Leitlinie zur Informationssicherheit

Mustervorlage zum Download

Klassifizierung:

Öffentlich

Anwendungsbereich:

<hier bitte den Anwendungsbereich dieses Dokuments angeben>

Version:

1.0

Dokumenten-ID	001
Dokumentenart	ISMS_LL
Dokumenteneigentümer:	Otto Normalverbraucher
Stand:	07.08.2025
Revisionszyklus:	jährlich
Status:	freigegeben
Zweck:	Die Leitlinie zur Informationssicherheit fasst die Leitaussagen zu Sicherheitsstrategien und die wesentlichen Rollen des Informationsmanagementsystems für den Anwendungsbereich zusammen. Zudem beschreibt diese Leitlinie zur Informationssicherheit den Stellenwert, die Bedeutung und die Ziele der Informationssicherheit für den Anwendungsbereich. Die Leitlinie zur Informationssicherheit enthält Verpflichtungserklärungen zur Umsetzung der Inhalte sowie zur kontinuierlichen Verbesserung. Diese Leitlinie zur Informationssicherheit tritt mit Bekanntmachung durch das Top-Management der [MANDANT] in Kraft.

Verteilerliste

Empfänger	Funktion im Projekt	Unternehmen

Top-Management, Führungskräfte und alle Mitarbeiter, die sicherheitsrelevante Aufgaben innerhalb des Anwendungsbereichs der Leitlinie zur Informationssicherheit ausführen.

Änderungshistorie

Version	Datum	Autor	Änderungsvermerk
0.1	TT.MM.YYYY	Max Mustermann	Initiale Erstellung

Freigaben

Version	Datum	Freigebender (Funktion)	Vermerk zur Freigabe
1.0	TT.MM.YYYY	Otto Normalverbraucher (Geschäftsführung)	Freigabe der Version 0.1

Inhalt

1 Zweck und Anwendungsbereich 3
1.1 Erklärung der Unternehmensleitung 3
1.2 Anwendungsbereich 3
2 Stellenwert der Informationsverarbeitung 4
3 Sicherheitsziele 4
4 Relevante Sicherheitsvorgaben 6
4.1 Gesetzliche Vorgaben 6
4.2 Vertragliche Vorgaben 6
4.3 Interne Vorgaben 6
5 Sicherheitsorganisation und Ressourcen 7
6 Umgang mit Informationssicherheitsrisiken 8
7 Mitwirkungspflichten 9
8 Durchsetzung 9
9 Kontinuierliche Verbesserung 9
10 Bekanntmachung 10
11 Gültigkeit 10

1 Zweck und Anwendungsbereich

1.1 Erklärung der Unternehmensleitung

Beschreiben Sie hier, wie Ihre Unternehmensleitung als ein wichtiger Faktor für den Erfolg der Informationssicherheit beiträgt.
Hinweis: Die nachfolgenden Beispiele dienen als einen möglichen Einstieg und müssen an die spezifische Situation Ihres Unternehmens angepasst und ausgebaut werden.

Beispiel:
Als Unternehmensleitung der [MANDANT] betrachten wir Informationssicherheit als entscheidenden Faktor für den Erfolg unseres Geschäftsbetriebs und der Innovationsfähigkeit bei der [MANDANT]. Sie spielt auch eine wichtige Rolle im Vertrauen in unsere Arbeit durch unsere Mitarbeitenden, Mitglieder und Partner der Selbstverwaltung.
Informationssicherheit geht über rein technische Anforderungen hinaus und ist daher auch ein wesentlicher Bestandteil unserer Geschäftsstrategie. Diese Leitlinie spiegelt den Willen und das Engagement des Vorstands wider, indem sie klare Ziele und Verantwortlichkeiten festlegt, um diese Geschäftsziele zu erreichen.
Es ist der Anspruch der Unternehmensleitung, notwendige Ressourcen zur Verfügung zu stellen, angemessene Prozesse zu implementieren und eine Kultur zu fördern, in der Informationssicherheit als gemeinschaftliche Verantwortung verstanden und aktiv umgesetzt wird.

1.2 Anwendungsbereich

Beschreiben Sie hier, welche organisatorischen Einheiten, Standorte, Prozesse, Systeme und externen Dienstleister vom ISMS erfasst werden. Der Anwendungsbereich sollte alle relevanten Ressourcen umfassen, die einen Einfluss auf die Informationssicherheit im Unternehmen haben – einschließlich IT-Systeme, Netzwerke, Anwendungen, Informationen (digital und analog) sowie räumliche Infrastruktur. Berücksichtigen Sie dabei auch Leistungen von Unterauftragnehmern, sofern diese sicherheitsrelevant sind.

Beispiel:
Das Informationssicherheitsmanagementsystem („ISMS“) gilt für den gesamten Geschäftsbetrieb der [MANDANT] (im Folgenden als „ISMS-Anwendungsbereich“ bezeichnet).
Das ISMS umfasst alle Ressourcen, die für die Informationssicherheit relevant sind, einschließlich Prozesse, analoger und digitaler Informationen, IT-Anwendungen, IT-Systeme, Netzwerke, Räume und Gebäude, die für den Geschäftsbetrieb der [MANDANT] von Bedeutung sind. Dies schließt auch die Leistungen ein, die von Unterauftragnehmern erbracht werden.

2 Stellenwert der Informationsverarbeitung

Beschreiben Sie hier, welche Bedeutung Informationssicherheit für Ihr Unternehmen hat. Insbesondere im Hinblick auf Digitalisierung, Schutz sensibler Daten, betriebliche Kontinuität und Vertrauen bei Kunden, Partnern oder der Öffentlichkeit. Gehen Sie darauf ein, welche Risiken (z. B. Cyberangriffe, Datenschutzverstöße) für Ihr Geschäft besonders relevant sind und welche Schutzbedarfe sich daraus ergeben. Benennen Sie gegebenenfalls auch Ihre zentralen Schutzziele.

Beispiel:
Die voranschreitende Entwicklung der Informationstechnologie führt dazu, dass Geschäftsprozesse, Kommunikation und Dokumentation zunehmend digitalisiert werden. Für die [MANDANT] ergibt sich die hohe Bedeutung der Informationssicherheit vor allem aus der Notwendigkeit, im Zuge dieser Digitalisierung die Dienstleistungen verfügbar zu halten und vertrauliche Daten sicher zu verarbeiten.

Um das Vertrauen unserer Mitglieder, Partner in der Selbstverwaltung und der Öffentlichkeit zu bewahren, ist es von entscheidender Bedeutung, Informationen und Daten vor unbefugtem Zugriff und Manipulation zu schützen. Es ist erforderlich, angemessene Maßnahmen zu ergreifen, um der wachsenden Bedrohung durch Cyberkriminalität entgegenzuwirken.
In diesem Zusammenhang ist es wichtig sicherzustellen, dass Informationen und Daten ausreichend geschützt werden, um wirtschaftliche Schäden zu verhindern und negative Auswirkungen auf das Ansehen von [MANDANT] zu vermeiden. Die Schutzziele der Informationssicherheit, nämlich "Vertraulichkeit", "Verfügbarkeit", "Integrität" und "Authentizität", müssen angemessen umgesetzt werden.

3 Sicherheitsziele

Beschreiben Sie hier, welche übergeordneten Ziele Ihre Organisation mit dem ISMS verfolgt. Gehen Sie darauf ein, wie das ISMS zur Absicherung von Geschäftsprozessen, zum Schutz sensibler Informationen und zur Erfüllung gesetzlicher Anforderungen beiträgt.
Benennen Sie Ihre konkreten Schutzziele und erläutern Sie, wie diese im Unternehmen umgesetzt werden sollen.
Erläutern Sie außerdem, wie das ISMS in Ihre Unternehmensstrategie eingebettet ist und welche Maßnahmen Sie zur kontinuierlichen Verbesserung und Wirksamkeitssicherung (z. B. Schulungen, technische Maßnahmen, Audits) vorgesehen haben.

Beispiel:
Unser Hauptziel besteht darin, ein angemessenes und an die Größe unseres Geschäftsbetriebs angepasstes Informationssicherheitsmanagementsystem (ISMS) zu implementieren. Dieses ISMS soll sicherstellen, dass die Informationssicherheit in unserer Organisation kontinuierlich gewährleistet und verbessert wird. Dabei werden Risiken identifiziert, bewertet und angemessen behandelt, Sicherheitsrichtlinien eingeführt, Mitarbeiter geschult, technische Sicherheitsmaßnahmen umgesetzt und regelmäßige Überprüfungen und Audits durchgeführt, um Nichtkonformitäten aufzudecken und zu behandeln. Dies gewährleistet, dass die Informationssicherheit stets auf dem neuesten Stand ist und den mit den sich wandelnden Bedrohungen standhalten kann. Das ISMS adressiert die folgenden grundlegenden Sicherheitsziele:

1. Verfügbarkeit: Gewährleistung kontinuierlicher und zuverlässiger Verfügbarkeit von Dienstleistungen, Informationen und Systemen, um deren Nutzung bei Bedarf sicherzustellen. Dies erfordert Maßnahmen zur Verhinderung von Ausfällen, Wartung und Wiederherstellung im Falle eines Zwischenfalls, wobei auf sichere Prozesse, Arbeitsmittel, Software-Produkte und Unterauftragnehmer zurückgegriffen wird.

2. Vertraulichkeit: Angemessene Vertraulichkeit unserer Informationen wird sichergestellt, indem wir unautorisierten Zugriff verhindern, insbesondere durch die Anwendung des Prinzips der geringsten Berechtigungen ('Need-to-Know'). Dies gewährleistet, dass Informationen nur für autorisierte Personen oder Systeme zugänglich sind, die einen legitimen Bedarf für den Zugriff nachweisen können.

3. Integrität: Die Integrität hat zum Ziel, die Manipulationssicherheit von Informationen sowie die ordnungsgemäße Funktionsweise von Systemen sicherzustellen, indem unbefugter Zugriff und Manipulation verhindert werden. Regelmäßige Tests und Überprüfungen stellen sicher, dass die Informationen und Systeme korrekt und zuverlässig sind.

4. Authentizität: Das Schutzziel der Authentizität stellt sicher, dass die Identität von Personen oder Systemen in jeder Interaktion oder Transaktion verifiziert und bestätigt wird. Dies gewährleistet eine sichere Authentifizierung und ermöglicht den Zugriff auf geschützte Ressourcen nur für autorisierte und verifizierte Nutzer, um unbefugten oder gefälschten Zugriff auf sensible Daten oder Systeme zu verhindern.

Das ISMS ist so auszurichten, dass es nahtlos in die Geschäftsziele und -strategien der Organisation integriert ist. Dies bedeutet, dass die Informationssicherheit als integraler Bestandteil der Unternehmensführung betrachtet wird.

Ein weiteres wichtiges Ziel des ISMS ist die kontinuierliche Verbesserung der Informationssicherheit in der Organisation. Dies wird durch die Identifizierung, Bewertung und angemessene Behandlung von Risiken erreicht, um potenzielle Sicherheitslücken zu minimieren und die Informationssicherheit zu erhöhen.

Um diese Ziele zu erreichen, wurden klare Vorgaben festgelegt. Dazu gehört die Einführung von Sicherheitsrichtlinien und -verfahren, die Schulung der Mitarbeiter in sicherheitsrelevanten Themen sowie die Implementierung technischer Sicherheitsmaßnahmen wie Firewall-Konfigurationen und Software-Patches.

Zusätzlich sind regelmäßige Überprüfungen und Audits durchzuführen, um sicherzustellen, dass die Sicherheitsziele erreicht und aufrechterhalten werden. Die Sicherheitsorganisation des ISMS überwacht auch die Einhaltung interner Richtlinien sowie externer rechtlicher und vertraglicher Vorgaben und hat klare Prozesse etabliert, um Regelverstöße angemessen zu behandeln und daraus zu lernen.

Insgesamt zielen die Vorgaben und Ziele des ISMS darauf ab, die Informationssicherheit in der Organisation zu stärken und sicherzustellen, dass die Informationen und Systeme vor Bedrohungen geschützt sind.

4 Relevante Sicherheitsvorgaben

Innerhalb des Anwendungsbereichs sind die folgenden Quellen für Vorgaben zu berücksichtigen:

4.1 Gesetzliche Vorgaben

Ziel ist es, die für die Informationssicherheit und für den Datenschutz relevanten, gesetzlichen Vorgaben zu identifizieren und ihre konsequente Umsetzung verbindlich zu regeln und sicherzustellen.

4.2 Vertragliche Vorgaben

Beschreiben Sie hier, wie Ihr Unternehmen sicherstellt, dass auch externe Partner und Dienstleister die Anforderungen an die Informationssicherheit einhalten. Legen Sie dar, welche sicherheitsrelevanten Themen vertraglich geregelt werden. Gehen Sie auch darauf ein, wie Schutzbedarf und Risiken dabei berücksichtigt werden.

Beispiel:

Mit Unterauftragnehmern muss die Umsetzung von Vorgaben an die Informationssicherheit verbindlich geregelt sein, um das erforderliche Sicherheitsniveau aufrechtzuerhalten und um etwaige Rechtsstreitigkeiten vorzubeugen.

Dazu gehört das Festlegen von Vorgaben hinsichtlich folgender Themenschwerpunkte:

- Informationssicherheits-Managementsystem und zugehörende Prozesse
- Asset-Management
- Zugriffsschutz und Berechtigungsvergabe
- Physische Sicherheit und Zutrittsschutz
- Operationelle Vorgaben an die Informationssicherheit (Netzwerksicherheit, Virenschutz, Logging & Monitoring, Backup & Restore etc.)
- Sicherheit in der Softwareentwicklung und IT-Änderungsprozessen
- Securtiy-Incident-Management
- Sicherheit bei Unterauftragnehmern bzw. bei ausgelagerten Prozessen

Die Ausgestaltung der Regelungen sollte dem Schutzbedarf und dem Risiko des Vertragsgegenstandes entsprechen.

4.3 Interne Vorgaben

Beschreiben Sie hier, wie Ihre internen Sicherheitsvorgaben in Prozesse, Systeme und Dienstleister integriert werden. Erläutern Sie, wie Verantwortlichkeiten geregelt, Maßnahmen wirtschaftlich bewertet und regelmäßig überprüft werden.

Beispiel:
Die internen Vorgaben zur Informationssicherheit müssen in die Prozesse, IT-Anwendungen, IT-Systemen und Unterauftragnehmern des Anwendungsbereichs integriert werden.

Alle Sicherheitsmaßnahmen müssen im Einklang mit den Geschäfts- und Sicherheitszielen der [MANDANT] stehen und dabei Folgendes sicherstellen:

- Transparente und eindeutige Verantwortungen durch die Definition von Risikoeignern zu den Geschäftsprozessen.
- Regelmäßige Überprüfung, um Effizienz, Effektivität sowie Angemessenheit der Risikobehandlung sicherzustellen.
- Wirtschaftlich vertretbare Umsetzung, im Verhältnis zum möglichen Schaden, indem Sicherheitsmaßnahmen nach dem Proportionalitätsprinzip bewertet werden.

Alle im Anwendungsbereich tätigen Beschäftigten sind dazu verpflichtet, die für sie relevanten internen Vorschriften konsequent einzuhalten.

5 Sicherheitsorganisation und Ressourcen

Beschreiben Sie hier, wie das Top-Management die Verantwortung für das ISMS wahrnimmt, z. B. durch Ressourcenbereitstellung, Rollenverteilung und Delegation an den ISB. Gehen Sie auf Aufbau, Zuständigkeiten, Vertretungsregelungen und Qualifikationsanforderungen der Sicherheitsorganisation ein.

Beispiel:
Das Top-Management der [MANDANT] trägt die Verantwortung dafür, dass im Anwendungsbereich ein ISMS gemäß dieser Leitlinie etabliert und fortlaufend weiterentwickelt wird. Hierfür werden durch das Top-Management alle notwendigen zeitlichen, finanziellen und personellen Ressourcen zur Verfügung gestellt.

Es ist erforderlich, eine Informationssicherheitsorganisation für den Betrieb des ISMS einzurichten und diese entsprechend zu dokumentieren. Zudem sind klare Verantwortlichkeiten für die Schutzbedarfseinstufungen und den sicheren Umgang mit allen betrachteten Prozessen, verarbeiteten Informationen, IT-Anwendungen und Informations- und Kommunikationssystemen im Anwendungsbereich festzulegen.

Bei der Auswahl von Sicherheitsmaßnahmen ist es wichtig, die jeweilige Risikosituation zu berücksichtigen und auch Kosten-Nutzen-Aspekte sowie die Praxistauglichkeit der Sicherheitsmaßnahmen in Betracht zu ziehen.

Die Verantwortlichen sind für die Erfüllung ihrer Aufgaben regelmäßig weiterzubilden. Für die verpflichteten Funktionen sind Vertretungen einzurichten, so dass eine konsequente Einhaltung der eigenen Vorgaben gewährleistet wird. Eine ausreichende Dokumentation aller bestehenden Vorgaben und Regelungen ist sicherzustellen.

Die operative Verantwortung für die Einrichtung, Koordination, Steuerung und Weiterentwicklung des ISMS wird vom Top-management auf den Informationssicherheitsbeauftragten (ISB) delegiert. Das Top-management verpflichtet sich selbst und fordert alle Führungskräfte und Mitarbeiter dazu auf, den ISB ausreichend zu unterstützen und frühzeitig in alle sicherheitsrelevanten Projekte im Anwendungsbereich einzubeziehen, um Sicherheitsaspekte bereits in der Planungsphase angemessen zu berücksichtigen.

6 Umgang mit Informationssicherheitsrisiken

Beschreiben Sie hier, wie Informationswerte identifiziert, Risiken bewertet und geeignete Maßnahmen in Ihrem Unternehmen abgeleitet werden. Erläutern Sie, wer für die Schutzobjekte verantwortlich ist und wie Maßnahmen ausgewählt werden (z. B. nach Wirksamkeit, Praxistauglichkeit, Wirtschaftlichkeit). Gehen Sie auch darauf ein, wie Risiken gemeldet, dokumentiert und vom Top-Management freigegeben werden.

Beispiel:

Um sicherzustellen, dass die Geschäfts- und Sicherheitsziele der [MANDANT] angemessen in den Betrieb und die Definition von Sicherheitsmaßnahmen integriert werden, ist ein dem Stand der Technik entsprechendes Informationssicherheits- und Risikomanagement zu betreiben. Es sind die möglichen Sicherheitsrisiken zu den Informationswerten zu identifizieren, zu bewerten und gegebenenfalls den relevanten Parteien zu kommunizieren.

Es ist erforderlich, für alle schützenswerten Ressourcen (nachfolgend als "Schutzobjekte" bezeichnet) fachliche und technische Verantwortliche zu benennen, die für den Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Authentizität dieser Schutzobjekte verantwortlich sind.

Basierend auf den Risikobewertungen sind angemessene Sicherheitsmaßnahmen zur Behandlung der Informationsrisiken umzusetzen. Angemessen bedeutet hierbei:

- wirksam (effektiv): Sie müssen vor den möglichen Gefährdungen wirksam schützen, also ein angemessenes Schutzniveau realisieren.
- geeignet: Sie müssen in der Praxis umsetzbar sein, dürfen also z. B. nicht die Organisationsabläufe zu stark behindern oder andere Sicherheitsmaßnahmen aushebeln.
- praktikabel: Sie sollen leicht verständlich, einfach anzuwenden und wenig fehleranfällig sein.
- wirtschaftlich: Die Sicherheitsmaßnahmen sollten einerseits das Risiko bestmöglich minimieren und andererseits in geeignetem Verhältnis zu den zu schützenden Werten stehen.
- konform: Sie müssen für alle Benutzer anwendbar (barrierefrei) sein und dürfen niemanden diskriminieren oder beeinträchtigen.

Alle möglichen Informationssicherheitsrisiken sind dem ISB zu melden. Der Risikobehandlungsplan ist durch das Top-Management zu genehmigen.

Die fachlich Verantwortlichen für die Schutzobjekte haben die Aufgabe sicherzustellen, dass die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen gemäß dem Risikobehandlungsplan angemessen umgesetzt werden.

7 Mitwirkungspflichten

Beschreiben Sie hier, wie alle Beschäftigten zur Umsetzung der Informationssicherheitsstrategie beitragen. Gehen Sie darauf ein, welche Verantwortung sie im Umgang mit Informationen und IT-Systemen tragen und wie das Sicherheitsbewusstsein gefördert wird.

Beispiel:

Es ist von großer Bedeutung, dass alle Mitarbeitenden sich ihrer Verantwortung im Umgang mit Informationen, IT-Anwendungen und Informations- sowie Kommunikationssystemen (IKT) bewusst sind. Sie sind angehalten die Sicherheitsstrategie aktiv zu unterstützen und zur Umsetzung dieser Leitlinie beizutragen, indem sie sich nach besten Kräften für die Informationssicherheit einsetzen.

8 Durchsetzung

Beschreiben Sie hier, wie mit Verstößen gegen die Leitlinie zur Informationssicherheit umgegangen wird. Gehen Sie auf mögliche arbeitsrechtliche, zivilrechtliche oder strafrechtliche Konsequenzen ein. Nennen Sie Beispiele für relevante Verstöße, etwa Missachtung interner Regelungen, Datenmissbrauch oder Reputationsschäden.

Beispiel:

Vorsätzliche oder [grob] fahrlässige Handlungen gegen die Leitlinie zur Informationssicherheit und die daraus resultierenden Regelungen werden als Verstöße betrachtet.
Verstöße können zu arbeitsrechtlichen Konsequenzen führen. Bei schweren Verstößen sind zivilrechtliche oder sogar strafrechtliche Folgen möglich. Verstöße können zu Regressforderungen führen.

Verstöße sind zum Beispiel:

- Verstöße gegen bestehende Gesetze, Verordnungen oder interne Regelungen,
- Zufügen von tatsächlichen oder potenziellen Vermögensschäden bei der [MANDANT] oder deren Mitglieder und Partner in der Selbstverwaltung,
- Schädigung der Reputation der [MANDANT], von Beschäftigten oder Mitglieder und Partner in der Selbstverwaltung oder
- Das Ermöglichen von unberechtigtem Zugriff auf Informationen oder Daten und deren Missbrauch.

9 Kontinuierliche Verbesserung

Beschreiben Sie, wie die Wirksamkeit des ISMS regelmäßig überprüft und weiterentwickelt wird. Erläutern Sie, wie der ISB über den Stand der Informationssicherheit berichtet, wie Abweichungen behandelt werden und in welchem Turnus das Top-Management das ISMS bewertet und neue Zielvorgaben festlegt.

Beispiel:
Der ISB ist für die Bereitstellung zur Erfüllung der generellen ISMS-Zielvorgaben zuständig und wird dem Top-Management regelmäßig, mindesten vierteljährlich in einem Management-Bericht zum Nachweis der Angemessenheit, Eignung und Wirksamkeit des ISMS bereitstellen. Durch die regelmäßige Revision der Regelungen und deren Einhaltung wird das angestrebte Informationssicherheitsniveau konstant sichergestellt. Alle festgestellten Abweichungen sind umgehend zu beheben und haben zur Verbesserung und zur Erhaltung des aktuellen Stands des ISMS beizutragen.

Das Top-Management sichert dem ISB seine ständige Unterstützung zur Aufrechterhaltung sowie erforderlich zur Verbesserung des Informationssicherheitsniveaus zu. Zudem wird das Top-Management das ISMS regelmäßig, mindestens jährlich, auf dessen Aktualität und Wirksamkeit hin bewerten, um die Einhaltung der Zielvorgaben dieser Leitlinie zu überprüfen. Bei Bedarf werden neue Zielvorgaben durch das Top-Management, in Abstimmung mit dem ISB festlegt.

10 Bekanntmachung

Beschreiben Sie hier, wie die Inhalte der Leitlinie allen Mitarbeitenden verbindlich kommuniziert werden. Erläutern Sie, wie relevante externe Parteien informiert werden und wie sichergestellt wird, dass alle Beteiligten den Anwendungsbereich und die Anforderungen kennen. Alternativ kann auf vertragliche Regelungen mit externen Dienstleistern verwiesen werden.

Beispiel:
Die Inhalte der Leitlinie zur Informationssicherheit müssen allen Mitarbeitenden verbindlich bekannt gemacht werden, und es muss auf die Einhaltung dieser Leitlinie hingewiesen werden. Zusätzlich müssen die wesentlichen Inhalte dieser Leitlinie nachweisbar an relevante externe Parteien weitergegeben werden, sofern diese an der Verarbeitung von Informationen im Anwendungsbereich beteiligt sind.

Es ist von entscheidender Bedeutung, dass jeder Mitarbeitende sowie alle mit Sicherheitsaufgaben betrauten Dienstleister den Anwendungsbereich dieser Leitlinie zur Informationssicherheit verstehen und die darin enthaltenen Inhalte kennen. Alternativ können Verträge abgeschlossen werden, die vergleichbare Sicherheitsanforderungen regeln.

11 Gültigkeit

Beschreiben Sie, wie häufig die Leitlinie überprüft wird, z. B. mindestens jährlich und wer dafür verantwortlich ist. Gehen Sie darauf ein, welche Anlässe für eine Aktualisierung relevant sind (z. B. rechtliche Änderungen, neue Geschäftsziele, geänderte Verantwortlichkeiten).

Beispiel:
Die Leitlinie zur Informationssicherheit ist durch das Top-Management in Zusammenarbeit mit dem Informationssicherheitsbeauftragten regelmäßig, mindestens jährlich, auf ihre Aktualität hin zu überprüfen. Dabei werden u.a. Änderungen in den gesetzlichen Vorgaben bzw. Geschäftszielen und -strategien sowie Verantwortlichkeiten berücksichtigt.