politik und der Prozess wie geplant zusammenwirken. Ebenso werden durch die IS-Auditoren Schwachstellen und Bedrohungen kenntlich gemacht, die in die Bewertung einfließen.	n/a	n/a	n/a	n/a	n/a	n/a	n/a

Tabelle 7: Rollen, Verantwortlichkeiten und Kompetenzen

1.11. Grundsätze zur Bestimmung und Kompensation von Rollenkonflikten

In der Praxis zeigt sich die unzulässige Abhängigkeit oder Weisungsgebundenheit regelmäßig in Interessenskonflikten, also im Vorliegen von Unvereinbarkeiten oder einer Befangenheit. Das ursprüngliche Beschäftigungsverhältnis des Mitarbeitenden steht dabei im Konflikt mit seiner Rolle bzw. Funktion.

Miteinander in Konflikt stehende Rollen, Funktionen und Verantwortlichkeitsbereiche sollten daher möglichst getrennt werden, um die Möglichkeiten von Fehlentscheidungen zu reduzieren, die unter anderem zu erhöhten unternehmerischen Risiken und/oder zur Nichteinhaltung interner Richtlinien, Vorgaben sowie gesetzlicher Bestimmungen führen könnten. Hierbei werden im Wesentlichen folgende Arten der Konflikte unterschieden:

Art des Konflikts	Konfliktpotential & organisatorische Vorgaben	Rollenkombination
Interessenskonflikt aufgrund einer Exekutivfunktion	Rollen, die Zwecke und Mittel der Datenverarbeitung festlegen können und eine Exekutivfunktion wahrnehmen, dürfen nicht gleichzeitig die Rolle der CC-Leitung, des IS-Managers oder des DSBs innehaben, da das Interesse an der wirtschaftlichen Führung des Unternehmens im Vordergrund steht. Es muss außerdem verhindert werden, dass die Person in der Ausübung der Rollen sich selbst kontrollieren kann.	Geschäftsführung ist gleichzeitig CC Leitung CC-Leitung ist gleichzeitig IS-Manager oder DSB
Familiärer Interessenskonflikt	Mitglieder der erweiterten Kernfamilie sind unter Umständen befangen in der Ausübung, der für die Rolle relevanten Aufgaben. Aus diesem Grund dürfen sicherheitskritische Rollen oder Rollen mit Exekutivfunktion nicht an Familienmitglieder der Geschäftsführung oder CC-Leitung vergeben werden.	Geschäftsführung / CC Leitung Geschäftsführung / IS-Manager oder DSB CC-Leitung / IS-Manager oder DSB
Fachlicher Interessenskonflikt	Bei der Ausübung der Rollen IS-Manager und DSB durch eine Person oder fachübergreifenden, administrativen Rollen kann es bei der Bewertung der Kritikalität von Risiken sowie der Angemessenheit von technischen und organisatorischen Maßnahmen zu fachlichen Interessenskonflikten durch unterschiedliche Betrachtungswinkel bzw. Schwerpunkte kommen. Gleichzeitige Vergabe der beiden Rollen IS-Manager und DSB an eine Person dürfen nur unter Berücksichtigung der absichernden Maßnahmen vergeben werden. Dabei muss die Unabhängigkeit dieser Rollen durch Bildung einer Stabsstelle unbedingt gewahrt bleiben. Fachübergreifende, administrative Tätigkeiten mit privilegierten Berechtigungen sind auf das notwendige Minimum zu reduzieren.	IS-Manager / DSB Administrative Rollen mit fachlich übergreifenden privilegierten Berechtigungen

Tabelle 8 - Konfliktmatrix

Die Geschäftsführung kann unter Einhaltung und Durchsetzung von absichernden Maßnahmen auf die Trennung der o.g. Rollen verzichten. Die absichernden Maßnahmen werden in Abhängigkeit von der vorliegenden Situation und unter Berücksichtigung der organisatorischen Vorgaben und der Kompensationsmatrix durch die Geschäftsführung bestimmt. Werden bspw. die Rollen DSB und IS-Manager gleichzeitig einer Person zugewiesen, so müssen mögliche fachliche Interessenskonflikte im Rahmen der IS-JourFixe-Termine durch den IS-Manager aufgezeigt und mit der Geschäftsführung diskutiert und aufgelöst werden. Außerdem muss die Person die relevanten Kompetenzen in beiden Fachbereichen vorweisen und unabhängig als Stabsstelle agieren können. Eine Unabhängigkeit ist nicht gegeben, wenn die Person im Rahmen der zugewiesenen Rollen sich selbst überprüfen muss und/oder eine Exekutivfunktion ausübt.

Art des Konflikts	Absichernde Maßnahmen
Interessenskonflikt aufgrund einer Exekutivfunktion	Enge Kontrolle der Umsetzung von internen Richtlinien, Vorgaben sowie gesetzlichen Bestimmungen durch unabhängige Prüfer. Strikte Dokumentation der mit einem Rollenkonflikt im Zusammenhang stehenden Entscheidungen. Mögliche Konflikte sind (sofern anwendbar) im Rahmen der JourFixe-Termine mit der Geschäftsführung durch die Rolle aufzuzeigen und mit der GF aufzulösen.
Familiärer Interessenskonflikt	Strikte Dokumentation der mit einem Rollenkonflikt im Zusammenhang stehenden Entscheidungen. Bestimmung einer weiteren Person (GF oder CC-Leitung) zur Durchsetzung eines 4-Augen-Prinzips im Rahmen der Entscheidungsfindung.
Fachlicher Interessenskonflikt	Prüfen und Durchsetzen der Eignung auf Basis vorhandener, fachlicher Kompetenzen, die zur Wahrnehmung der relevanten Rollen vorhanden sein müssen. Mögliche Konflikte sind im Rahmen der JourFixe-Termine mit der Geschäftsführung durch den Mitarbeiter aufzuzeigen und mit der GF aufzulösen. Ergänzung für fachübergreifende, administrative Tätigkeiten: privilegierte Berechtigungen sind auf das notwendige Minimum zu reduzieren. Tätigkeiten bei der Ausübung der Rollen sind nachvollziehbar zu protokollieren.

Tabelle 9 - Kompensationsmatrix

1.12. Schlussbestimmung

Die Geschäftsführung hat die Informationssicherheitsrichtlinie und weitere Richtlinien zur Informationssicherheit beauftragt und freigegeben. Die Einhaltung folgender Richtlinien ist für alle Mitarbeiter und Dienstleister der im Anwendungsbereich agierender Gesellschaften verbindlich:

Dokument	
▪ Informationssicherheitsrichtlinie ▪ ISMS Handbuch ▪ Richtlinie Arbeitsplatzsicherheit ▪ Richtlinie Sicherheit mobiler Geräte ▪ Richtlinie Audit ▪ Richtlinie E-Mail ▪ Richtlinie Informationssicherheitskategorien für Dokumente ▪ Richtlinie Internet	▪ Richtlinie Kryptographie ▪ Richtlinie Lieferanten und Dienstleister ▪ Richtlinie Passwort ▪ Richtlinie Passwort Sonderaccount ▪ Richtlinie Transponder und Schlüssel ▪ Richtlinie sichere Softwareentwicklung ▪ Richtlinie Entsorgung Papier und Datenträger ▪ Richtlinie Unterschriftenregelung ▪ Richtlinie Risiko Management ▪ Richtlinie KI

Hamburg, den 08.11.2024

Die Geschäftsführung