|  |  |
| --- | --- |
| Version: | 1.0 |
| Status: | Freigegeben |
| Dokumentenklassifizierung: | intern |

Leitlinie zur Informationssicherheit

1. Januar 2020

Allgemeine Informationen zum vorliegenden Dokument

|  |  |  |
| --- | --- | --- |
| Bezeichnung | Inhalt | Bearbeitungshinweis |
| Eigentümer |  | [verantwortlich für die Erstellung und Pflege des Dokuments = Abteilungsleitung] |
| Autor |  | [operative Verantwortung für das Dokument] |
| Status | Freigegeben | [Einstufung des aktuellen Dokumentenstatus <Entwurf, Finaler Entwurf, Final/Freigegeben>] |
| Klassifizierung | intern | [Einstufung der Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS100001 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Leitlinie zur Informationssicherheit | [Bezeichnung des Dokuments wie auf dem Titelblatt beschrieben.] |
| Version  | 1.0 | [zweistellige Versionsnummer] |
| Veröffentlichungsform | digital | [Veröffentlichungsform Papier, digital] |
| Speicherort |  | [Ablageort des Dokumentes] |
| Freigabe am | <TT.MM.YYYY> | [Datum der Freigabe durch den Eigentümer] |
| Freigabe bis | <TT.MM.YYYY> | [Datum der Freigabe bis durch den Eigentümer] |
| Revisionszyklus | Alle zwei Jahre | [Revisionszyklus alle 1, 2 Jahre] |
| Archivierungszeitraum | 10 Jahre | [Archivierungszeitraum nach Ablauf 5, 10 Jahre] |

# Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Beschreibung | Autor | Datum |
| 0.1 | initiale Erstellung |  |  |
| 0.2 – 0.8 | draft |  |  |
| 0.9 | final draft |  |  |
| 1.0 | final/freigegeben |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhaltsverzeichnis

[Allgemeine Informationen zum vorliegenden Dokument 2](#_Toc74995247)

[Dokumentenhistorie 3](#_Toc74995248)

[Inhaltsverzeichnis 4](#_Toc74995249)

[Allgemeine Festlegungen 5](#_Toc74995250)

[Stellenwert der Informationssicherheit 5](#_Toc74995251)

[Ziel der Informationssicherheit 5](#_Toc74995252)

[Sicherheitsstrategie 5](#_Toc74995253)

[Geltungsbereich und Zuständigkeiten 6](#_Toc74995254)

[Genehmigungs- und Änderungsverfahren 6](#_Toc74995255)

[Gesamtverantwortung für das Informationssicherheitsmanagement 6](#_Toc74995256)

[Rollen und Gremien 7](#_Toc74995257)

[<Informationssicherheitsbeauftragten> 7](#_Toc74995258)

[<Datenschutzbeauftragter> 7](#_Toc74995259)

[<Informationssicherheitsteam> 8](#_Toc74995260)

[Regelungsstruktur 8](#_Toc74995261)

[Verstöße und Sanktionen 8](#_Toc74995262)

# Allgemeine Festlegungen

## Stellenwert der Informationssicherheit

Für die <Institution> nimmt die Informationsverarbeitung in Zeiten der Digitalisierung aller Geschäftsprozesse eine Schlüsselrolle ein. Alle wesentlichen strategischen und operativen Funktionen und Aufgaben werden durch Informationstechnik maßgeblich unterstützt.

Über die gesetzlichen und vertraglichen Anforderungen hinaus besteht eine besondere Vertrauensstellung, Erwartungshaltung und Vorbildfunktion, da teilweise Informationen mit erhöhtem Schutzbedarf erhoben, verarbeitet und gespeichert werden. Sicherheitsvorfälle können daher zu einem erheblichen Schaden bei Mitarbeitenden, Kunden, Partnern oder Dritten führen und sich dadurch auch nachhaltig auf das allgemeine Vertrauen in die <Institution> auswirken.

## Ziel der Informationssicherheit

Basierend auf dem Tätigkeitsbereich sind die Informationssicherheitsziele der <Institution> der Schutz der Verfügbarkeit, Vertraulichkeit und Integrität der anvertrauten sowie eigenen Daten und Informationen. Darüber hinaus werden die gesetzlichen, vertraglichen und aufsichtsrechtlichen Vorgaben gewährleistet.

Als weiteres Sicherheitsziel gilt die Aufrechterhaltung des Geschäftsbetriebs durch die Gewährleistung von angemessenen Wiederanlauf- und Wiederherstellungszeiten im Rahmen des Notfallmanagement.

Die Ziele der Informationssicherheit sind angemessen sicherzustellen. Angemessenheit meint hierbei die Berücksichtigung des jeweiligen Schutzbedarfs und die Beachtung der Sparsamkeit und Wirtschaftlichkeit bei der Implementierung von Sicherheitsmaßnahmen. Diese sollten in einem haushälterisch vertretbaren Verhältnis zu materiellen und immateriellen Schäden stehen, die durch die Verletzung der Ziele verursacht werden könnten.

## Sicherheitsstrategie

Um den regulatorischen und gesetzlichen Anforderungen gerecht zu werden, entwickelt die <Institution> ein ISO 27001 kompatibles Informationssicherheitsmanagementsystem (ISMS) auf Basis des BSI- Standards 200-1 „Managementsysteme für Informationssicherheit (ISMS)“ und unter Anwendung der BSI Standards 200-2 „IT-Grundschutz-Methodik“ und 200-3 „Risikomanagement“. Mit der Einführung vom ISMS soll den sich dynamisch ändernden gesetzlichen Vorschriften, technischen Innovationen, regulatorischen Vorgaben und Marktbedingungen entsprochen werden.

Bezogen auf alle Verwaltungsprozesse lassen sich allgemein verbindlich nachfolgende Leitziele für das ISMS festschreiben:

* Hohe Verlässlichkeit des Handelns
* Reduzierung des Haftungsrisikos der verantwortlichen Führungskräfte sowie aller Mitarbeitenden
* Reduzierung der im Schadensfall entstehenden Kosten
* Beitrag zur Sicherung der Geschäftskontinuität und damit des Erfolgs von der <Institution>
* Zuverlässige Unterstützung und Sicherstellung der Kontinuität der digitalisierten Arbeitsabläufe
* Sicherheits- und Kontrollumfang der IT-Systeme sind am jeweiligen Verfahrens- bzw. IT-Servicerisiko ausgerichtet
* Sensibilisierung und Stärkung des Sicherheitsbewusstseins bei allen Mitarbeitenden in Abhängigkeit ihrer Rolle und Verantwortlichkeit

## Geltungsbereich und Zuständigkeiten

Die Leitlinie zur Informationssicherheit und die daraus abgeleiteten Dokumente gelten für die <Institution>. Sie sind für jeden, der bei oder mit der <Institution> arbeitet (Mitarbeitende, Vertragspartner, Berater oder Zulieferer, etc.), verpflichtend. Die Einhaltung der dort aufgeführten Vorgaben durch Dritte ist durch interne Mitarbeitende sicherzustellen. Die Leitlinie zur Informationssicherheit gilt nicht nur für die elektronisch verarbeiteten und gespeicherten Daten, sondern auch für in Papierform vorliegende Informationen.

Durch eine interne Veröffentlichung der Leitlinie zur Informationssicherheit wird sichergestellt, dass die aktuell gültige Version allen Mitarbeitenden der <Institution> zur Verfügung steht. Es wird erwartet, dass jeder Mitarbeitende diese Leitlinie zur Informationssicherheit und die daraus abgeleiteten Standards und Sicherheitsrichtlinien beachtet. Jegliche Ausnahmen sind zu begründen, zu dokumentieren und bedürfen der expliziten Zustimmung durch den <Informationssicherheitsbeauftragter>. Sofern personenbezogene Daten betroffen sind, ist zusätzlich eine Zustimmung des <Datenschutzbeauftragter> erforderlich.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Leitlinie zur Informationssicherheit“ wird durch die Geschäftsführung verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragten>. Änderungen werden ausschließlich von dieser Person vorgenommen. Eine Genehmigung und Freigabe erfolgt durch die Geschäftsführung.

# Gesamtverantwortung für das Informationssicherheitsmanagement

Die Gesamtverantwortung für die Informationssicherheit liegt bei der Geschäftsführung der <Institution>. Zur angemessenen Entwicklung, Einführung, Weiterentwicklung und Betrieb eines ISMS sowie zur Gewährleistung der definierten Sicherheitsziele wird ein Informationssicherheitsmanagement eingesetzt. Das Informationssicherheitsmanagement wird in seiner Aufgabe durch die Geschäftsführung angemessen unterstützt.

## Rollen und Gremien

Um den vielseitigen Ansprüchen und Sicherheitszielen der <Institution> zu entsprechen, setzt sich das Informationssicherheitsmanagement aus mehreren Rollen zusammen. Die Aufgaben und Befugnisse der einzelnen Rollen, werden im Standard „Rollen und Gremien“ weiter detailliert.

### <Informationssicherheitsbeauftragten>

Der <Informationssicherheitsbeauftragten> ist für die Entwicklung, Einführung, Weiterentwicklung und den Betrieb vom ISMS verantwortlich. Seine Aufgabe ist es, die Einhaltung der gesetzten Sicherheitsziele der <Institution> zu gewährleisten.

Der <Informationssicherheitsbeauftragten> ist befugt, sämtliche hierfür erforderlichen Regelungen, Konzepte und Maßnahmen zu entwickeln und einzuführen. Er ist in Abstimmung mit der Geschäftsführung ermächtigt, IT-Anwendungen ganz oder zeitweise einzustellen, wenn die Sicherheitsziele von der <Institution> gefährdet sind. Im Falle einer Gefahr im Verzuge kann er auch ohne Abstimmung mit der Geschäftsführung eigenmächtig die Abschaltung von IT-Anwendungen und IT-Systemen verfügen, diese Entscheidung ist dann zeitnah mit der Geschäftsführung zu überprüfen.

Der <Informationssicherheitsbeauftragten> ist in dieser Funktion organisatorisch dem <CEO oder CFO oder CTO> unterstellt und hat direktes Vortragsrecht bei der Geschäftsführung. Er verantwortet seine Handlungen gegenüber der Geschäftsführung der <Institution>.

### <Datenschutzbeauftragter>

Der <Datenschutzbeauftragter> ist in seiner Funktion direkt der Geschäftsführung unterstellt. Er ist bei der Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei. Er berät die Geschäftsführung und stimmt sich mit ihr über die Umsetzung notwendiger Maßnahmen ab. Er hat direktes Vortragsrecht bei der Geschäftsführung.

Der <Datenschutzbeauftragter> ist ermächtigt, Audits für den Aufschluss über tatsächliche Einhaltung der Datenschutzziele durchzuführen. Der <Datenschutzbeauftragter> ist darüber hinaus befugt, bei externen Dienstleistern Datenschutzaudits durchzuführen. Zu diesem Zweck sind entsprechende Vertragsklauseln in den Verträgen mit den externen Dienstleistern vorzusehen.

Der <Datenschutzbeauftragter> hat im erforderlichen Umfang seines Aufgabenbereichs in Abstimmung mit der Geschäftsführung das permanente Zutrittsrecht zu allen Stellen in der <Institution>.

### <Informationssicherheitsteam>

Aufgrund der engen Verzahnung der Themen und den Unternehmenszielen der <Institution> wird ein Informationssicherheitsteam gebildet. Es unterstützt die etablierten Rollen gemäß dem Standard "Rollen und Gremien“ bei der Gewährleistung der Sicherheitsziele.

## Regelungsstruktur

Die Dokumentationsstruktur des Informationssicherheitsmanagements wird durch eine hierarchische Regelungsstruktur abgebildet. Sie legt 4 Ebenen fest, die sich an einer Top-Down-Architektur orientieren.

Jede Ebene der Sicherheitsdokumentation ist verantwortlichen Einheiten in der <Institution> und Dienstleistungserbringern zugeordnet, die federführend die Sicherheitsdokumentation auf der jeweiligen Ebene und in der entsprechenden Detailtiefe erstellen, pflegen und gewährleisten.

Die Ebene 1 wird durch die „Leitlinie zur Informationssicherheit“ repräsentiert. Die Ebene 2 beinhaltet <Institution>-eigene Standards, mit denen die Anforderungen an die Umsetzung der Informationssicherheit festgelegt werden. Mit den Sicherheitsrichtlinien der Ebene 3 werden diese Anforderungen hinsichtlich ihrer Umsetzung detailliert. Die Ebene 4 wird durch die Konzepte und Dokumentationen der internen oder externen Dienstleistungserbringer anhand der steuernden Vorgaben der übergeordneten Ebenen gebildet und durch das Informationssicherheitsmanagement der <Institution> regelmäßig kontrolliert.

# Verstöße und Sanktionen

Als Verstöße gegen die „Leitlinie zur Informationssicherheit“ gelten vorsätzliche oder grob fahrlässige Handlungen,

* welche die Missachtung gesetzlicher Vorgaben darstellen,
* die den unberechtigten Zugriff auf Informationen, deren Preisgabe und/oder Änderung beinhalten,
* welche die Nutzung von Informationen der <Institution> für illegale Zwecke beinhalten,
* Zuwiderhandlungen gegen die Verschwiegenheitserklärung der <Institution>,
* die Sicherheit der Mitarbeitenden, Partnern und der <Institution> gefährden,
* welche Persönlichkeitsrechte von Partnern, Mitarbeitenden oder anderen Betroffenen verletzen und
* die der <Institution> durch das Kompromittieren der Sicherheit von Daten oder Geschäftsinformationen tatsächlich oder potenziell finanzielle Verluste einbringen.

Die Nichteinhaltung oder bewusste Verletzung der „Leitlinie zur Informationssicherheit“ und der nachgeltenden Dokumente kann zu einer den arbeitsrechtlich zugrunde liegenden Haftungsmaßnahmen führen.