LL-INFORMATIONSSICHERHEIT

Dokumentenklassifizierung

Titel	LL-INFORMATIONSSICHERHEIT
Version	4.0
Freigabedatum	14.01.2025
Autor	sguhl
Verantwortlich	akusch
Freigegeben durch	akusch, mschmidt
Vertraulichkeitsstufe	Öffentlich
Freigegeben für	interessierte Parteien
Revisionsintervall	Jährlich
Nächste Revision	14.01.2026

Änderungen

Datum	Version	Autor	Beschreibung
16.11.2021	0.1	aknieper	Erste Version des Dokuments
17.11.2021	0.2	aknieper	Rohfassung zur Abstimmung erstellt
25.03.2022	0.3	sguhl	physische Sicherheit überarbeitet
19.07.2022	0.4	sguhl	Dokumententrennung: Leitlinie <> Richtlinie, grundlegende Überarbeitung
04.10.202	0.5	sguhl	Review zus. mit auraSec Consultants
02.11.2022	0.6	akusch	Review mit 2 Kommentaren und Änderungswünschen
04.11.2022	1.0	akusch	Freigabe mittels elektronischer Unterschrift
28.05.2023	1.1	sguhl	Dokumentenlenkung angepasst auf neues Format, Formulierung zu DSVGO Belastbarkeit der Systeme hinzugefügt
07.08.2023	1.2	sguhl	Anpassung Geltungs- und Anwendungsbereich
08.08.2023	2.0	akusch, mschmidt	Freigabe durch elektronische Unterschrift
05.02.2024	2.1	sguhl	Ergänzung Rollen und Verantwortung der Mitarbeiter und der IT-Administration hinzugefügt
07.02.2024	3.0	akusch, mschmidt	Freigabe durch elektronische Unterschrift
10.01.2025	3.1	sguhl	Weibliche Form von DSB entfernt, Aufgaben des ISB und IS-Team eingefügt
14.01.2025	4.0	akusch, mschmidt	Freigabe durch elektronische Unterschrift

Inhalt

1 Einleitung

1.1 Heutiges Gefährdungspotential für vertrauliche Daten

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

Die Forderungen nach einem ISMS bestehen aufgrund verschiedener Regelungen:

- Verpflichtung der avodaq AG zur Informationssicherheit;
- Gesetzliche Verpflichtung zum Schutz der personenbezogenen Daten auf der Basis der EU-DSGVO;
- Vertragliche Verpflichtungen gegenüber interessierten Parteien;
- Der Tatsache, dass die Folgen einer unangemessenen Informationssicherheit nicht auf die avodaq AG begrenzt bleiben, sondern Folgen für die Beteiligten, darunter die Mitarbeiter der Kunden, haben.

1.2 Risiken für Unternehmensdaten

Zum Schutz vertraulicher Daten werden angemessene Sicherheitsmechanismen eingesetzt. Ein unbefugter Zugriff auf diese Daten hätte neben den rechtlichen Konsequenzen einen erheblichen Image- und Vertrauensverlust zur Folge. Dennoch kann es zweckgebunden erforderlich sein, diese Daten nach Maßgabe entsprechender Regularien Anderen zugänglich zu machen oder zu übertragen.

Unternehmensdaten müssen vor unbefugten Zugriffen oder ungewollten Übertragungen geschützt werden. Die stetig wachsende Vernetzung mit externen Stellen (z.B. Finanzamt, Banken, Krankenversicherungen, Lieferanten, etc.) erhöht die Risiken auch für Unternehmensdaten.

2 Unternehmenspolitik

Als einer der führenden Anbieter von IT-Kommunikations- und Infrastrukturlösungen und Digital Business Partner unserer Kunden ist der Einsatz von moderner IT und Kommunikationstechnik wesentlich für die Aufgabenerfüllung der avodaq AG. Der Vorstand der avodaq AG sieht die Qualität, Innovation, Informationssicherheit und den Datenschutz als Verpflichtung für das gesamte Unternehmen.

Unser Handeln und unsere Prozesse werden maßgeblich von moderner IT-Technologie ermöglicht und unterstützt. Dazu zählen unsere interne Administration, das Projektmanagement und die technischen Projektarbeiten, die Softwareentwicklung sowie die interne und externe Kommunikation.

Unser strategisches Ziel ist es kontinuierlich Erträge für das Unternehmen zu erwirtschaften. Wir wollen unsere geschäftlichen Aktivitäten weiter ausbauen und wachstumsorientiert handeln, um unseren Kunden, Lieferanten und Mitarbeitern ein verlässlicher Partner zu sein. Voraussetzung hierfür ist die kontinuierliche Weiterentwicklung unserer Prozesse, Systeme und der Mitarbeiter.

Auf Basis der aufgeführten Forderungen und Verpflichtungen gelten die folgenden

Grundsätze:

- Wir sind weltoffen, neugierig, leidenschaftlich.
- Wir stehen für Qualität und Innovation in allen Bereichen.
- Technik ist unsere Leidenschaft. Lösungen, die im Arbeitsalltag funktionieren, und der Erfolg unserer Kunden sind unser Antrieb.
- Wir hören zu, bevor wir Antworten geben. Unsere Lösungen sind gut durchdacht und gut gemacht.
- Wir arbeiten uns intensiv in die Geschäftsmodelle unserer Kunden ein. Deshalb verstehen wir uns als Digital Business Partner.
- Unter Partner verstehen wir: gemeinsam mit unseren Kunden Lösungen entwickeln, mit denen sie produktiver am Markt agieren und besser für die Zukunft aufgestellt sind.
- Als echter Partner fühlen wir uns unseren Kunden immer persönlich verpflichtet. Hierzu zählen neben gesetzlichen und vertraglichen Anforderungen auch der Umgang mit Daten. Dabei berücksichtigen wir stets die Aufrechterhaltung der Verfügbarkeit, Vertraulichkeit und Integrität.
- In einem hochtechnologischen Umfeld vergessen wir nie, wofür wir all unser Wissen einsetzen: für Menschen.
- Unser Ziel: Digital Business Partner Nr. 1 für den führenden Mittelstand.
- Unser Weg: herausragende technische Kompetenz plus Consulting, Service und Innovationskraft – mit dieser Kombination schaffen wir einzigartige Mehrwerte für unsere Kunden.

Um dies zu gewährleisten, wird von der avodaq AG ein ISMS betrieben und kontinuierlich weiterentwickelt. Das ISMS soll dazu beitragen, die gesetzlichen Anforderungen des Datenschutzes umzusetzen.

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

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

Alle Mitarbeiterinnen und Mitarbeiter der avodaq AG sind aufgefordert, im Rahmen ihrer beruflichen Tätigkeit auf die Einhaltung der in dieser Leitlinie definierten Ziele hinzuwirken.

3 Normative Grundlage und Schutzziele

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

Unter Berücksichtigung der Anforderungen der DSGVO gemäß Art. 32 Abs. 1 lit. b) sowie der Anforderungen des BSIG ergeben sich folgende Schutzziele:

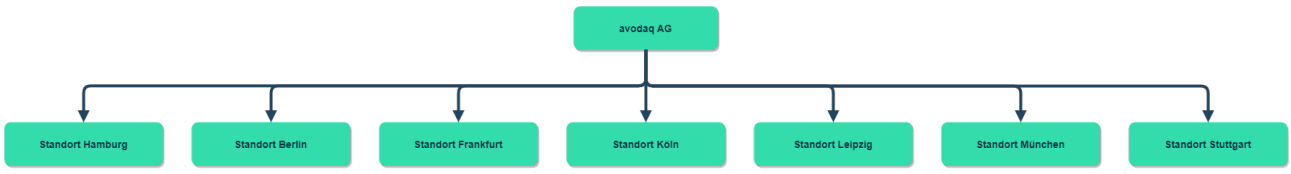
- Gewährleistung der Vertraulichkeit von schutzbedürftigen Daten
- Gewährleistung der Integrität aller relevanten Daten
- Gewährleistung der Verfügbarkeit von relevanten Prozessen und Systemen

Das ISMS trägt zudem der Forderung des Art. 32 DSVGO nach der Verbesserung der „Belastbarkeit der Systeme“ insofern Rechnung, als dass ein aktives Risikomanagement die Wirksamkeit der einzelnen Schutzmaßnahmen bezüglich Vertraulichkeit, Verfügbarkeit und Integrität kontinuierlich überwacht und verbessert. Wiederherstellungs- und Notfallkonzepte ermöglichen es uns, auch auf unvorhergesehene Ereignisse angemessen zu reagieren.

4 Anwendungsbereich

Der Anwendungsbereich des Informationssicherheits-Management-Systems der avodaq AG umfasst alle Prozesse, IT-basierten Dienste und den Betrieb von dazu genutzten IT-Systemen an allen Standorten mit allen Beschäftigten und Schnittstellen.

Die folgende Darstellung zeigt die Organisationsstruktur der avodaq AG.



5 Geltungsbereich

Das Informationssicherheitsmanagementsystem der avodaq AG bezieht sich auf die interne Administration, Projektdienstleistungen, Servicedienstleistungen, Entwicklung von Softwareprodukten und das Handels- und Liefergeschäft der Hard- und Software.

Das ISMS wird aus dem Firmensitz in München und der Niederlassung Hamburg heraus gesteuert und zertifiziert.

6 Verpflichtung von Geschäftsführung und Führungskräften

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

Der Vorstand legt hiermit die Informationssicherheitspolitik und die Informationssicherheitsziele fest. Er stellt sicher, dass die in dieser Leitlinie festgelegten Ziele und die Umsetzung des ISMS mit der strategischen Ausrichtung der Organisation vereinbar sind. Er bestimmt die erforderlichen Ressourcen für den Aufbau, die Umsetzung, die Aufrechterhaltung und die fortlaufende Verbesserung des Informationssicherheitsmanagementsystems und stellt diese bereit.

Mit Unterstützung aller Führungskräfte stellt der Vorstand sicher, dass die Anforderungen des ISMS in die Geschäftsprozesse der Organisation integriert werden. Der Vorstand und alle Führungskräfte sind dafür verantwortlich, die Bedeutung eines wirksamen Informationssicherheitsmanagements sowie die Wichtigkeit der Erfüllung der gesetzlichen und normativen Anforderungen zur Informationssicherheit und zum Datenschutz zu vermitteln. Mit Unterstützung des Informationssicherheitsbeauftragten (ISB), dem Datenschutzbeauftragten (DSB) sowie aller Führungskräfte stellt der Vorstand sicher, dass das ISMS die beabsichtigten Ergebnisse erzielt und der Datenschutz innerhalb der Organisation sichergestellt wird. Die Führungskräfte sind dafür verantwortlich, ihre Mitarbeiter und gegebenenfalls auch die Mitarbeiter von involvierten Dienstleistern anzuleiten und dabei zu unterstützen, zur Wirksamkeit des ISMS beizutragen und sicherzustellen, dass die gesetzlichen Anforderungen zum Datenschutz umgesetzt werden. Unternehmensleitungen und Führungskräfte wirken darauf hin, dass die fortlaufende Verbesserung der Informationssicherheit gefördert wird.

7 Rolle und Verantwortung der Mitarbeiter

Alle Mitarbeitenden der avodaq AG sind verpflichtet, die Vorgaben und Regelungen des ISMS anzuwenden und zu befolgen, um so ihren Beitrag zur Wirksamkeit des ISMS zu leisten. Im Einzelnen müssen alle Mitarbeitenden der avodaq AG:

- Die Richtlinien zum ISMS und Datenschutz kennen und befolgen
- An den verpflichtenden Schulungsmaßnahmen teilnehmen
- Informationssicherheitsvorfälle und Datenschutzpannen melden
- Erkannte Risiken für die Informationssicherheit und den Datenschutz melden
- IT -Systeme und Geräte gemäß den Richtlinien nutzen
- Andere Mitarbeitende für Informationssicherheit und Datenschutz sensibilisieren

8 Rolle und Verantwortung der IT-Administration

In der Verantwortung der IT-Administration liegen im Besonderen folgende Aufgaben, die in den entsprechenden Richtlinien näher beschrieben sind:

- Unterstützung aller Mitarbeiter bei der sicheren Nutzung der IT-Systeme.
- Wo technisch möglich, die Einhaltung von Vorgaben technisch erzwingen. (z.B. Passwort Policy, Rechtevergabe, Einsatz von Kryptografie)
- Jederzeit den sicheren Betrieb von IT-Systemen gewährleisten. (z.B. durch regelmäßiges Einspielen von Patches und Updates, Abändern von Default-Passwörtern, Installieren von Antivirusprogrammen)
- Durchführen von Datensicherungen und überprüfen der Wiederherstellbarkeit.
- Bei Fehlern in angemessener Zeit die Betriebsfähigkeit wieder herstellen.
- Für Administrationsaufgaben ausschließlich die dafür vorgesehenen Accounts mit den auf die jeweilige Rolle abgestimmten Zugriffsrechten zu benutzen.
- Für reguläre Bürotätigkeiten ausschließlich die normalen Benutzeraccounts, aber niemals die Administratoraccounts zu verwenden.
- Über nicht für sie bestimmte Informationen, von denen Administratoren im Rahmen ihrer Tätigkeit Kenntnis erlangen, haben sie absolutes Stillschweigen zu bewahren.

9 Sicherheitsstrategie

Bei der Planung und Umsetzung von Geschäftsprozessen werden die Vertraulichkeit, die Integrität, und die Authentizität der Daten sowie die Verfügbarkeit der Geschäftsprozesse und der dazu erforderlichen Systeme und Infrastruktur sichergestellt. Dabei muss gewährleistet werden, dass die getroffenen Maßnahmen in einem wirtschaftlich vertretbaren Verhältnis zum Schutzbedarf stehen.

Durch das Risikomanagement wird sichergestellt, dass Risiken identifiziert und mit angemessenem Aufwand durch geeignete und wirksame Maßnahmen reduziert werden. Dabei werden insbesondere folgende Kategorien von Gefährdungen berücksichtigt:

- Vorsätzliche Handlungen
- Menschliches Fehlverhalten
- Technisches Versagen
- Organisatorische Mängel
- Höhere Gewalt

10 Sicherheitsziele

Bei der Implementierung des Informationssicherheitsmanagementsystems verfolgt die avodaq AG folgende Sicherheitsziele:

- Verfügbarkeit der IT-Systeme mit tolerierbaren Ausfallzeiten und ohne wesentliche Auswirkungen auf den Geschäftsbetrieb
- Fehlfunktionen in IT-Systemen, die zum Verlust der Integrität führen, müssen auf ein Mindestmaß reduziert werden
- Anforderungen an die Vertraulichkeit müssen vor allem in Bezug auf die gesetzlichen und vertraglichen Anforderungen gewährleistet werden
- Für personenbezogene Daten der Mitarbeiter wird ein hoher Vertraulichkeitsschutz gewährleistet
- Risiken materieller und immaterieller Folgen für das Unternehmen durch Verstöße sollen systematisch reduziert werden
- Verspätete und fehlerhafte Managemententscheidungen müssen verhindert werden. Hierzu unterliegen Informationen zu Steuerungsdaten für wichtige Managemententscheidungen einem hohen Sicherheitsniveau in Bezug auf Verfügbarkeit und Integrität
- Kontinuierliche Reduktion der Risiken bei der Internet- und E-Mail-Nutzung, um die Bürokommunikation jederzeit aufrecht zu erhalten
- Bewusstsein der Verantwortung aller Beschäftigten im Umgang mit der IT und Unterstützung der Sicherheitsstrategie
- Kenntnis und Einhaltung aller Beschäftigten über einschlägige Gesetze (z.B. Strafgesetzbuch, DSGVO usw.) und vertragliche Regelungen
- Schutz der eigenen Betriebsgeheimnisse
- Erstellung und Auslieferung sicherer und integrer Softwareprodukte

11 Sicherheitsmaßnahmen

Für alle Verfahren, Informationen, IT-Anwendungen und IT-Systeme wird eine verantwortliche Person benannt, die den jeweiligen Schutzbedarf bestimmt und Zugriffsberechtigungen vergibt.

Für alle verantwortlichen Funktionen sind Vertretungen einzurichten. Es muss durch Unterweisungen und ausreichende Dokumentationen sichergestellt werden, dass Vertreter ihre Aufgaben erfüllen können.

Gebäude und Räumlichkeiten werden durch ausreichende Zutrittskontrollen geschützt. Der Zugang zu IT-Systemen wird durch angemessene Zugangskontrollen und der Zugriff auf die Daten durch ein restriktives Berechtigungskonzept geschützt.

Computer-Viren-Schutzprogramme werden auf allen IT-Systemen eingesetzt. Alle Internetzugänge werden durch eine geeignete Firewall gesichert. Alle Schutzprogramme werden so konfiguriert und administriert, dass sie einen effektiven Schutz darstellen und Manipulationen verhindert werden. Des Weiteren unterstützen die IT-Benutzer diese Sicherheitsmaßnahmen durch eine sicherheitsbewusste Arbeitsweise und informieren bei Auffälligkeiten die entsprechend festgelegten Stellen.

Datenverluste können nie vollkommen ausgeschlossen werden. Durch eine umfassende Datensicherung wird daher gewährleistet, dass der IT-Betrieb kurzfristig wiederaufgenommen werden kann, wenn Teile des operativen Datenbestandes verloren gehen oder offensichtlich fehlerhaft sind.

Um größere Schäden in Folge von Notfällen zu begrenzen bzw. diesen vorzubeugen, muss auf Sicherheitsvorfälle zügig und konsequent reagiert werden. Maßnahmen für den Notfall werden in einem separaten Notfallvorsorgekonzept zusammengestellt. Unser Ziel ist, auch bei einem Systemausfall kritische Geschäftsprozesse aufrecht zu erhalten und die Verfügbarkeit der ausgefallenen Systeme innerhalb einer tolerierbaren Zeitspanne wiederherzustellen.

IT-Benutzer nehmen regelmäßig an Schulungen zur korrekten Nutzung der IT-Dienste und den hiermit verbundenen Sicherheitsmaßnahmen teil. Der Vorstand bzw. die Personalabteilung unterstützen dabei die bedarfsgerechte Fort- und Weiterbildung.

Ausgehend von der ISO 27001 Methodik zur Einführung und Aufrechterhaltung eines Managementsystems für Informationssicherheit werden diverse weiterführende Regelungen geschaffen und verabschiedet, die dieses ISMS konkretisieren und gleichfalls gültig sind.

12 Organisation des Informationssicherheits- und Datenschutzmanagements

Zur Erreichung der Informationssicherheitsziele hat die avodaq AG eine Sicherheitsorganisation implementiert.

Der Informationssicherheitsbeauftragte (ISB) ist für alle Fragen zur Informationssicherheit bei avodaq zuständig. Der ISB ist organisatorisch unabhängig und hat dem Vorstand gegenüber unmittelbares Vortragsrecht. Er wird von allen Führungskräften bei der Erfüllung seiner Aufgaben unterstützt.

Die Hauptaufgaben des ISB sind:

- Aufbau, Betreuung und Weiterentwicklung eines ISMS (Informationssicherheitsmanagement-systems) gemäß ISO/IEC 27001
- Erstellung, Koordination und Genehmigung bereichsübergreifender Regelungen zum Informationssicherheitsmanagementsystem sowie Vorgaben für den Betrieb des ISMS
- Überwachung von Maßnahmen und relevanten Prozessen; Entscheidung bei Fragen der Informationssicherheit
- Überprüfung der Erreichung der Informationssicherheitsziele
- Bewertung von Sicherheitsaspekten in Projekten
- Durchführung interner und Koordinierung externer Audits zur Überprüfung der Wirksamkeit des ISMS
- Koordinierung der Durchführung sowie Auswertung der Risikoanalyse; Festlegen von Maßnahmen zur Risikobehandlung
- Unterstützung bei der Auswertung und Verfolgung von Sicherheitsvorfällen im Rahmen der Eskalation
- Verbesserung des Sicherheitsbewusstseins mittels Durchführung von (internen) Schulungen und Sicherheitsaudits und Beratung aller Abteilungen in Fragen der Informationssicherheit
- Beantwortung von Fragen zum ISMS, die seitens interessierter Dritter gestellt werden
- Erarbeitung von Vorschlägen zur Risikominimierung an den Vorstand
- Berichterstattung an den Vorstand
- Zusammenarbeit mit dem Datenschutzbeauftragten
- Leitung des Informationssicherheitsteams

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

Dem ISB und dem DSB werden die zur Erfüllung ihrer Aufgaben erforderlichen Ressourcen zur Verfügung gestellt. Dazu gehört die regelmäßige Teilnahme an Fortbildungsmaßnahmen, angemessene Unterstützung bei der Durchführung von internen Auditierungen sowie die Unterstützung bei der Ausübung ihres Weisungsrechts im Kontext der Informationssicherheit bzw. des Datenschutzes.

Aufgrund der Synergien im Informationssicherheits- und Datenschutzmanagement arbeiten ISB und DSB eng zusammen.

Der ISB und der DSB unterstützen alle Führungskräfte und Beschäftigten bei der Umsetzung der Regelungen zur Einhaltung der Informationssicherheit und der gesetzlichen Anforderungen zum Datenschutz bei der avodaq AG.

Das Risikomanagement stellt sowohl für den Datenschutz im Sinne der DSGVO als auch für das Informationssicherheitsmanagement auf der Basis der Norm ISO/IEC 27001 ein wichtiges Hilfsmittel dar. Das Risikomanagement der Organisation soll soweit möglich einheitlich erfolgen. Dabei muss den besonderen Anforderungen des Datenschutzes und der Informationssicherheit Rechnung getragen werden.

12.1 Informationssicherheitsteam

Neben dem ISB gibt es bei der avodaq AG ein Informationssicherheitsteam, das vom ISB geleitet wird. Das Team der Informationssicherheit ist ein Gremium, welches übergreifende Belange der Informationssicherheit (inklusive IT-Sicherheit) steuert und kontrolliert.

Insbesondere soll über folgende Angelegenheiten beraten werden:

- Allgemeine Themen der Informationssicherheit
- Beobachtungen, die Störungen im Betriebsablauf oder Sicherheitsrisiken verursachen
- Änderungen bzw. Neuerungen, die Auswirkungen auf die Ziele der Informationssicherheit der avodaq AG haben (z.B. durch Einführung, Erweiterung und Änderungen von IT-Systemen)
- Einsatz von Investitionen für die Umsetzung der Informationssicherheit
- Anfragen von Mitarbeitern, die Themen des Informationssicherheitsteams berühren

13 Einbindung von Informationssicherheit und Datenschutz innerhalb der Organisation

Der Informationssicherheitsbeauftragte muss frühzeitig in alle relevanten Projekte eingebunden werden, damit schon in der Planungsphase sicherheitsrelevante Aspekte berücksichtigt werden können. Sofern personenbezogene Daten betroffen sind, gilt gleiches für den Datenschutzbeauftragten.

Alle IT-Benutzer haben sich in sicherheitsrelevanten Fragestellungen an die Anweisungen des Informationssicherheitsbeauftragten zu halten.

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

14 Audits und Kontrollen

Informationssicherheit erfordert permanente Anstrengungen (Sicherheitsstrategie) und ist folglich keine einmalige Aktivität. Verlässliche Informationssysteme erfordern kontinuierliche Aufmerksamkeit. Nach der Implementierung wird kontrolliert, ob die Maßnahmen tatsächlich wie geplant durchgeführt werden (Kontrolle). Eine regelmäßige Evaluierung ist erforderlich, um festzustellen, ob die gewählten Maßnahmen noch ausreichen oder an welcher Stelle Anpassungen erforderlich sind.

Unter der Verantwortung des ISB werden in den einzelnen Betriebsteilen Kontrollen zu folgenden Punkten durchgeführt:

- Vorhandensein angemessener Sicherheitspläne und Notfallpläne;

- Beachtung der festgestellten Basisanforderungen und Implementierung der erforderlichen zusätzlichen Sicherheitsmaßnahmen;
- Engagement des Managements für die dauerhafte Wirkung der Maßnahmen, beispielsweise durch Ausführungen von Arbeitsplatz-Inspektionen, d.h. es ist die Einhaltung von Richtlinien zu überprüfen und auf Abweichungen hinzuweisen und darauf hinzuwirken, dass diese behoben werden.

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

15 Kontinuierliche Verbesserung

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

Durch eine kontinuierliche Revision der Regelungen und deren Einhaltung wird das angestrebte Sicherheits- und Datenschutzniveau sichergestellt. Abweichungen werden mit dem Ziel analysiert, die Sicherheitssituation zu verbessern und diese ständig auf dem aktuellen Stand der IT-Sicherheitstechnik und konform zu den jeweiligen gesetzlichen Regelungen und normativen Vorgaben zu halten.

16 Schlussbestimmungen

16.1 Folgen bei Zuwiderhandlung

Beabsichtigte oder grob fahrlässige Handlungen, die Sicherheitsvorgaben verletzen, können finanzielle Verluste bedeuten, Mitarbeiter, Geschäftspartner und Kunden schädigen oder dem Ruf des Unternehmens schaden. Bewusste Verstöße gegen verpflichtende Sicherheitsregeln können arbeitsrechtliche und unter Umständen auch strafrechtliche Konsequenzen haben und zu Regressforderungen führen.

17 Inkrafttreten

Diese Leitlinie tritt am Tag nach der Veröffentlichung in Kraft.

15.01.2025

DocuSigned by:
DA986EAFD5C7408...

14.01.2025

DocuSigned by:
5125B89C12D44D9...

DS

SMART IT FOR YOUR BUSINESS ESTD. 1997 www.avodaq.com 80687 München