Richtlinie Informationssicherheit

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern

Version 23.0

Fassung gemäß Vorstandsbeschluss vom 02.03.2023

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Richtlinie Informationssicherheit
Version	23.0
Geltungsbereich	VAV Versicherungs-Aktiengesellschaft
Erstmalige Freigabe	01.12.2016
Verabschiedet durch (Datum)	Vorstand (02.03.2023),
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Thomas Pinka Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Mag. (FH) Thomas Pinka (thomas.pinka@vav.at)
Letztes Review	März 2023
Wiedervorlage	März 2024

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
1.0	09.11.2016	Anpassungen an die Konzernrichtlinie (Ersterstellung)	Gerhard Steinwendter
17.0	30.11.2017	Anpassungen an die Konzernrichtlinie (Seiten: 3, 4)	Sascha Budinsky, Gerhard Steinwendter
19.0	20.09.2019	Anpassungen an die Konzernrichtlinie (Alle Seiten angepasst – die Konzernrichtlinie wurde komplett überarbeitet)	Daniel Fürdauer
20.0	10.12.2020	Übernahme der Änderungen der Konzernrichtlinie; Annäherung der Informationseigentümer an die Konzern-Version, allerdings ohne der Erforderns eines Vorstandsbeschluss vor Inbetriebnahme eines Informationssystems; Vereinfachung des Risikomeldeprozesses	Daniel Fürdauer
21.0	30.11.2021	Übernahme der Änderungen der Konzernrichtlinie; VHV.mobil heißt weiterhin mobiles Arbeiten; Übergangslösung für die „Arbeitsrichtlinie Externe Prüfungen und Penetrationstests“	Daniel Fürdauer
23.0	02.03.2023	Überführung der „VHV Gesellschaftsrichtlinie Informationssicherheit 23.0“ in die „VAV Richtlinie Informationssicherheit 23.0“ mit den Anforderungen der Group Policy „Information Security	Thomas Pinka

Art der Freigabe – VHV Konzern

Version	Datum	Wesentliche Änderungen	Bestätigt von
1.0	29.11.2016	Nein	
17.0	20.12.2017	Nein	Vollmer, Mathias (ISB)
19.0	20.09.2019	Nein	Matthias Vollmer (ISB)
20.0	12.12.2020	Nein	i.V. Ulrich Lintker (Leiter KDI)
21.0	03.12.2021	Nein	Ulrich Lintker (ISB; Leiter KDI)
Da in der VHV eine übergeordnete Group Policy etabliert wurde und die Umsetzungen der darin enthaltenen Anforderungen vom Vorstand zu bestätigen sind, ist eine Freigabe durch die VHV nicht mehr notwendig.			
Wesentliche Änderungen → Nein: Bestätigung durch ISB (VHV) → Ja: Bestätigung durch Vorstand VHV Holding			

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS

ABKÜRZUNGSVERZEICHNIS

BCM ..... Business Continuity Management
DSB .....Datenschutzbeauftragter
DSGVO.....Datenschutzgrundverordnung
ISMS ..... Informationssicherheitsmanagementsystem
ISO..... International Organization for Standardization, International Organization for Standardization
ISRT..... Informationssicherheitsreaktionsteam oder Information Security Response Team
SDI.....Stabstelle Datenschutz und Informationssicherheit
KPI ..... Key Performance Indicator

1 EINLEITUNG

1.1 Zielsetzung

Die VAV ist Teil der VHV Gruppe, einem traditionsreichen Konzern von Spezialisten für Versicherungen, Vorsorge und Vermögen. Im Zentrum der Strategie der VAV stehen ihre Kunden und Vertriebspartner.

Die steigende Abhängigkeit der Geschäftsprozesse der VAV von der Verfügbarkeit, Vertraulichkeit, Authentizität und Integrität der Informationen in den IT-Systemen und in sonstiger Form, bedingt die Notwendigkeit, diese Informationen vor unzulässiger und unsachgemäßer Nutzung sowie Missbrauch, Verlust, Preisgabe, Zerstörung und Manipulation zu schützen.

Für die VAV stellt die Informationssicherheit daher einen integralen Bestandteil der Geschäftspolitik dar. Die Verlässlichkeit der eingesetzten IT-Systeme sowie eine angemessene Verfügbarkeit der Informationen sichern die Leistungsfähigkeit und Wettbewerbsposition der VAV und damit das Vertrauen der Kunden und Geschäftspartner sowie das Ansehen in der Öffentlichkeit.

Die Informationssicherheitsziele leiten sich aus der Geschäftsstrategie VAV ab. Hiernach haben die Gewährleistung von Informationssicherheit sowie die Einhaltung der jeweils einschlägigen rechtlichen und regulatorischen Vorgaben einen hohen Stellenwert für die VAV. Ziel ist es dabei, unter Berücksichtigung der Schutzziele (Verfügbarkeit, Vertraulichkeit, Integrität und Authentizität[1]) sowie mit Blick auf das Risikoprofil der VAV, ein angemessenes Sicherheitsniveau nach dem Stand der Technik zu erreichen. Zu diesem Zweck betreibt die VAV ein Informationssicherheitsmanagementsystem (ISMS), das sich an der DIN ISO/IEC 27001:2017 orientiert.

Die Informationssicherheitsziele werden regelmäßig (einmal jährlich) mit Blick auf ihre Vereinbarkeit mit den Zielen in der Strategie abgeglichen und bei Bedarf angepasst.

Zur Gewährleistung eines angemessenen Informationssicherheitsniveaus werden von der Geschäftsleitung die erforderlichen Ressourcen (Personal und Finanzmittel) für den Aufbau, die Verwirklichung, die Aufrechterhaltung und die Verbesserung des ISMS bereitgestellt.

Zur Erreichung der Informationssicherheitsziele hat die Geschäftsleitung der VAV zehn Informationssicherheitsgrundsätze definiert, welche richtungsweisend bezüglich der strategischen Ausrichtung des ISMS der VAV sind und somit das gewünschte „Informationssicherheitsniveau“ definieren.

Grundsatz 1: Sicherheit als integraler Bestandteil

Die Informationssicherheit wird im Unternehmen strategisch positioniert und als unverzichtbarer Bestandteil der gesamten Unternehmenspolitik aufgefasst.

[1] Die Schutzziele Revisionsfähigkeit und Transparenz lassen sich aus den genannten Schutzzielen ableiten und werden daher nicht explizit behandelt.

Grundsatz 2: Einhaltung gesetzlicher und regulatorischer Anforderungen

Alle gesetzlichen und regulatorischen Anforderungen an die VAV sind identifiziert und werden kontinuierlich auf Vollständigkeit und Aktualität geprüft. Vorgaben, welche in dieser Richtlinie und den nachgelagerten Arbeitsrichtlinien enthalten sind, müssen beachtet und Abweichungen dokumentiert werden. Die Einhaltung der Sicherheitserfordernisse wird regelmäßig auf ihre Umsetzung im Unternehmen und bei den Dienstleistern überprüft.

Grundsatz 3: Schutz von Informationen

Die Schutzziele Integrität, Vertraulichkeit, Authentizität und Verfügbarkeit von Informationen werden unter Berücksichtigung des Stands der Technik sowie des Risikoprofils sichergestellt.

Grundsatz 4: Schutz von personenbezogenen Daten

Es werden angemessene technische und organisatorische Maßnahmen eingesetzt, um personenbezogene Daten (z.B. von Kunden, Partnern, Mitarbeitern und Dienstleistern) vor missbräuchlicher Verarbeitung zu schützen.

Grundsatz 5: Gewährleistung der Nachvollziehbarkeit

Die Nachvollziehbarkeit der Aktivitäten, die für die Informationssicherheit relevant sind, ist eine unabdingbare Forderung, sowohl aus gesetzlichen Anforderungen, als auch aus Eigeninteresse des Unternehmens. Der für eine Aktivität Verantwortliche muss jederzeit eindeutig festgestellt werden können.

Grundsatz 6: Standards und Regeln

Durch die Anlehnung an die für das Unternehmen relevanten Standards und Regelwerke wird die einheitliche und möglichst vollständige Erkennung und Behandlung aller Sicherheitsrisiken in den Geschäftsprozessen und die Vorbereitung auf interne und externe Prüfungen sichergestellt.

Grundsatz 7: Schutz vor Angriffen

Alle Prozesse werden risikobasiert vor Ausfall oder Beeinträchtigung durch Angriffe geschützt.

Grundsatz 8: Gewährleistung der Informationssicherheit in Vertragsbeziehungen

Durch vertragliche Vereinbarungen ist die notwendige Transparenz über die gesamten vereinbarten Leistungen für die betroffenen Unternehmensbereiche und für die dafür verantwortlichen externen und internen Dienstleister klarzustellen und die Anforderung an die Einhaltung der Informationssicherheitserfordernisse sicherzustellen.

Grundsatz 9: Gewährleistung des Betriebs

Unabhängig von der Tatsache, ob und welche Teile des Betriebs im Unternehmen selbst erfolgen und welche Teile an einen externen Dienstleister ausgelagert sind, wird ein sicherer und geregelter Geschäftsbetrieb gewährleistet.

Grundsatz 10: Berücksichtigung von Wirtschaftlichkeitsaspekten

Die Sicherheitsmaßnahmen müssen risikobasiert und in einem wirtschaftlich vertretbaren Verhältnis zum Schaden stehen, der durch einen Vorfall verursacht werden kann.

1.2 Geltungsbereich

Diese Richtlinie findet Anwendung auf die VAV Versicherungs-Aktiengesellschaft.

Die Regelungen dieser Richtlinie richten sich an die gesetzlichen Vertreter, Führungskräfte und Mitarbeiter sowie beauftragte Dienstleister im Rahmen ihrer Vertragserfüllung.

Die Bezeichnung „Geschäftsleitung“ meint im Folgenden die Vorstände (Aktiengesellschaft).

Zum Geltungsbereich des Informationssicherheitsmanagementsystems (ISMS) siehe unter 2.1.

1.3 Änderungen

Wesentliche inhaltliche Änderungen an dieser Richtlinie bedürfen der vorherigen Zustimmung der Geschäftsleitung. Redaktionelle Änderungen sowie Änderungen an dieser Richtlinie, die aufgrund veränderter Rahmenbedingungen notwendig geworden sind, dürfen durch den Informationssicherheitsbeauftragten (ISB) ohne vorherige Zustimmung der Geschäftsleitung vorgenommen werden. Die Geschäftsleitung wird über die erfolgten Änderungen informiert.

Geänderte Rahmenbedingungen können sich z.B. aus rechtlichen und regulatorischen Anforderungen, der Strategie der Gesellschaft, aus Veränderungen in der Auf- und Ablauforganisation, aus neuen Bedrohungsszenarien oder mit Blick auf neue Sicherheitstechnologien ergeben.

Wesentliche inhaltliche Änderungen an den konkretisierenden Arbeitsrichtlinien, die auf Basis dieser Richtlinie erstellt werden, dürfen durch den Informationssicherheitsbeauftragten (ISB) ohne vorherige Zustimmung der Geschäftsleitung vorgenommen werden.

1.4 Informationssicherheitsverstöße

Verstöße gegen die Vorgaben der Informationssicherheit können im Einzelfall zu disziplinarischen oder arbeitsrechtlichen Maßnahmen oder im Einzelfall zu strafrechtlichen Sanktionen führen.

2 INFORMATIONSSICHERHEITSMANAGEMENTSYSTEM

Die VAV hat ein Informationssicherheitsmanagementsystem (ISMS), das sich an dem DIN ISO/IEC 27001:2017 orientiert, etabliert. Ein ISMS bildet die Grundlage zur Identifikation, Bewertung, Behandlung, Kommunikation und Überprüfung von Informationssicherheitsrisiken. Ziel des ISMS ist es,

- das angestrebte Informationssicherheitsniveau zu erreichen,
- dieses kontinuierlich zu gewährleisten und
- laufend auskunftsfähig über dessen Status zu sein.

Der Vorstand verantwortet das ISMS und schafft dafür die nötigen Rahmenbedingungen, insbesondere mit Blick auf die notwendigen finanziellen und personellen Ressourcen.

Die Chancen und Risiken, die sich aus einem ISMS ergeben können, sind im Anhang C aufgeführt. Dort ist auch geregelt, welche Maßnahmen zum Umgang mit den Risiken ergriffen werden.

2.1 Anwendungsbereich des ISMS und Informationsverbund

Der Anwendungsbereich und der Informationsverbund des ISMS umfassen alle Mitarbeiter, geschäftsrelevanten Informationen, Geschäftsprozesse, IT-Systeme sowie Netz- und Gebäudeinfrastrukturen, Standorte und Dienstleister der VAV Versicherungs-Aktiengesellschaft.

Eine detaillierte Anwendbarkeitserklärung zum ISMS (sog. Statement Of Applicability) wird vom ISB geführt und nachgehalten.

2.2 Interessierte Parteien und externe Anforderungen

Im Rahmen des ISMS werden die Interessen und Anforderungen aller Personen und Personengruppen (interessierte Parteien), sowohl intern als auch extern, erhoben, ausgewertet und berücksichtigt. Anforderungen ergeben sich insbesondere aus gesetzlichen und regulatorischen Vorgaben sowie freiwilligen Selbstverpflichtungen. Die derzeit geltenden externen Anforderungen sind im Anhang aufgeführt. Anforderungen können sich aber auch aufgrund von vertraglichen Verpflichtungen, z.B. mit Dienstleistern, ergeben. Eine Übersicht der interessierten Parteien sowie der diesbezüglichen Anforderungen finden sich im Anhang A.

2.3 Richtlinienorganisation

Die Dokumente, die das ISMS der VAV beschreiben, sind hierarchisch organisiert. Den Ausgangspunkt bildet die IT-Strategie, die sich aus der Geschäftsstrategie der VAV ableitet. Hier ist beschrieben, welche Bedeutung die Informationssicherheit für die VAV hat und welche Ziele diesbezüglich erreicht werden sollen. Ausgehend von diesen strategischen Zielen werden in der Richtlinie Informationssicherheit die allgemeinen Anforderungen definiert, die zur Erreichung der Informationssicherheitszeile notwendig sind. Auf der darunterliegenden Ebene folgen themenspezifische Arbeitsrichtlinien, z.B. zur Protokollierung oder zur Kryptographie. Technische Detaillierungen sind in Betriebshandbüchern beschrieben. Details zu einzelnen Systemen sind in Konfigurations- oder Nachweisdokumenten zu dokumentieren.

2.4 Rollen und Verantwortlichkeiten

Für die Informationssicherheit sind unterschiedliche Rollen und Verantwortlichkeiten im Unternehmen erforderlich und in die ISMS-Prozesse eingebunden. Entsprechende fachliche Vertretungen sind sicherzustellen. In den nachfolgenden Unterkapiteln sind wesentliche am ISMS beteiligte Rollen aufgeführt und deren Aufgaben in wesentlichen Zügen beschrieben. Detaillierte Informationen zu den einzelnen Rollen und deren Aufgaben werden in den Stellen- und Funktionsbeschreibungen beschrieben, die in den jeweiligen Abteilungen aufbewahrt werden.

2.4.1 Informationssicherheitsbeauftragter

Zur Etablierung und Überprüfung der Vorgaben dieser Richtlinie und dauerhaften Umsetzung der ISMS-Regelprozesse wurde die Funktion des ISB eingerichtet. Zur Vermeidung von Interessenkonflikten ist diese Funktion unabhängig ausgestaltet und aufbau- und ablauforganisatorisch von den Bereichen getrennt, die für den Betrieb und die Weiterentwicklung der IT-Systeme zuständig sind. Die Funktion des ISB wird für die VAV wahrgenommen.

Der ISB hat die Aufgabe, die Belange der Informationssicherheit im Unternehmen und gegenüber Dritten zu vertreten. Der ISB ist als überwachende Funktion dafür zuständig, dass die in der IT-Strategie, der Richtlinie Informationssicherheit und den diesbezüglichen Arbeitsrichtlinien niedergelegten Ziele und Anforderungen intern und – soweit erforderlich – gegenüber Dritten transparent gemacht und deren Einhaltung überprüft und überwacht wird. Der ISB ist ferner dafür zuständig, Sensibilisierungs- und Schulungsmaßnahmen zur Informationssicherheit zu initiieren und zu koordinieren.

Die Geschäftsleitung hat den ISB zur Durchführung der ihm übertragenen Aufgaben mit allen dazu notwendigen Befugnissen und Kompetenzen mittels der Stellen- und Funktionsbeschreibung ausgestattet. So hat der ISB insbesondere das Recht, über alle informationssicherheitsrelevanten Vorfälle unmittelbar und umfassend informiert zu werden. Ferner ist er – ungeachtet der vierteljährlichen Berichterstattung – dazu berechtigt, die Geschäftsleitung über informationssicherheitsrelevante Sachverhalte zu informieren. Weitere Details zu den konkreten Aufgaben, Befugnissen und Kompetenzen des ISB sind der Stellen- und Funktionsbeschreibung des ISB zu entnehmen.

2.4.2 Datenschutzbeauftragter

Der Datenschutzbeauftragte (DSB) wirkt darauf hin, dass die externen und internen Vorgaben des Datenschutzes eingehalten werden. Neben der Unterrichtung und Beratung der Verantwortlichen im Unternehmen gehört die Überwachung der Einhaltung der einschlägigen Datenschutzvorschriften zu seinen Aufgaben. Im Rahmen der Überprüfung der technischen und organisatorischen Maßnahmen wird der DSB durch den ISB sowie das IT-Security Management unterstützt.

Weitere Details zu den konkreten Aufgaben des DSB sind der Stellen- und Funktionsbeschreibung des DSB zu entnehmen.

2.4.3 Notfallmanager

Der Notfallmanager ist für die Koordination, Planung und Überwachung der Umsetzung der Notfallmanagement-Prozesse in der VAV zuständig. Seine Rollen und Verantwortlichkeiten sind in der Richtlinie BCM definiert.

Im Rahmen von wesentlichen Informationssicherheitsvorfällen erfolgt eine Information des Notfallmanagers durch den ISB. Sollten im Rahmen von Meldungen an den Notfallmanager Hinweise auf Einschränkungen der Informationssicherheit erkennbar sein, erfolgt eine Information an den ISB. Ebenfalls ist der ISB einzubinden, wenn Notfallkonzepte die Informationssicherheit beeinflussen.

Bei einer Aktivierung des Information Security Response Teams (ISRT) erfolgt ein Einbezug des Notfallmanagers gemäß der „Arbeitsrichtlinie Sicherheitsvorfall“.

2.4.4 Business Continuity Manager

Der BC-Manager ist für die Koordination, Planung und Überwachung der Umsetzung der BCM-Prozesse in der VAV zuständig. Seine Rollen und Verantwortlichkeiten sind in der Richtlinie BCM definiert. Der BC-Manager ist Ansprechpartner für den ISB in Bezug auf die Berücksichtigung von Informationssicherheitsaspekten im BCM Regelprozess. Zu diesem Zweck findet ein regelmäßiger Austausch zwischen dem ISB und BC-Manager statt.

2.4.5 IT-Security-Management

Das IT-Security Management ist für die Erstellung, Kommunikation und Pflege von Richtlinien zur IT-Sicherheit (z.B. Kryptographie, Protokollierung) zuständig und überwacht deren Einhaltung. Diese Richtlinien konkretisieren die Regelungen der Richtlinie Informationssicherheit und berücksichtigen den Stand der Technik. Das IT-Security Management überprüft IT-Sicherheitskonzepte und berät Fachbereiche und Projekte bei der Umsetzung der Richtlinien. Ferner führt es Sicherheits- und Gefährdungsanalysen bei der Einführung von neuen Informationstechnologien durch. Das IT-Security Management unterstützt zudem den ISB bei Informationssicherheitsrisikoanalysen und bei der Erarbeitung von Vorschlägen für risikominimierende Maßnahmen. Das IT-Security Management ist ferner dafür zuständig, IT-sicherheitsrelevante Vorfälle zu bewerten und geeignete Abhilfemaßnahmen zu initiieren.

Das IT-Security Management steht in enger Abstimmung mit dem ISB, welcher die Schnittstelle zum ISMS der VAV bildet.

Weitere Details zu den konkreten Aufgaben der Mitarbeiter des IT-Security-Managements sind der Stellenbeschreibung zu entnehmen.

2.4.6 Mitarbeiter

Alle Mitarbeiter sind zur Einhaltung der Vorgaben zur Informationssicherheit verpflichtet. Im Rahmen ihrer Tätigkeit und Aufgaben sind sie für eine ordnungsgemäße Verarbeitung und Sicherung der ihnen zugänglichen Informationen zuständig.

Der Begriff „Mitarbeiter“ umfasst auch Zeitarbeitskräfte.

2.4.7 Dienstleister

Dienstleister im Sinne dieser Richtlinie sind alle Personen und Unternehmen, die für die VAV Informationen verarbeiten oder auf diese Zugriff haben. Dienstleister sind zur Einhaltung der Informationssicherheit entsprechend der vertraglichen Vorgaben verpflichtet. Im Rahmen ihrer Tätigkeit und Aufgaben sind sie für eine ordnungsgemäße Verarbeitung und Sicherung der ihnen zugänglichen Informationen verantwortlich.

2.4.8 Informationseigentümer

Zur Gewährleistung der Informationssicherheit in den Informationssystemen sind vom Vorstand Informationseigentümer (ehemals Dataowner) zu benennen. Die Informationseigentümer sind die jeweils bestellten Dezentralen Datenschutz-Verantwortlichen. Dies sind in der Regel die fachlich zuständigen Abteilungsleiter. Diese werden in dem Dokument „Verantwortliche und Beauftragte in der VAV“ geführt.

Der Informationseigentümer hat folgende Aufgaben:

- Erstellung und Pflege von Rollen- und Berechtigungskonzepten für die von ihm verantworteten Informationssysteme unter Berücksichtigung der internen Vorgaben,
- Festlegung aller Rollen und der damit verbundenen Berechtigungen für die von ihm verantworteten Informationssysteme,
- Berücksichtigung der Funktionstrennung,
- Regelmäßige (mindestens jährliche) Überprüfung des Rollen- und Berechtigungskonzepts auf Aktualität und Vollständigkeit,
- Erstellung von Lösch- und Sperrkonzepten für das von ihm verantwortete Informationssystem unter Berücksichtigung etwaiger rechtlicher oder betrieblicher Aufbewahrungsfristen,
- Bewertung und Freigabe von Anfragen zum Testen mit Produktivdaten des betroffenen Informationssystems,
- Überprüfung der Datenqualität im Informationssystem (die Verantwortung für die Qualität verbleibt beim erhebenden Bereich) und Veranlassung von Maßnahmen zur Qualitätsverbesserung in Abstimmung mit den betroffenen Fachbereichen.

Weitere Regelungen zur Bestimmung und zu den Voraussetzungen eines Informationseigentümers sind im Anhang D aufgeführt.

2.4.9 Risikoverantwortliche

Die Risikoverantwortlichen tragen die interne Verantwortung für die ihnen zugeordneten Risiken und entscheiden über die Risikobehandlungsstrategie. Die Risikoverantwortlichen sind im Risikomanagement dokumentiert. Die Risikoverantwortlichen sind für die Inventarisierung der Informationswerte und die Festlegung des Schutzbedarfs der von ihnen verantworteten Prozesse zuständig.

2.4.10 Information Security Response Team

Das Information Security Response Team (ISRT) hat eine koordinierende Funktion und soll die schnelle Entscheidungsfindung im Falle von Sicherheitsvorfällen mit hohem Schadenpotential[2] ermöglichen. Das ISRT wird vom ISB einberufen und geleitet.

Das ISRT ist ein virtuelles Team und setzt sich bei einem IT-Sicherheitsvorfall aus folgenden Rollen zusammen:

- ISB
- DSB
- zwei Mitarbeiter IT (inkl. Protokollführung)

Bei einem Non-IT-Sicherheitsvorfall aus folgenden Rollen:

- ISB
- DSB
- Zwei Mitarbeiter FM (inkl. Protokollführung)

Das Team kann bei Bedarf durch den ISB um weitere Funktionen, z.B. den Compliance-Beauftragten, den Leiter Unternehmenskommunikation, den Leiter Personal etc. erweitert werden. Der ISB bildet die Schnittstelle zum Lagezentrum, sollte dies aktiv sein.

[2] Gemäß den Wesentlichkeitsgrenzen zum Schadenpotenzial aus dem Risikomanagement

2.5 Informationssicherheitsrisikomanagement

Informationssicherheitsrisiken müssen frühzeitig erkannt, bewertet, behandelt und überwacht werden. Hierzu bedarf eines einheitlichen und nachvollziehbaren Verfahrens zur Ermittlung und Bewertung von Risiken.

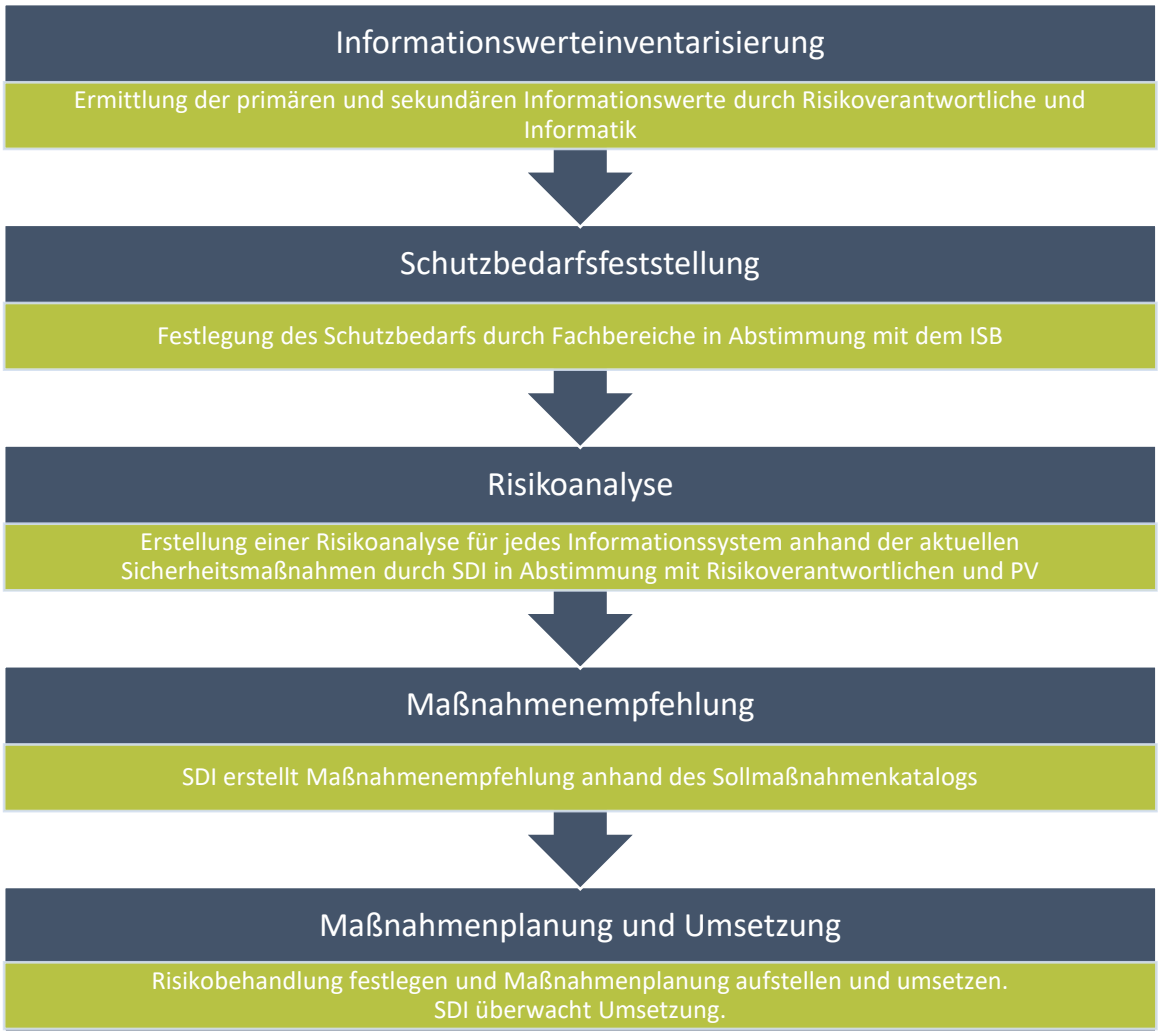

Abbildung 1: Ablauf der Informationssicherheitsrisikoanalyse

Neben dem standardisierten Verfahren zur Erkennung von Informationssicherheitsrisiken ist es notwendig, dass jeder, der ein Informationssicherheitsrisiko vermutet oder erkannt hat, dieses z.B. beim ISB meldet. Selbstverständlich werden die Meldungen bzw. der Melder bei Bedarf vertraulich behandelt. Meldungen, die sich im Nachhinein nicht als relevant herausstellen, ziehen keine negativen Folgen für den Melder nach sich.

2.5.1 Inventarisierung der Werte

Informationen und andere Werte im Informationsverbund sind zu inventarisieren. Das Inventar der Werte sollte genau, aktuell und konsistent sowie mit anderen Inventarverzeichnissen konsistent sein. Die Inventarisierung obliegt dem jeweils zuständigen Bereich.

2.5.2 Schutzbedarfsfeststellung

Die Schutzbedarfsfeststellung ist der Ausgangspunkt jeder Informationssicherheitsrisikoanalyse. Da sich Rahmenbedingungen im Laufe der Zeit ändern können, sollte alle zwei Jahre überprüft werden, ob die Einstufung des Schutzbedarfs noch der aktuellen Situation entspricht. Bei neuen Prozessen oder bei wesentlichen Änderungen an bestehenden Prozessen, insbesondere der Einführung neuer Systeme oder bei sicherheitsrelevanten Änderungen an Systemen sollte ebenfalls eine erneute Schutzbedarfsfeststellung durchgeführt werden.

Die Schutzbedarfsfeststellung ist auf Basis der Geschäftsprozesse von den Risikoverantwortlichen in Abstimmung mit dem ISB durchzuführen. Hierbei sind die in dem jeweiligen Geschäftsprozess verwendeten Informationssysteme zu berücksichtigen und zu dokumentieren. Die Bewertung des Schutzbedarfs hat anhand der Schutzziele Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität sowie der Wesentlichkeitsgrenzen des Risikomanagements zu erfolgen (vgl. Richtlinie Risikomanagement). Die Ergebnisse der Schutzbedarfsfeststellung sind vom ISB an die IT zu übergeben. Die IT hat sicherzustellen, dass der ermittelte Schutzbedarf von den Geschäftsprozessen auf die IT-Komponenten im Verantwortungsbereich der IT vererbt wird. Die Vererbung ist von der IT zu dokumentieren.

2.5.3 Informationssicherheitsrisikoanalyse

Die Informationssicherheitsrisikoanalyse ist vom ISB auf Grundlage der Schutzbedarfsfeststellung durchzuführen und muss sich auf Informationssysteme beziehen. Darüber hinaus können Risikoanalysen für Dienstleister, Personal, Standorte und Hardware durchgeführt werden. Bei der Analyse sind die bestehenden Sicherheitsmaßnahmen zu berücksichtigen und zu dokumentieren und mit den Soll-Maßnahmen zu vergleichen. Für die Soll-Maßnahmen ist von SDI ein Katalog mit Standardmaßnahmen unter Berücksichtigung der rechtlichen und regulatorischen Anforderungen und gängiger Standards zu erstellen. Die Maßnahmen in dem Katalog müssen den Schutzbedarf berücksichtigen. Sollte sich im Rahmen der Informationssicherheitsrisikoanalyse ergeben, dass einzelne Maßnahmen aus dem Soll-Maßnahmen-Katalog im Einzelfall nicht anwendbar oder nicht notwendig sind, ist dies vom ISB im Rahmen der Risikoanalyse zu dokumentieren.

Bei der Ermittlung von Gefährdungen sind (branchen-)spezifische Gefährdungen, die das Unternehmen betreffen, zu berücksichtigen. Darüber hinaus können die Standardgefährdungen des BSI (BSI – G 0 Elementare Gefährdungen) vom ISB herangezogen werden.

Die Ermittlung des konkreten Risikowerts hat anhand der nachfolgend dargestellten Matrix zu erfolgen, welche neben der Eintrittswahrscheinlichkeit das mögliche Schadenausmaß berücksichtigt. Die Ergebnisse der Informationssicherheitsrisikoanalyse sind nachvollziehbar vom ISB zu dokumentieren. Den konkreten Ablauf der Informationssicherheitsrisikoanalyse kann der ISB auf Basis der hier geregelten Vorgaben und unter Berücksichtigung der Anforderungen des Risikomanagements in einem ISMS-Handbuch regeln.

EINTRITTSWAHRSCHEINLICHKEIT		RISIKOWERT		
sehr hoch (=4)	< 2 Jahre	4	8	12
Hoch (=3)	> 2 - 5 Jahre	3	6	9
Mittel (=2)	> 5 - 20 Jahre	2	4	6
Gering (=1)	> 20 Jahre	1	2	3[3]
SCHADENSZENARIEN		SCHADENPOTENZIAL		
Finanzieller Schaden		Gering (=1)	Mittel (=2)	Hoch (=3)
Reputativer Schaden				
Regulatorischer Schaden				

Tabelle 1: Risikomatrix

Ungeachtet der turnusmäßigen Schutzbedarfsfeststellungen und Risikoanalysen (alle zwei Jahre) sind Informationssicherheitsrisiken auch dann zu ermitteln und zu bewerten, wenn es zu wesentlichen Änderungen an bestehenden Prozessen, z.B. durch die Einführung neuer Systeme oder sicherheitsrelevanter Änderungen kommt.

2.5.4 Risikobehandlung

Die Risikobehandlung dient der dokumentierten Entscheidungsfindung, wie mit den identifizierten und bewerteten Risiken umzugehen ist. Die Behandlung von Risiken im „grünen Bereich“ (siehe Risikomatrix unter 2.5.3) wird von den Risikoverantwortlichen verantwortet und gesteuert. Risiken im „gelben“ und „roten“ Bereich sind immer zu behandeln. Die Art und Weise der Behandlung ist vom Risikoverantwortlichen in Abstimmung mit dem ISB festzulegen und der Geschäftsleitung zu berichten.

Bei der Risikobehandlung stehen den Risikoverantwortlichen grundsätzlich vier unterschiedliche Steuerungsmöglichkeiten (Reduktion, Transfer, Vermeidung und Akzeptanz) zur Verfügung.

[3] Risiken in dieser Kategorie werden individuell vom ISB in Abstimmung mit dem Risikomanagement betrachtet und sodann über die Art und Weise der Behandlung und etwaige notwendige Maßnahmen entschieden. Soweit eine Behandlung erforderlich ist, erfolgt eine Aufnahme in den Risikobehandlungsplan des ISB.

2.5.4.1 Reduktion

Eine Möglichkeit zur Reduzierung von Risiken ist die Ergreifung von zusätzlichen Sicherheitsmaßnahmen unter Berücksichtigung des Soll-Maßnahmenkatalogs von SDI. Bei der Auswahl von geeigneten Maßnahmen sind neben den Auswirkungen auf das Sicherheitsniveau auch immer Kosten-Nutzen-Aspekte und die Praxistauglichkeit mit zu betrachten. Dies ist wichtig, um Ressourcen nicht unnötig aufzubringen und um die notwendigen Investitionen zur Erreichung eines angemessenen Sicherheitsniveaus gewährleisten zu können. Bei der Auswahl von Sicherheitsmaßnahmen sollte sich insbesondere auf solche fokussiert werden, die Risiken mit einem hohen Risikowert (vgl. Risikomatrix) entgegenwirken und / oder besonders effektiv sind.

2.5.4.2 Transfer

In Einzelfällen kann es sinnvoll sein, Risiken auf andere Unternehmen zu übertragen, beispielsweise durch den Abschluss einer Versicherung oder die Auslagerung einer Tätigkeit. Gründe hierfür können z.B. sein:

- die möglichen Schäden sind rein finanzieller Art,
- es ist ohnehin, aus anderen Gründen, geplant, Teile der Geschäftsprozesse auszulagern,
- der Vertragspartner ist aus wirtschaftlichen oder technischen Gründen besser in der Lage mit dem Risiko umzugehen.

Im Bereich der kritischen Dienstleistung steht die Versorgungssicherheit der Bevölkerung im Vordergrund, so dass Risiken mit Blick auf die Verfügbarkeit der kritischen Dienstleistung nicht transferiert werden können.

2.5.4.3 Vermeidung

Durch die Einstellung eines Geschäftsfeldes oder sich ändernde Rahmenbedingungen können Risiken entfallen.

2.5.4.4 Akzeptanz

Eine weitere Form der Risikobehandlung ist die bewusste Akzeptanz von Risiken (auch Risikoübernahme genannt).

Eine Akzeptanz von wesentlichen Risiken (d. h. solchen im gelben und roten Bereich) ist nur möglich, wenn

- die entsprechende Gefährdung nur unter ganz speziellen Voraussetzungen zu einem Schaden führt, oder
- gegen die Gefährdung derzeit keine wirksamen Gegenmaßnahmen bekannt sind und die Gefährdung sich in der Praxis auch kaum vermeiden lässt, oder
- die Umsetzung von Maßnahmen oder Informationssicherheitsvorgaben aus technischen oder rechtlichen Gründen (aktuell) nicht möglich ist,
- Aufwand und Kosten unverhältnismäßig sind mit Blick auf den angestrebten Schutzzweck, und
- die Gründe vom Risikoverantwortlichen dokumentiert, vom ISB bewertet und von der Geschäftsleitung akzeptiert werden. Die Risikoakzeptanz seitens der Geschäftsleitung kann über bestehende Genehmigungsverfahren, z.B. im Rahmen des „ORSA-Berichts“ erfolgen.

Eine dauerhafte Akzeptanz von gelben und roten Risiken mit Auswirkungen auf die Verfügbarkeit der

kritischen Dienstleistung ist grundsätzlich ausgeschlossen.

2.5.5 Risikobehandlungsplan

Für wesentliche Risiken, d. h. Risiken im gelben und roten Bereich ist die Art der Behandlung durch den Risikoverantwortlichen in Abstimmung mit dem ISB festzulegen und durch den ISB im Risikobehandlungsplan zu dokumentieren. Im Falle der Risikoreduktion ist eine Beschreibung der Maßnahme(n) sowie des aktuellen Status aufzunehmen, der Name des/der Risikoverantwortlichen sowie die Umsetzungsfrist(en). Aus dem Risikoplan muss darüber hinaus der Risikowert (vor und nach der Maßnahme) erkennbar sein. Im Falle der Risikoakzeptanz sind die Gründe im Risikobehandlungsplan zu vermerken. Änderungen am Status von Maßnahmen, den Terminen oder am Risiko sind vom ISB nachvollziehbar im Risikobehandlungsplan zu dokumentieren. Fristverlängerungen bedürfen der vorherigen Zustimmung des ISB und sind der Geschäftsleitung im Rahmen der vierteljährlichen Berichterstattung des ISB zur Kenntnis zu bringen.

Die Risikoverantwortlichen sind für die Maßnahmenplanung, Budgetierung und Umsetzung von Maßnahmen verantwortlich. Der ISB überwacht den Umsetzungsstand. Änderungen am vereinbarten Umsetzungstermin oder in der Ausgestaltung der Maßnahmen sind umgehend von den Risikoverantwortlichen an den ISB zu melden.

Der ISB hat über die Risiken und Maßnahmen aus dem Risikobehandlungsplan und deren Status sowie etwaige Prolongationen vierteljährlich zu berichten.

Wesentliche Informationssicherheitsrisiken sind durch den ISB an das Risikomanagement und den Vorstand zu melden.

2.6 Schulung und Sensibilisierung

Alle Mitarbeiter müssen über ein angemessenes Informationssicherheitsbewusstsein, in Abhängigkeit ihrer Tätigkeit, verfügen. Dieses ist über regelmäßige und zielgruppenspezifische Schulungen und Sensibilisierungen sicherzustellen. Der ISB initiiert und überwacht die insoweit notwendigen Maßnahmen.

2.7 Überprüfungen der Informationssicherheit

Um Nichtkonformitäten zum ISMS und Informationssicherheitsrisiken frühzeitig zu erkennen, sind regelmäßig Überprüfungen hinsichtlich der Einhaltung der Anforderungen der Informationssicherheit durch SDI durchzuführen. Bei der Auditplanung sollen insbesondere die Bedeutung der betroffenen Prozesse (z.B. für den Geschäftsbetrieb), Ergebnisse vorheriger interner und externer Prüfungen sowie Erkenntnisse aus Sicherheitsvorfällen berücksichtigt werden. Für jedes Audit sind die Auditkriterien festzulegen. Die Bewertung muss anhand einer einheitlichen Systematik erfolgen. Die Ergebnisse der Audits sind der verantwortlichen Geschäftsleitung zur Kenntnis zu bringen. Feststellungen sind von SDI einem Risikoverantwortlichen zuzuordnen. Die Umsetzung der vereinbarten Maßnahmen ist durch SDI nachzuhalten.

Detaillierte Regelungen zu Informationssicherheitsaudits der SDI sind der „Arbeitsrichtlinie Auditmanagement" zu entnehmen.

Der Reifegrad des ISMS sollte regelmäßig erhoben werden. Die Prüfung und Bewertung des Managementteils der ISO 27001 sollte dabei durch die Interne Revision, die Prüfung und Bewertung des Annexes der ISO 27001 hingegen durch SDI erfolgen. Zum Zwecke der Vergleichbarkeit sollte eine einheitliche Bewertungsmatrix, die von der Geschäftsleitung verabschiedet ist, verwendet werden. Beide Bewertungen sollten alle zwei Jahre erfolgen.

Die Geschäftsleitung sollte darüber hinaus regelmäßig den Umsetzungsstand des ISMS bewerten. Die Bewertung sollte auf der Grundlage der Berichte des ISB, der Risikoberichterstattung des Risikomanagements und der Ergebnisse der Reifegradbeurteilung von SDI und der Internen Revision erfolgen. Zur Bestätigung der Wirksamkeit des ISMS können etablierte Verfahren und Berichte, mit der die Wirksamkeit von Governancesystemen im Unternehmen bewertet wird, genutzt werden.

2.8 Vorstandsberichterstattung und Bewertung des ISMS

Zur Überprüfung und Bewertung des ISMS ist eine regelmäßige (jährliche) Berichterstattung des ISB gegenüber der Geschäftsleitung erforderlich. Der Bericht sollte insbesondere eine Bewertung der Informationssicherheitslage umfassen, Informationen zu Projekten mit Informationssicherheitsbezug, Ausführungen zu Informationssicherheitsvorfällen und Ergebnisse aus internen und externen Audits. Der Bericht kann mit anderen Berichten, z.B. zum Datenschutz verbunden werden.

Darüber hinaus hat der ISB vierteljährlich über Änderungen der Risikosituation (im Vergleich zum Vorbericht) der Geschäftsleitung gegenüber zu berichten, d.h. insbesondere über bestehende Risiken, deren Behandlung und den Umsetzungsstand von Maßnahmen. Ad-hoc Berichtspflichten, z.B. im Falle von Sicherheitsvorfällen, bleiben hiervon unberührt.

2.9 Kontinuierliche Verbesserung der Informationssicherheit

Die kontinuierliche Verbesserung des ISMS soll durch regelmäßig durchgeführte Effektivitätsmessungen gefördert werden. Hierzu sind Kennzahlen (KPI) vom ISB in Abstimmung mit der IT bzw. den Fachbereichen festzulegen, die eine Aussage über den Zustand, die Effektivität und die Reichweite geben und eine Steuerung ermöglichen. Die Ergebnisse der durchgeführten Messungen sind im Rahmen der Vorstandsberichterstattung und der Bewertung des ISMS dem Vorstand vorzulegen.

Die getroffenen Maßnahmen zur Aufrechterhaltung der Informationssicherheit sind jährlich durch SDI unter Beteiligung der betroffenen Fachbereiche dahingehend zu überprüfen, ob Sie dem Stand der Technik entsprechen.

3 VORGABEN ZUR INFORMATIONSSICHERHEIT

Um einen besseren Überblick über die allgemeinen Vorgaben und Regelungen zur Informationssicherheit zu bekommen, sind nachfolgend die wichtigsten Vorgaben in Kapitelform aufgeführt, die in themenspezifischen Arbeitsrichtlinien weiter konkretisiert werden.

Die Vorgaben zur Informationssicherheit sind grundsätzlich nach dem Stand der Technik umzusetzen. Etwaige Abweichungen vom Stand der Technik sind zu dokumentieren und bei entsprechender Relevanz als Risiko oder Nichtkonformität zu prüfen.

3.1 Meldung eines Informationssicherheitsvorfalls

Mitarbeiter und Dienstleister der VAV sind bei Verdacht oder zufälligem Bemerken eines etwaigen Informationssicherheitsvorfalls verpflichtet, diesen umgehend zu melden.

Hierfür dient folgende Kontaktstelle:

E-Mail: sicherheitsvorfall@vav.at

oder

telefonisch beim IT-Support

Durchwahl 666

Im Intranet und in der „Arbeitsrichtlinie Sicherheitsvorfall“ wird genau beschrieben, wie ein Informationssicherheitsvorfall zu melden ist.

Zur Orientierung sind im Glossar einige Beispiele zu Informationssicherheitsvorfällen aufgeführt. Im Zweifelsfall ist eine Meldung abzugeben. Meldungen, die sich im Nachhinein nicht als relevant herausstellen, ziehen keine negativen Folgen für den Melder nach sich.

Detaillierte Informationen zum Vorgehen bei Sicherheitsvorfällen sind der „Arbeitsrichtlinie Sicherheitsvorfall“ zu entnehmen.

Alle betroffenen Mitarbeiter haben eine schnelle und umfassende Unterstützung sicherzustellen.

Aufgrund des hohen technischen Vernetzungsgrades der Systeme innerhalb der VHV Gruppe können Informationssicherheitsrisiken nicht isoliert für einzelne Unternehmen betrachtet werden, sondern müssen in einen übergeordneten Kontext gestellt werden. Um diesen Kontext zu ermitteln, informiert die SDI die VHV Gruppe regelmäßig über die Umsetzung der Informationssicherheitsanforderungen dieser Richtlinie im Rahmen der Konzernsicht zur Informationssicherheit.

Die Ansprechpartner für Informationssicherheit treffen sich regelmäßig zu Abstimmungsgesprächen zur Informationssicherheit. Die VAV muss die Selbstauskunft zur Dokumentation der Organisation der Informationssicherheit eigenständig führen. Die definierten Mindestinhalte und die Darstellung der Selbstauskunft sind in der VHV Group Policy Information Security (A) aufgeführt. Die wesentlichen Informationen aus Konzernsicht sind im Jahresbericht des Konzern-Informationssicherheitsmanagements enthalten.

Im Falle eines Sicherheitsvorfalles mit hohem Schadenpotential (siehe Kapitel „Schutzbedarfsfeststellung“ Handbuch Informationssicherheitsmanagementsystem) hat die SDI an die zentrale Anlaufstelle securityincident@vhv.de zu berichten, um eine Bewertung aus Gruppensicht anstellen zu können.

3.2 Berücksichtigung der Informationssicherheit in Projekten und Prozessen

Informationssicherheitsaspekte müssen bei Projekten, Maßnahmen und im Rahmen von Linienprozessen angemessen berücksichtigt werden. Dies sollte schon zu Beginn eines Projektes (z.B. bei der Anschaffung neuer Software oder bei der Planung von Geschäftsprozessen) erfolgen. In Projekten mit erhöhten Sicherheitsanforderungen ist die Bewertung der Risiken im Projektverlauf regelmäßig (z.B. bei Erfüllung von Meilensteinen) zu prüfen und bei Veränderungen anzupassen. Im Linienbetrieb ist die Einbindung von SDI insbesondere bei wesentlichen Änderungen von IT-Systemen oder an sicherheitsrelevanten Prozessen erforderlich. Sicherheitsmaßnahmen sind zu dokumentieren und von SDI im Rahmen der vorgesehenen Prozesse (z.B. im SEP) abzunehmen.

3.3 Clean Desk-Strategie

Nach der Clean-Desk-Strategie (auch Prinzip des aufgeräumten Schreibtisches genannt) muss der unbefugte Zugriff auf vertrauliche und streng vertrauliche Informationen am Arbeitsplatz verhindert werden. Daher sind vertrauliche und streng vertrauliche Informationen, z.B. auf Papier oder auf elektronischen Speichermedien, sicher zu verwahren.

Es dürfen nur Informationen am Arbeitsplatz verfügbar sein, die zur Erledigung der aktuellen Aufgaben benötigt werden. Für die momentane Arbeit nicht benötigte Informationen sind sicher zu verwahren.

Bei temporärer Abwesenheit vom Arbeitsplatz ist der Arbeitsplatzrechner zu sperren. Bei Arbeitsende ist der Arbeitsplatzrechner vollständig herunterzufahren.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Clean Desk" zu entnehmen.

3.4 Informationsklassifizierung

Damit sichergestellt ist, dass Informationen über ein angemessenes Schutzniveau verfügen, sind diese anhand der gesetzlichen Anforderungen, ihres Wertes, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung zu klassifizieren. Informationen bezeichnen alle Daten und Dokumente, die nicht durch die Schutzbedarfsfeststellung erfasst werden, unabhängig davon, in welcher Form sie vorliegen (elektronisch, auf Papier etc.). Die Verpflichtung zur Klassifizierung trifft den Dokumentenverantwortlichen und erfolgt über die Dokumentenlenkung (siehe hierzu „Arbeitsrichtlinie Lenkung dokumentierter Informationen“).

Die Klassifizierung bietet Personen im Umgang mit Informationen eine prägnante Angabe zu deren Handhabung und den notwendigen Schutzanforderungen.

Die Klassifizierung erfolgt anhand eines einheitlichen Klassifizierungsschemas, welches die Kategorien „offen“, „intern“, „vertraulich“ und „streng vertraulich“ enthält. Die Kategorie „intern“ ist gesellschaftsübergreifend zu verstehen und bezieht sich auf die gesamte VHV Gruppe.

Detaillierte Regelungen zu den einzelnen Klassifizierungsstufen sowie den damit verbundenen Sicherheitsanforderungen sind der „Arbeitsrichtlinie Informationsklassifizierung“ zu entnehmen.

3.5 Lenkung dokumentierter Informationen

Dokumente der schriftlich fixierten Ordnung müssen durch den Dokumentenverantwortlichen gelenkt werden, um sicherzustellen, dass sie verfügbar und für die Verwendung geeignet sind und angemessen geschützt werden, z.B. vor Verlust der Vertraulichkeit, vor unsachgemäßem Gebrauch oder Verlust der Integrität. Gleiches gilt für die von der ISO 27001 geforderten Dokumente sowie Dokumente, die eine wesentliche Bedeutung für die Wirksamkeit des ISMS haben.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Lenkung dokumentierter Informationen“ zu entnehmen.

3.6 Entsorgung von Datenträgern

Vertraulich und streng vertraulich Informationen sind sicher zu entsorgen bzw. zu vernichten. Dateien auf Datenträgern oder sonstigen Speichermedien müssen nach der Aussonderung sicher gelöscht oder zerstört werden, um eine nachträgliche Rekonstruktion der Daten zu verhindern.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Entsorgung von Datenträgern“ zu entnehmen.

3.7 Physische und umgebungsbezogene Sicherheit

Maßnahmen zum Zutrittsschutz und zum Schutz vor unberechtigten Dritten müssen umgesetzt werden.

Besonders wichtige IT-Komponenten (Server, Sicherungsmedien, Netzwerkkoppelungselemente, etc.) sollten in ausreichend geschützten Räumen untergebracht werden, um diese vor äußerlichen Einflüssen (Feuer, Wasser etc.) zu schützen. Zusätzlich sollten sie an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein. Der Zutritt zu wichtigen IT-Systemen und Räumen ist zu regeln.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Physische und umgebungsbezogene Sicherheit“ zu entnehmen.

3.8 Zugangssteuerung

Datenzugriffsmöglichkeiten sollten auf das erforderliche Mindestmaß beschränkt werden (Need-to-Know-Prinzip). Jeder Benutzer und Administrator sollte nur auf die Datenbestände zugreifen können, die er für seine tägliche Arbeit tatsächlich benötigt. Ausführbare Programme verfügen – analog zu Anwendern – über bestimmte Zugriffsrechte und Systemprivilegien. Auch Programme dürfen nur mit den Berechtigungen ausgestattet sein, die sie für ein fehlerfreies Funktionieren benötigen.

Allen Nutzern sollten Rollen und Profile zugeordnet werden.

Ebenso muss ein geeigneter Prozess existieren, um Berechtigungen bei Einstellung, Funktionsänderung oder Weggang von Mitarbeitern einzuräumen bzw. zu entziehen.

Die benötigten Rollen (fachlicher, technischer und administrativer Art), die damit verbundenen Rechte sowie die Vergabe- und Entzugsprozesse sind vom Informationseigentümer zu beschreiben. Das Konzept ist regelmäßig auf Aktualität und Angemessenheit vom Informationseigentümer zu überprüfen. Das Konzept hat auch Aspekte der Funktionstrennung zu berücksichtigen.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Zugangssteuerung“ zu entnehmen.

3.9 Umgang mit Kennwörtern

Kennwörter sind regelmäßig zu wechseln und müssen eine gewisse Mindestlänge und Komplexität aufweisen. Sie sind streng vertraulich. Es sollten unterschiedliche Kennwörter für Systeme und Anwendungen genutzt werden. Voreingestellte Passwörter (z.B. nach dem Kauf von Softwareprodukten) sind unverzüglich zu ändern.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Kennwörter" zu entnehmen.

3.10 Mobile Endgeräte

Es dürfen ausschließlich dienstlich bereitgestellte mobile Endgeräte und Datenträger in der VAV eingesetzt werden. Für mobile Endgeräte sind angemessene Zugriffs-/Zugangskontrollen einzurichten.

Mobile Endgeräte und Datenträger sind nach einem anerkannten Verfahren zu verschlüsseln (siehe hierzu auch Kapitel Kryptographie).

Detaillierte Regelungen sind der „Arbeitsrichtlinie Mobile Endgeräte" zu entnehmen.

3.11 Telearbeit

Bei Telearbeit (Homeoffice, alternierende Teleheimarbeit, mobiles Arbeiten) werden Informationen außerhalb der geschützten Betriebsumgebung verarbeitet. Um Sicherheitsrisiken zu minimieren, müssen insbesondere Vorkehrungen zur Absicherung der Kommunikation (durch eine angemessene Verschlüsselung) sowie zur Identifizierung- und Authentisierung der Nutzer getroffen werden.

Alle relevanten Daten, die im Rahmen der Telearbeit erstellt oder verändert werden, müssen gesichert werden.

Unabhängig davon, in welcher Form Informationen vorliegen, müssen sie vor unbefugtem Zugriff und anderen Sicherheitsrisiken geschützt werden.

Zudem muss eine sichere Entsorgung von Datenträgern bzw. eine sichere Löschung von Daten auch im Rahmen der Telearbeit gewährleistet sein.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Telearbeit“ zu entnehmen.

3.12 Fernwartung

Detaillierte Regelungen, insbesondere zu den Anforderungen, technischen Maßnahmen, Protokollierungen und sonstigen Regelungen, bezüglich Fernwartungen sind der „Arbeitsrichtlinie Fernwartung“ zu entnehmen.

3.13 Individuelle Datenverarbeitung (IDV)

Individuelle Datenverarbeitungen (IDV) müssen grundsätzlich dieselben Datenschutz- und Informationssicherheitsanforderungen erfüllen, wie die zentral zur Verfügung gestellten Anwendungssysteme. Der Risikoverantwortliche, der die IDV betreibt, ist dafür zuständig, wesentliche IDV in einem zentralen Register zu inventarisieren und der Kritikalität entsprechende Sicherheitsvorkehrungen zu treffen.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Individuelle Datenverarbeitung" zu entnehmen.

3.14 Datensicherung (Backup)

Um Daten vor Verlust zu schützen, sind regelmäßig Sicherungskopien (Backups) von Informationen, Software und Systemen zu erstellen. Es ist zu gewährleisten, dass alle wichtigen Informationen und Softwareanwendungen nach einem Schaden oder Medienausfall wiederhergestellt werden können.

Es sollte regelmäßig verifiziert werden, dass die Datensicherung auch tatsächlich funktioniert und die Daten erfolgreich wieder eingespielt werden können.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Datensicherung" zu entnehmen.

3.15 E-Mail

E-Mails sind während des Transports grundsätzlich zu verschlüsseln. Hierfür ist ein anerkanntes Verschlüsselungsverfahren zu verwenden.

Die Einrichtung einer automatischen Weiterleitungsfunktion an Empfänger außerhalb des VAV-Netzes ist grundsätzlich untersagt.

Weiterhin ist durch ein Anti-Spam-Konzept sicherzustellen, dass keine Spam-E-Mails zu den Mitarbeitern gelangen und verhindert wird, dass Spam-E-Mail vom Unternehmen an Dritte (Kunden, Partnerunternehmen usw.) geschickt bzw. weitergeleitet werden. E-Mails, die durch den Spam-Filter zurückgehalten wurden, sind mit größter Sorgfalt vor einer Weiterleitung an das eigene Postfach zu prüfen.

3.16 Kryptographie

Bei der Übertragung vertraulicher bzw. streng vertraulicher Informationen innerhalb und außerhalb des VAV-Netzwerkes (z.B. über das Internet) und der Speicherung von Informationen auf mobilen Endgeräten und mobilen Datenträgern, sind kryptographische (verschlüsselte) Verfahren einzusetzen, um die Vertraulichkeit, Integrität, Authentizität und Verbindlichkeit sicherzustellen.

Bei der Anwendung von kryptographischen Verfahren ist auf die jeweils gängigen Standards zurückzugreifen.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Kryptographie" zu entnehmen.

3.17 Protokollierung und Überwachung

Sicherheitsrelevante Aktivitäten von Benutzern und Administratoren sind zum Zwecke einer späteren Nachvollziehbarkeit für alle IT-Systeme und Anwendungen manipulationssicher zu protokollieren und auszuwerten. Durch eine laufende Überwachung der Protokolle sollen Anomalien erkannt und die Ursache ermittelt werden. Es ist ein Monitoring der Systeme zu etablieren, um insbesondere Störungen der Verfügbarkeit zeitnah zu erkennen und Gegenmaßnahmen einzuleiten.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Protokollierung und Überwachung" zu entnehmen.

3.18 Schutz vor Schadsoftware

Auf allen potenziell von Schadsoftware gefährdeten Systemen ist ein angemessener, aktiver Schutz vor Schadcode einzurichten. Hierbei ist ein mehrstufiges Konzept zum Schutz vor Schadcode mit unterschiedlichen Erkennungstechnologien zu etablieren.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Schutz vor Schadsoftware“ zu entnehmen.

3.19 Handhabung technischer Schwachstellen

Für alle in der VAV eingesetzten Softwareprodukte (z.B. Anwendungen, Betriebssysteme) ist ein standardisiertes Softwareaktualisierungsverfahren für sicherheitsrelevante Patches zu betreiben. Hierbei ist insbesondere sicherzustellen, dass kritische Sicherheitslücken zeitnah geschlossen werden. Sollten keine Softwareaktualisierungen zur Schließung der Sicherheitslücke vorhanden sein, sind andere mitigierende Maßnahmen zu ergreifen. Das Einspielen von Sicherheitspatches ist vorab zu testen.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Sicherheitspatches“ zu entnehmen.

Weiterhin muss aktiv nach Schwachstellen in Anwendungen und IT-Systemen gesucht und die erkannten Schwachstellen müssen zeitnah geschlossen werden. Hierzu sind geeignete Verfahren und Prozesse zu etablieren.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Handhabung technischer Schwachstellen“ zu entnehmen.

3.20 Betriebssicherheit

Betriebsverfahren und Abläufe sind zu dokumentieren (z.B. Installationen und Konfigurationen von Systemen, Verfahren für System-Neustarts, Umgang mit Datensicherungen etc.).

Änderungen an Geschäftsprozessen, an den informationsverarbeitenden Einrichtungen und an den Systemen sind zu planen. Wesentliche Änderungen sind zu dokumentieren und müssen formelle Genehmigungsverfahren durchlaufen. Im Rahmen dieser Verfahren sind auch Sicherheitsaspekte zu berücksichtigen. Änderungen, welche ein bestehendes Risiko verändern können, müssen an SDI gemeldet werden.

Aktualisierungen von Betriebssoftware, Anwendungen oder Programmbibliotheken obliegen grundsätzlich geschulten Administratoren.

Es dürfen nur IT-Systeme und sonstige technische Arbeitsmittel (z.B. mobile Endgeräte) genutzt werden, die von der VAV zur Verwendung freigegeben wurden.

Firmeneigene Hard- und Software darf vom Anwender nur für dienstliche Belange genutzt werden. Grundsätzlich ist sicherzustellen, dass jede Software oder Anwendung vor Inbetriebnahme in der VAV einen geregelten Software-Abnahme- / Beschaffungsprozess (inkl. Lizenzvorgaben) durchläuft, um die funktionalen und nichtfunktionalen Anforderungen der Informationssicherheit zu erfüllen.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Betriebssicherheit“ zu entnehmen.

3.21 Härtung von IT-Systemen und Servern

Betriebssysteme, Server und Clients müssen vor der Inbetriebnahme gehärtet werden. „Härten“ bedeutet, dass Softwarebestandteile und Funktionen, die zur Erfüllung der vorgesehenen Aufgabe des Programms nicht zwingend notwendig sind, entfernt/deaktiviert werden müssen, um Sicherheitsrisiken zu minimieren. Die Härtung ist zu testen. Die Umsetzung der Härtung ist nachvollziehbar zu dokumentieren.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Härtung von Systemen und Anwendungen“ zu entnehmen.

3.22 Kommunikationssicherheit

Interne Netze sind durch geeignete Schutzmechanismen voneinander abzuschotten, um Bedrohungen vorzubeugen. Entwicklungs- Test und Produktionsumgebungen sind getrennt voneinander zu betreiben.

Kein Computer, der geschäftsmäßig genutzt wird, darf ohne Schutz durch geeignete Firewalls mit dem Internet verbunden werden.

Es muss regelmäßig überprüft werden, ob die bestehenden Filterregeln und das Firewall-Konzept noch aktuell und angemessen sind.

Alle Funktionen, Serverdienste und offenen Kommunikationsports, die nach außen angeboten werden, erhöhen das Risiko, dass eine Schwachstelle ausgenutzt werden kann. Daher sollte sorgfältig geprüft werden, ob einzelne Dienste und Funktionen tatsächlich benötigt werden oder lediglich aufgrund von Standardeinstellungen aktiv sind.

Im Webbrowser sollten nur die aktiven Inhalte bzw. Skriptsprachen und Multimedia-Plugins zugelassen werden, die für die Arbeit unverzichtbar sind. Besonders riskante Skriptsprachen sollten deaktiviert werden.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Kommunikationssicherheit“ zu entnehmen.

3.23 Sichere Entwicklung

In den verschiedenen Phasen des Softwareentwicklungsprozesses ist der Grundsatz „Security by Design“ zu beachten. Zudem sind die Datenschutzgrundsätze „Privacy by Design“ und „Privacy by Default“ zu berücksichtigen.

Entwickler haben sich an anerkannte Standards der Programmierung zu halten, um Schwachstellen vorzubeugen. Zur Qualitätssicherung sind Code Reviews durchzuführen.

Produktive Daten dürfen nur in Ausnahmefällen – soweit dies zur Erfüllung des konkreten Testzwecks erforderlich ist – genutzt werden. Ansonsten sind synthetische, anonymisierte oder zumindest pseudonymisierte Daten zu nutzen. Testdaten sind sorgfältig auszuwählen und zu schützen. Die Testumgebungen sind angemessen – entsprechend den Produktivumgebungen – abzusichern.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Sichere Entwicklung“ zu entnehmen.

3.24 Externe Prüfungen und Penetrationstests

Externe Audits sollten regelmäßig durchgeführt werden, um Nichtkonformitäten mit rechtlichen, regulativen und gesetzlich vorgeschriebenen Anforderungen zu identifizieren. Die identifizierten Abweichungen sind entsprechend ihrer Kritikalität zu behandeln.

Penetrationstests sollten insbesondere für Systeme, die aus den externen bzw. nicht abgesicherten Netzen erreichbar sind (z.B. Webserver), durchgeführt werden. Sie ersetzen nicht Qualitätssicherungen (Code-Reviews) oder technische Audits. Penetrationstests sind zu planen. Erkannte Schwachstellen sind entsprechend ihrer Kritikalität zu behandeln.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Externe Prüfungen und Penetrationstests“ zu entnehmen.

3.25 Informationssicherheitsaspekte im BCM

Im Rahmen des Business Continuity Managements (BCM) sind Aspekte der Informationssicherheit angemessen zu berücksichtigen. Informationssicherheitsmaßnahmen sind auch in Notfall- und Krisensituationen einzuhalten. Falls die Sicherheitsmaßnahmen die Informationen nicht mehr schützen können, sollten andere Maßnahmen festgelegt, umgesetzt und aufrechterhalten werden, um eine ausreichende Informationssicherheit zu gewährleisten. Hierbei ist der ISB einzubinden.

Für Notfall- und Krisensituationen sind angemessene Verfahren zu etablieren, die die Handhabung beschreiben und die Verantwortlichkeiten regeln.

Notfall- und Wiederherstellungspläne müssen regeln, welche Maßnahmen im Falle von Notfällen zu ergreifen sind.

Detaillierte Regelungen sind der „Konzernrichtlinie Business Continuity Management“ zu entnehmen.

3.26 Personelle Sicherheit

Bei der Einstellung neuer Mitarbeiter ist abhängig von der Funktion eine angemessene Sicherheitsüberprüfung durchzuführen und zu dokumentieren. Weiterhin sind alle Mitarbeiter auf Verschwiegenheit und auf die Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen zu verpflichten. Diese Pflicht muss über die Beendigung des Arbeitsverhältnisses hinaus gelten.

Es sind Regeln und Prozesse zu implementieren, die sicherstellen, dass bei Einstellung, Stellenwechsel oder Beendigung des Arbeitsverhältnisses alle Assets zurückgenommen und Berechtigungen angepasst bzw. entzogen werden.

Detaillierte Regelungen sind der „Arbeitsrichtlinie Personalsicherheit" zu entnehmen.

3.27 Dienstleister

Es sind klare Regelungen mit Dienstleistern bezüglich der zu erbringenden Leistung und der Vertragsmodalitäten, zu treffen.

Betreffend der Informationssicherheit sind Mindestanforderungen zu definieren, die von Dienstleistern (je nach Art Dienstleistung) zu erfüllen sind. Hierbei sind die gesetzlichen und regulatorischen Anforderungen zu beachten.

In Abhängigkeit von der Dienstleistung und dem damit verbundenen Risiken, sind Regelungen zur Mitteilung von Sicherheitsvorfällen, Meldestellen sowie Vorkehrungen im Falle von Notfällen zu treffen, um die Verfügbarkeit der Informationen sicherzustellen.

Dienstleister sind auf Vertraulichkeit zu verpflichten. Datenschutzvereinbarungen sind zu treffen, wenn personenbezogene Daten verarbeitet werden.

A Interessierte Parteien

Interessierte Partei	Anforderung	Art der Berücksichtigung
Mitarbeiter	• Sicherer Umgang mit den eigenen Daten (insbesondere Wahrung der Vertraulichkeit) • Transparenz über die Anforderungen der Informationssicherheit (insbesondere über die bestehenden Pflichten)	• Berücksichtigung von Datenschutz- und Sicherheitsaspekten in Personalprozessen und Betriebsvereinbarungen • Zentrales Postfach zur Kontaktaufnahme für Mitarbeiter • Schulungen und Awareness-Kampagnen für Mitarbeiter
Gesetzgeber	• Beachtung der geltenden Gesetze (Compliance)	• Frühwarnfunktion der Abteilung Compliance & Recht und Rechtsmonitoring durch SDI mit Blick auf datenschutz- und sicherheitsrelevante Änderungen.
Kunden und sonstige Betroffene (Versicherungsnehmer, Anspruchsteller etc.)	• Angemessene Vorkehrungen zum Schutz der Daten • Verfügbarkeit von Diensten (z.B. Portalen) • Schnelle und unkomplizierte Bearbeitung von Anträgen, Schäden etc.	• Umsetzung von Maßnahmen entsprechend der internen und externen Vorgaben • Notfallkonzepte • Laufendes Monitoring der Verfügbarkeit von Systemen • Transparenz über Maßnahmen, z.B. über Datenschutzhinweise • Hinweise auf der Homepage
Vorstand	Einhaltung von Gesetzen, Regularien und internen Vorgaben • Vermeidung der persönlichen Haftung • Verhinderung von Schäden für das Unternehmen • Sicherstellung eines angemessenen Sicherheitsniveaus • Transparenz über Risiken	• Entscheidung über sicherheitsrelevante Maßnahmen (vgl. Kapitel 2.5) • Regelmäßige Berichterstattung über Berichte und Vorstellungen in Vorstands-/ GF-Sitzungen • Abstimmung über Ressortmeetings • Informationen über aktuelle Themen, z.B. rechtliche Änderungen
Betriebsrat	• Frühzeitige Einbindung bei mitbestimmungspflichtigen Sachverhalten • Einhaltung der Regelungen in der Betriebsvereinbarung	• Regelmäßiger Austausch z.B. bei der Erstellung von Betriebsvereinbarungen • Austausch über Betriebsratssitzungen bei aktuellen Anlässen
Datenschutzbeauftragter	• Vorhaltung von angemessenen technischen und organisatorischen Vorkehrungen nach dem Stand der Technik zur Erreichung der Schutzziele der DSGVO	• Einbindung des DSB in wesentliche, datenschutzrechtliche Geschäftsprozesse
Aufsichtsbehörden	• Einhaltung der regulatorischen Vorgaben	• Auswertung von FMA und VVO Newslettern

	• Berichterstattung bei Unregelmäßigkeiten	• Teilnahme an Veranstaltungen der FMA • Berichterstattung über Compliance • Teilnahme an Abfragen der FMA
Vertriebspartner, z.B. Vermittler	• Sicherer Umgang mit den Kundendaten sowie mit den eigenen Daten (insbesondere Vertraulichkeit) • Verfügbarkeit von Diensten (z.B. von Portalen und Anwendungen) • Schnelle Bearbeitung von Anliegen • Berücksichtigung der vertrieblichen Belange bei der Sicherheitsplanung und Umsetzung	• Umsetzung von Maßnahmen entsprechend der internen und externen Vorgaben • Notfallkonzepte • Laufendes Monitoring der Verfügbarkeit von Systemen • Transparenz über Maßnahmen, z.B. über Datenschutzhinweise • Regelmäßiger Austausch des Vertriebs mit Maklern • Maklerzufriedenheitsumfragen
Bevölkerung	• Versorgungssicherheit bei der Erbringung der kritischen Dienstleistung • Vermeidung von Versorgungsengpässen der kritischen Dienstleistung • Gewährleistung der öffentlichen Sicherheit	• Berücksichtigung bei der Auswahl von Risikobehandlungsalternativen, sofern die kritische Dienstleistung betroffen ist
Gesellschaften der VHV Gruppe außerhalb des Geltungsbereichs dieser Richtlinie	• Vorgabe umsetzbarer Anforderungen an die Informationssicherheit • Austausch und Hilfestellung zu Themen der Informationssicherheit • Unterstützung bei Sicherheitsvorfällen mit hohem Schadenpotenzial	• Allgemeingehaltene Vorgaben in der Konzernrichtlinie Informationssicherheit • Regelmäßiger Austausch mit den Ansprechpartnern zur Informationssicherheit

B Externe Anforderungen

Anforderung	Kurzbeschreibung
DSGVO und DSG	Verpflichtung zur Vorhaltung von technischen und organisatorischen Maßnahmen nach dem Stand der Technik, Einhaltung der Datenschutzgrundsätze (Vertraulichkeit, Verfügbarkeit, Zweckbindung, Datensparsamkeit etc.)
VAG	Aufsichtsrechtliche Anforderungen an Versicherungsunternehmen bzw. im Gesetz definierte Gesellschaftsformen. Enthält u.a. Vorgaben zur Geschäftsorganisation und zu Berichtspflichten
Österreichischer Branchenstandard (Code of Conduct)	Freiwilliger Verhaltenskodex zum Umgang mit personenbezogenen Daten; Vorgaben zur Umsetzung der Datenschutzgrundsätze und zur Gewährleitung von Datensicherheit
Vertragliche Anforderungen	Service Level Agreements Verpflichtungen aus Auftragsverarbeitungs- bzw. Auslagerungsverträgen mit Dienstleistern Einhaltung von Vertraulichkeitsvereinbarungen
Gängige Standards (ISO/ IEC 27001)	Anforderungen für die Einrichtung, Umsetzung, Aufrechterhaltung und fortlaufende Verbesserung eines dokumentierten Informationssicherheits-management-Systems unter Berücksichtigung des Kontextes einer Organisation

C Chancen und Risiken des ISMS

C.1 Chancen durch ein ISMS

#	Chancen
1	Klare Strukturen
2	reproduzierbare und vergleichbare Prozesse und Ergebnisse
3	Erhöhung der Transparenz, z.B. für das Management und Außenstehende
4	Klare Verantwortlichkeiten
5	Verbesserte Risikoerkennung und Behandlung
6	Zielgerichtete und risikoorientierte Maßnahmensteuerung

7	Bessere Vergleichbarkeiten, auch mit anderen Unternehmen
8	Möglichkeiten zur Qualitätsmessung und kontinuierlichen Verbesserung
9	Erhöhung der Awareness bei Mitarbeitern und bei der Geschäftsleitung
10	Reduzierung von Sicherheitsrisiken
11	Erhöhung der Qualität der angebotenen Produkte und Leistungen
12	Beitrag zur Sicherung des Unternehmenserfolg und der dauerhaften Existenz
13	Minimierung von Haftungsrisiken und Sanktionen

Tabelle 2: Chancen durch ein ISMS

C.2 Risiken durch ein ISMS

#	Risiko
1	Fehlende oder unzureichende finanzielle Mittel
2	Fehlende oder unzureichende Ressourcen
3	Fehlende oder unzureichende inhaltliche Unterstützung der Geschäftsleitung
4	Widerstreitende Interessen (Wirtschaftlichkeit / betriebliche Interessen versus Sicherheit)
5	Verlust an Usability und Komfort
6	Fehlendes Verständnis der Mitarbeiter, z.B. aufgrund erhöhter Aufwände

Tabelle 3: Risiken durch ein ISMS

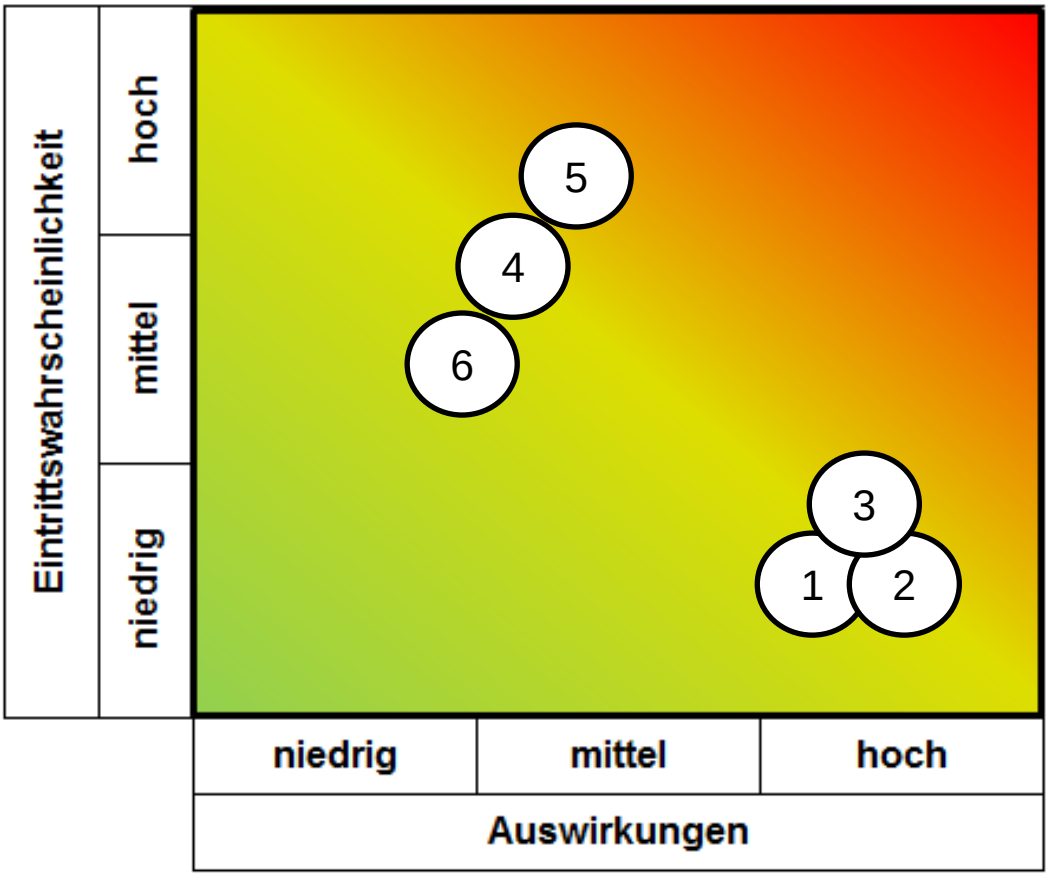

Abbildung 2: Matrix zu Risiken des ISMS

#	Risiko	Maßnahmen zur Risikoreduktion	Umsetzung	Wirksamkeitsprüfung
1	Fehlende oder unzureichende Mittel	Bekenntnis der Geschäftsleitung zur Bereitstellung von notwendigen Mitteln	IT-Strategie und Richtlinie Informationssicherheit	Bewilligte Budgetplanungen
2	Fehlende oder unzureichende Ressourcen	Bekenntnis der Geschäftsleitung zur Bereitstellung von notwendigen Ressourcen	IT-Strategie und Richtlinie Informationssicherheit	Bewilligte Personalanforderungen
3	Fehlende oder unzureichende inhaltliche Unterstützung der Geschäftsleitung	Schaffung von Awareness durch eine laufende Berichterstattung, Aufzeigen von Chancen und Risiken, Etablierung von Vortragsrechten im Rahmen von Geschäftsleitungssitzungen, Leitenden-Treffen etc.	SDI Berichte, Geschäftsordnung SDI, Rollen- und Funktionsbeschreibungen der Mitarbeiter SDI	Vortragsrechte in Vorstandssitzungen, Leitenden Runden, etc. Aktive Angebote zur Unterstützung durch die Geschäftsleitung
4	Widerstreitende Interessen (Wirtschaftlichkeit / betriebliche Interessen versus Sicherheit)	Regeln definieren, wie mit Zielkonflikten umzugehen	IT-Strategie und Richtlinie Informationssicherheit	Keine Umsetzung von Maßnahmen entgegen der Empfehlungen von SDI
5	Verlust an Usability und Komfort	Den Gewinn an Sicherheit den Betroffenen aufzeigen und die Reduktion von Risiken transparent machen	Projektbegleitung und Beratung durch SDI, Schulungs- und Awarenessmaßnahmen	Mitwirkung von SDI in Projekten, sofern inhaltlich notwendig oder sinnvoll. Durchgeführte Schulungs- und Awarenessmaßnahmen
6	Fehlendes Verständnis der Mitarbeiter, z.B. aufgrund erhöhter Aufwände	Vorteile aufzeigen, Alternativen und Lösungsmöglichkeiten bei der Umsetzung aufzeigen, Beratung anbieten; Schulungen durchführen	Projektbegleitung und Beratung durch SDI, Schulungs- und Awarenessmaßnahmen	Mitwirkung von SDI in Projekten, sofern inhaltlich notwendig oder sinnvoll. Durchgeführte Schulungs- und Awarenessmaßnahmen

Tabelle 4: Risiken des ISMS und deren Steuerung

D Glossar

Begriff	Erläuterung
Anwendbarkeitserklärung	Die Anwendbarkeitserklärung oder auch Statement of Applicability, kurz SOA, ist ein Vorgabedokument nach ISO 27001. Das Dokument enthält eine Beschreibung zur Umsetzung der einzelnen Maßnahmenvorgaben der ISO 27001.
Authentizität	Die Authentizität gehört zu den vier Schutzzielen der Informationssicherheit. Wie echt (glaubwürdig, zuverlässig, unverfälscht, wahr) ist eine Information? • Gewährleistung, dass ein Kommunikationspartner tatsächlich derjenige ist, der er vorgibt zu sein. • Eine authentische Information ist definitiv von der angegebenen Quelle erstellt worden. Gilt nicht nur für Personen, sondern auch für IT-Komponenten (Systeme) oder Anwendungen.
Bedrohung	Eine Bedrohung ist der potenzielle Verlust eines Schutzziels durch Ausnutzung von Schwachstellen durch einen Angreifer.
Datenqualität	Datenqualität beschreibt die Beurteilung der verwendeten oder bereitgestellten Informationen nach definierten, auf den jeweiligen Verwendungszweck abgestimmten Kriterien. Datenqualität gibt damit an, in welchem Maße die Daten den bestehenden Anforderungen entsprechen. Die Mindestkriterien hierfür sind: Angemessenheit / Gültigkeit: Die Daten dienen dem vorgesehenen Zweck und sind frei von Widersprüchen. Sie sind konsistent mit den zugrundeliegenden Annahmen bzw. Vorgaben für die weitere Verwendung. Richtigkeit / Exaktheit: Die Daten sind frei von wesentlichen Fehlern. Sie werden im Zeitablauf einheitlich und zeitgerecht erfasst. Vollständigkeit: Die Daten liegen lückenlos vor (z.B. der einzelne Antrag wurde vollständig ausgefüllt; alle Anträge wurden vom System verarbeitet). Fehlende Daten können eindeutig als solche identifiziert werden. Darüber hinaus können weitere Kriterien durch interne oder externe Vorgaben festgelegt werden (z.B. Solvency II, Standards, Arbeitsrichtlinien).
Dokumentenverantwortlicher	Ein Dokumentenverantwortlicher ist verantwortlich für den Inhalt, die Einhaltung der Vorgaben zur Dokumentenlenkung, das Review und die Ablage bzw. die Übergabe der jeweils aktuellen Fassung.

Begriff	Erläuterung
Gefährdung	Eine Gefährdung ist eine Bedrohung, die konkret über eine Schwachstelle auf ein Objekt einwirkt. Eine Bedrohung wird somit erst durch eine vorhandene Schwachstelle zur Gefährdung für ein Objekt.
Geschäftsleitung	Zusammenfassende Bezeichnung für die Vorstände (Aktiengesellschaften) und Geschäftsführer (GmbH) der hier genannten Konzerngesellschaften.
IDV	Individuelle Datenverarbeitung ist die Erstellung, Weiterentwicklung und der Betrieb von Anwendungen durch den Endbenutzer an seinem Arbeitsplatz, um Problemstellungen aus seinem individuellen Aufgabenbereich oder dem Aufgabenbereich des Fachbereichs zu lösen (betrifft nicht von der IT betriebene Kernsysteme).
Informationen	Informationen bezeichnen alle Daten und Dokumente, unabhängig davon in welcher Form sie vorliegen (elektronisch, auf Papier etc.) Informationen sind Vermögensgegenstände des Unternehmens und müssen geschützt werden.
Informationssicherheitsereignis	Informationssicherheitsereignisse sind Ereignisse, die die Sicherheit tangieren oder durch Sicherheitsmechanismen erzeugt wurden. Diese Ereignisse stellen in der Regel keine Verletzung von Sicherheitsvorgaben oder -mechanismen dar, sondern zeigen auf, dass diese funktioniert haben. So können Informationssicherheitsereignisse zum Beispiel durch einen Virenscanner erkannte Viren sein.
Informationssicherheitsvorfall	Als Informationssicherheitsvorfall wird ein informationssicherheitskritischer Vorfall bezeichnet, welcher eine angemessene Reaktion der VAV erfordert. Informationssicherheitsvorfälle können hierbei durch unterschiedlichste Situationen hervorgerufen werden. Oft ist nicht sofort erkennbar, ob der Vorfall auf einen gezielten Angriff, eine Fehlfunktion, eine unbeabsichtigte Handlung oder auf einen Irrtum zurückzuführen ist. Zur Verdeutlichung der Begrifflichkeit “Informationssicherheitsvorfall” hier einige Beispiele: Typische Sicherheitsvorfälle sind beispielsweise: • Auftreten von Schadsoftware z.B.: o Kryptotrojaner o Kryptominer • kriminelle Handlungen z.B.: o SPAM-Versand durch VAV o „CEO-Fraud“ o APT o De-Facing/Übernahme Website o Übernahme Social-Media-Account o Akten und sonstige Speichermedien gestohlen o Sabotage / Innentäter (Diskreditierung (falsche Spuren)) o Erpressung von Personen aufgrund gestohlener Daten

Begriff	Erläuterung
	○ Einbruch in Gebäude/Räumlichkeiten der VAV • Technologien mit schweren Sicherheitslücken (z.B. Spectre/Meltdown) • Gebrochene Krytoverfahren • Verlust zentraler Schlüssel • Ausfall von wesentlichen Teilen der IT-Systeme Solche Sicherheitsvorfälle können zum Beispiel ausgelöst werden durch: • Veröffentlichung oder Kenntnisnahme schutzwürdiger Informationen • Missbrauch von Rechten • das Fehlverhalten von Benutzern, Administratoren oder externen Dienstleistern, das zu sicherheitskritischen Änderungen von Systemparametern führt und gegen interne Richtlinien oder Anweisungen verstößt • gezielte oder ungezielte Cyber-Angriffe • Feststellung von Schadsoftware oder ungewöhnlichem Verhalten von IT-Geräten mit Sicherheitsbezug • Verletzung von Zugriffsrechten • Ausfall der Zutrittsberechtigungssysteme • unzureichende physische Sicherung des Zugriffs auf Informationen • durchgeführte Änderungen an Software, Hardware oder Infrastruktur • Hochwasser, Feuer, sonstige Umwelteinflüsse Abgrenzung: Die Bearbeitung von Störungen, Vorfällen und Konfigurationsfehlern des Regelbetriebs wird hier nicht betrachtet.
Informationssysteme	Ein Informationssystem ist eine Software bzw. ein Software-Paket für zugehörige fachliche Funktionen, die sich logisch und technisch von anderen Funktionsbereichen abgrenzen lässt und durch IT ganz oder überwiegend unterstützt wird.
Informationswerte	Informationswerte sind alle digitalen und physischen (elektronischen und papierbezogenen Daten) sowie das geistige Eigentum (Wissen) in einem Unternehmen. Informationswerte stellen den wesentlichen Faktor bei der Risikobetrachtung der Informationssicherheit dar. Sie werden in primäre und sekundäre Informationswerte unterschieden.
Informationswerte, primäre	Primäre Informationswerte sind Informationen, die für die Durchführung von Aktivitäten bzw. Prozessen notwendig sind und einen „Produktionsfaktor“ darstellen (z.B. Vertrags-, Kunden-, Tarifdaten).

Begriff	Erläuterung
Informationswerte, sekundäre	Sekundäre Informationswerte umfassen die zur Verarbeitung und Speicherung der primären Informationswerte genutzten Ressourcen (z.B. Software, Hardware, Papierakte, Standorte etc.). Bspw. wird ein Versicherungsantrag (primärer Informationswert) mit Hilfe einer Applikation verarbeitet und auf einer Datenbank, die wiederum auf einem Server liegt, gespeichert. Die Applikation, die Datenbank und der Server, auf dem die Datenbank liegt, können jeweils als sekundäre Informationswerte bezeichnet werden.
Informationsverbund	Der Informationsverbund ist eine Zusammenfassung der geschäftsrelevanten Informationen und Prozesse, der unterstützenden Prozesse und der zugehörigen IT-Systeme.
Integrität	Die Integrität gehört zu den vier Schutzzielen der Informationssicherheit. Die Integrität ist das Ziel der Sicherstellung der Richtigkeit und Vollständigkeit von Informationen und Verarbeitungsmethoden (Schutz vor unberechtigter Veränderung).
Mobile Endgeräte und Datenträger	Mobile Endgeräte sind zum Beispiel: • Mobile Computer, Notebooks, Tablets, • Smartphones, Mobiltelefone (z.B. Blackberry, iPhone). Mobile Datenträger sind zum Beispiel: • CDs/DVDs, • USB-Speichermedien, • Speicherkarten.
Penetrationstests	Penetrationstest (kurz Pentest) sind gezielte und beauftragte Angriffe von außen oder innen durch unabhängige Dritte, um Schwachstellen und sicherheitsrelevante Konfigurationsfehler zu erkennen.
Risk Committee	Die VHV Gruppe betreibt ein konzernweit konsistentes Risikomanagementsystem. Aufgrund der Vielzahl von Konzernunternehmen existiert das RC als gesellschaftsübergreifendes Organ. Die Hauptaufgabe des RC besteht vor diesem Hintergrund darin, im Auftrag der Vorstandsgremien, die konzerneinheitliche Weiterentwicklung der Risikomanagementsysteme, -methoden und -verfahren sicherzustellen.

Begriff	Erläuterung
Risiko	Risiko ist die häufig auf Berechnungen beruhende Vorhersage eines möglichen Schadens im negativen Fall (Gefahr) oder eines möglichen Nutzens im positiven Fall (Chance). Was als Schaden oder Nutzen aufgefasst wird, hängt von Wertvorstellungen ab. Risiko wird auch häufig definiert als die Kombination aus der Wahrscheinlichkeit, mit der ein Schaden auftritt, und dem Ausmaß dieses Schadens. Im Unterschied zu „Gefährdung“ umfasst der Begriff „Risiko“ bereits eine Bewertung, inwieweit ein bestimmtes Schadensszenario im jeweils vorliegenden Fall relevant ist.
Schadensszenario	Modellhafte Vorstellung einer bestimmten Schadenssituation, die durch eine Verletzung eines oder mehrerer Schutzziele (z.B. Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität) hervorgerufen worden ist.
Schutzziel	Die Schutzziele der Informationssicherheit lauten: • Vertraulichkeit, • Verfügbarkeit, • Integrität, • Authentizität.
Schwachstelle	Eine Schwachstelle ist ein sicherheitsrelevanter Fehler eines IT-Systems oder einer Institution. Ursachen können in der Konzeption, den verwendeten Algorithmen, der Implementation, der Konfiguration, dem Betrieb sowie der Organisation liegen. Eine Schwachstelle kann dazu führen, dass eine Bedrohung wirksam wird und eine Institution oder ein System geschädigt wird. Durch eine Schwachstelle wird ein Objekt (eine Institution oder ein System) anfällig für Bedrohungen.
Sicherheitsrelevante Aktivitäten	Sicherheitsrelevante Aktivitäten sind alle Aktionen: • die durch Administratoren, Benutzerkonten mit privilegierten Rechten und technischen Benutzerkonten durchgeführt werden, • von Anwendern, die eine Protokollierung gemäß DSGVO oder anderer regulatorischer Vorgaben erfordern.
Softwaresicherheitslücke	Eine Softwaresicherheitslücke ist im Gebiet der Informationssicherheit ein Fehler in einer Software, durch den ein Programm mit Schadwirkung oder ein Angreifer in ein Computersystem eindringen kann.
Statement Of Applicabilitiy (SOA)	Siehe „Anwendbarkeitserklärung“

Begriff	Erläuterung
Verfügbarkeit	Die Verfügbarkeit gehört zu den vier Schutzzielen der Informationssicherheit. Die Verfügbarkeit hat das Ziel, dass Informationen und Dienste im benötigten Umfang und Qualität zu einer definierten Zeit zur Verfügung stehen. Sie betrifft auch den Schutz notwendiger Ressourcen und damit zusammenhängender Fähigkeiten.
Vertraulichkeit	Die Vertraulichkeit gehört zu den vier Schutzzielen der Informationssicherheit. Die Vertraulichkeit bezeichnet das Ziel, dass Informationen ausschließlich berechtigten Personen, Einheiten oder Prozessen zur Verfügung stehen.
Werte	Siehe Informationswerte
Zu klassifizierende Informationen	Der Begriff der „zu klassifizierenden Informationen“ bezieht sich im Sinne dieser Richtlinie auf folgende Aspekte: • Informationen/Daten, die **automatisiert** mit Hilfe der IT-Anwendungen der VAV erzeugt, verarbeitet und ggf. weitergeleitet werden. Auf Informationen, die mit Hilfe der IT-Anwendungen automatisiert verarbeitet werden, hat der Mitarbeiter in der Regel den Zugriff auf diese Informationen ausschließlich über die IT-Anwendung und damit keinen Einfluss auf die vertrauliche Behandlung der Informationen innerhalb der IT-Anwendung. Die IT-Anwendung selbst regelt wie die Informationen verarbeitet und abgelegt werden, • Informationen, die aus IT-Anwendungen **individuell** weiterverarbeitet werden und/oder weitere individuell erzeugte Informationen (eingehende Schreiben, E-Mails, mit Office erzeugte Dateien, Faxe, individuelle Ausdrucke von IT-Anwendungen, Gespräche in öffentlichen Bereichen etc.) Bei diesen Informationen muss der Mitarbeiter selbst entscheiden, wer die Informationen lesen darf, wo er die Informationen ablegt, an wen er sie weiterleitet, wann und wie er sie vernichtet und wie er die Informationen ausdruckt. Beispiele hierfür sind Office-Dokumente und Ausdrucke aus IT-Anwendungen, • individuellen Informationen, bei denen der Autor/Dokumenteneigentümer selbst entscheiden muss, wer die Informationen lesen/erhalten darf, wo er die Informationen ablegt, an wen er sie weiterleitet, wann und wie er sie vernichtet und wie er die Informationen ausdruckt.