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

Sicherheitsrichtlinie "Compliance-Management (Anforderungsmanagement)"

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 | ISMS300009 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments |  | [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](#_Toc79384911)

[Dokumentenhistorie 3](#_Toc79384912)

[Inhaltsverzeichnis 4](#_Toc79384913)

[Allgemeine Festlegungen 5](#_Toc79384914)

[Ziel / Zweck 5](#_Toc79384915)

[Geltungsbereich 5](#_Toc79384916)

[Zuständigkeiten 5](#_Toc79384917)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79384918)

[Aufbau des Dokuments 6](#_Toc79384919)

[Sicherheitsrichtlinie „Compliance-Management (Anforderungsmanagement)" 7](#_Toc79384920)

[Basismaßnahmen 7](#_Toc79384921)

[Identifikation der rechtlichen Rahmenbedingungen (ORP.5.A1) 7](#_Toc79384922)

[Beachtung rechtlicher Rahmenbedingungen (ORP.5.A2) 7](#_Toc79384923)

[Verpflichtung der Mitarbeitenden auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen (ORP.5.A3) 7](#_Toc79384924)

[Standardmaßnahmen 7](#_Toc79384925)

[Konzeption und Organisation des Compliance Managements (ORP.5.A4) 8](#_Toc79384926)

[Ausnahmegenehmigungen (ORP.5.A5) 8](#_Toc79384927)

[Einweisung des Personals in den sicheren Umgang mit IT (ORP.5.A6) 8](#_Toc79384928)

[Aufrechterhaltung der Informationssicherheit (ORP.5.A7) 8](#_Toc79384929)

[Regelmäßige Überprüfungen des Compliance Managements (ORP.5.A8) 8](#_Toc79384930)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc79384931)

[Schutz gegen nachträgliche Veränderungen von Informationen (ORP.5.A9 - I) 9](#_Toc79384932)

[Klassifizierung von Informationen (ORP.5.A10 - CIA) 9](#_Toc79384933)

[Erhebung der rechtlichen Rahmenbedingungen für kryptografische Verfahren und Produkte (ORP.5.A11 - CI) 9](#_Toc79384934)

# Allgemeine Festlegungen

## Ziel / Zweck

In der <Institution> gibt es gesetzliche, vertragliche, strukturelle und interne Richtlinien und Vorgaben, die beachtet werden müssen. Viele dieser Vorgaben haben direkte oder indirekte Auswirkungen auf das Informationssicherheitsmanagement.

Die Geschäftsführung der <Institution> muss die Einhaltung der Anforderungen („Compliance“) durch angemessene Überwachungsmaßnahmen sicherstellen.

Die <Institution> kann verschiedene Managementprozesse etablieren, welche sich mit unterschiedlichen Aspekten des Risikomanagements beschäftigen. Dazu zählen beispielsweise Informationssicherheitsmanagement, Datenschutzmanagement, Compliance Management und Controlling. Die verschiedenen Einheiten sollten vertrauensvoll zusammenarbeiten, um Synergieeffekte zu nutzen und Konflikte frühzeitig auszuräumen.

Ziel der Sicherheitsrichtlinie ist es, aufzuzeigen, wie sich Verantwortliche einen Überblick über die verschiedenen Anforderungen an die einzelnen Bereiche der <Institution> verschaffen können. Dazu wird beschrieben, wie aus gesetzlichen, vertraglichen, strukturellen und internen Richtlinien und Vorgaben entsprechende Sicherheitsanforderungen abgeleitet werden können. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines ORP.5 "Compliance Management (Anforderungsmanagement)" zurückgegriffen.

## Geltungsbereich

Die Vorgaben des Dokumentes sind für alle Prozessverantwortlichen der <Institution> verbindlich und entsprechend durch die zuständigen Rollenträger umzusetzen.

Anzuwenden sind die Vorgaben für alle durch die <Institution> verantworteten Geschäftsprozesse, Hard- und Softwarekomponenten sowie ihren Konfigurationen. Die Umsetzung dieser Arbeitsanweisung ist durch die entsprechenden Führungskräfte sicherzustellen.

Die im Folgenden beschriebenen Vorgaben sind hingegen nicht bindend für Prozessverantwortliche von Geschäftsprozessen, die nicht durch die <Institution> wahrgenommen werden. In diesen Fällen besitzen die beschriebenen Vorgaben einen empfehlenden Charakter, auf eine Einhaltung muss durch die <Institution> hingewirkt werden.

Interne Regelungen sind geschlechterneutral zu formulieren. Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung männlicher und weiblicher Sprachformen verzichtet. Sämtliche personenbezogenen Bezeichnungen in männlicher Form werden verallgemeinernd verwendet und beziehen sich stets auf alle Geschlechter.

## Zuständigkeiten

Zuständig für die Einhaltung der in diesem Dokument aufgeführten Pflichten und Anforderungen sind:

* Eigene Mitarbeitende und beauftragte Dienstleister, welche administrative Arbeiten an IT- Systemen und Anwendungen von der <Institution> durchführen,
* Eigene Mitarbeitende und beauftragte Dienstleister, welche Applikationsbetreuung mit administrativem Charakter (z. B. Versionspflege, Benutzerverwaltung) betreiben. Die Kontrolle der korrekten Umsetzung der Vorgaben erfolgt durch den <Bereich ???> bei der <Institution>.

## Genehmigungs- und Änderungsverfahren

Das Dokument „Sicherheitsrichtlinie Compliance-Management (Anforderungsmanagement)“ wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Informationssicherheitsbeauftragter>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Informationssicherheitsbeauftragter>.

## Aufbau des Dokuments

Das vorliegende Dokument ist wie folgt aufgebaut:

* Kapitel Basismaßnahmen: Beschreibung der Kernmaßnahmen, die für das Anforderungsmanagement zwingend erforderlich sind.
* Kapitel Standardmaßnahmen: Definition von Maßnahmen zur Erreichung eines vollumfänglichen Standardabsicherungsschutzniveaus für einen Schutzbedarf von „Normal“ in den Informationssicherheitsschutzzielen Vertraulichkeit, Integrität und Verfügbarkeit.
* Kapitel Maßnahmen bei erhöhtem Schutzbedarf: Erläuterung von Maßnahmen die einen erhöhten Schutzbedarf (Schutzbedarfe „Hoch“, „Sehr hoch“) gewährleisten. Der Einsatz ist je Anwendungsfall im Rahmen einer Verhältnismäßigkeitsprüfung abzuwägen.

# Sicherheitsrichtlinie „Compliance-Management (Anforderungsmanagement)"

## Basismaßnahmen

Die nachfolgenden Basismaßnahmen sind vorrangig zur Gewährleistung der sicherheitstechnischen Anforderungen aus der Leitlinie umzusetzen.

### Identifikation der rechtlichen Rahmenbedingungen (ORP.5.A1)

Die <Institution> etabliert einen Prozess zur Identifikation aller relevanten rechtlichen, vertraglichen und sonstigen Vorgaben. Diejenigen rechtlichen und vertraglichen Rahmenbedingungen, die Auswirkungen auf das Sicherheitsmanagement haben, werden zusätzlich dokumentiert.

In einer strukturierten Übersicht werden die relevanten gesetzlichen und vertraglichen Vorgaben an die Bereiche der <Institution> aufgearbeitet. Durch angemessene Maßnahmen wird sichergestellt, dass diese Übersicht jederzeit aktuell ist.

Die <Institution> gewährleistet, dass die sicherheitsrelevanten Anforderungen in der Planung und Konzeption von Geschäftsprozessen, SaaS-Lösungen, Anwendungen und IT-Systemen berücksichtigt werden.

### Beachtung rechtlicher Rahmenbedingungen (ORP.5.A2)

Die Umsetzung der rechtlichen Vorgaben unterliegt denjenigen Führungskräften, die die rechtliche Verantwortung in der <Institution> tragen. Die daraus resultierende Verantwortung und Zuständigkeit zur Einhaltung der rechtlichen Vorgaben wird entsprechend festgelegt.

Die <Institution> identifiziert und etabliert angemessene Maßnahmen, um etwaige Verstöße gegen relevante Vorschriften und Gesetze zu verhindern. Falls Verstöße dennoch festgestellt wurden, leitet die <Institution> angemessene Korrekturmaßnahmen zur Behebung der Abweichung ein.

### Verpflichtung der Mitarbeitenden auf Einhaltung einschlägiger Gesetze, Vorschriften und Regelungen (ORP.5.A3)

Durch angemessene Maßnahmen gewährleistet die <Institution>, dass alle Mitarbeitenden der <Institution> bzgl. einschlägiger Gesetze, Vorschriften und internen Regelungen eingewiesen und verpflichtet wurden und diese befolgen. Dabei wird ebenso sichergestellt, dass den Mitarbeitenden der rechtliche Rahmen ihrer ausgeführten Tätigkeit bekannt ist.

## Standardmaßnahmen

Gemeinsam mit den Basismaßnahmen sind die folgenden Standardmaßnahmen zum Erzielen eines normalen Schutzbedarfs zu betrachten und sollten grundsätzlich umgesetzt werden.

### Konzeption und Organisation des Compliance Managements (ORP.5.A4)

Zur Gewährleistung eines kontinuierlichen Überblicks über die verschiedenen Vorgaben und Anforderungen werden angemessene Prozesse und Organisationsstrukturen innerhalb der <Institution> etabliert. In diesem Rahmen werden ebenso entsprechende Verantwortlichkeiten und ihre Aufgaben im Bereich des Compliance Management definiert.

Durch eine angemessene Kollaboration zwischen der Unternehmenssteuerung, den Leitern der Bereiche und dem <Informationssicherheitsbeauftragter> wird sichergestellt, dass Sicherheitsanforderungen im Compliance Management berücksichtigt werden und sicherheitsrelevante Anforderungen in Sicherheitsmaßnahmen überführt und kontrolliert werden.

### Ausnahmegenehmigungen (ORP.5.A5)

Insofern ein Abweichen von Regelungen notwendig ist, werden diese Ausnahmen begründet und durch eine autorisierte Stelle im Rahmen einer Risikoabschätzung genehmigt. Zur Dokumentation, Überprüfung und Freigabe dieser Ausnahmegenehmigungen werden angemessene Prozesse etabliert. Dabei wird insbesondere sichergestellt, dass alle Ausnahmegenehmigungen befristet und in einer zentralen Übersicht festgehalten sind.

### Einweisung des Personals in den sicheren Umgang mit IT (ORP.5.A6)

Es ist sicherzustellen, dass alle Mitarbeitenden der <Institution> sowie externe Mitarbeitende (Freelancer) angemessen in den sicheren Umgang mit der IT eingewiesen werden. Den internen und externen Mitarbeitenden wird dazu eine verbindliche, verständliche und aktuelle Dokumentation zur IT-Nutzung bereitgestellt. Der Fokus der Dokumente liegt bei den Rechten und Pflichten, die die Mitarbeitenden bei der IT-Nutzung haben und welche zusätzlichen Sicherheitsmaßnahmen umzusetzen sind. Insofern sich Änderungen an den Vorgaben ergeben, werden diese den Mitarbeitenden zeitnah bekannt gegeben.

### Aufrechterhaltung der Informationssicherheit (ORP.5.A7)

Zur Aufrechterhaltung und kontinuierlichen Verbesserung des bestehenden Sicherheitsniveaus werden alle Sicherheitsmaßnahmen und -konzepte hinsichtlich ihrer Umsetzung und ihres Verbesserungsbedarfs überprüft. Bei der Überprüfung ist sicherzustellen, dass diese durch unabhängige und qualifizierte Mitarbeitende oder externe Dienstleister erfolgt. Die Ergebnisse dieser Überprüfung werden der Geschäftsführung vorgelegt und angemessen dokumentiert. Insofern sich durch die Überprüfung Mängel ergeben haben, werden diese unverzüglich nachverfolgt und behoben.

### Regelmäßige Überprüfungen des Compliance Managements (ORP.5.A8)

Zur Gewährleistung eines angemessenen Compliance Managements wird dieses und seine abgeleiteten Anforderungen und Maßnahmen regelmäßig auf Effektivität und Effizienz bewertet. Dabei wird insbesondere überprüft, ob die zugrundliegenden Prozesse und Organisationsstrukturen angemessen sind.

## Maßnahmen bei erhöhtem Schutzbedarf

Gemeinsam mit den Basismaßnahmen und den Standardmaßnahmen sind zum Erzielen eines erhöhten Schutzbedarfs die hier aufgeführten Maßnahmen zu betrachten und sollten grundsätzlich umgesetzt werden. Ist dies aus wirtschaftlichen bzw. organisatorischen Gründen nicht möglich, so ist dies mit dem Sicherheitsmanagement zur weiteren Begegnung von Risiken für die Infrastruktur der <Institution> zu begründen und abzustimmen. Im Folgenden werden die Maßnahmen bei erhöhtem Schutzbedarf aufgeführt. Die jeweils in Klammern angegebenen Buchstaben zeigen an, welche Grundwerte durch die Anforderung vorrangig geschützt werden (C = Vertraulichkeit, I = Integrität, A = Verfügbarkeit).

### Schutz gegen nachträgliche Veränderungen von Informationen (ORP.5.A9 - I)

In Abhängigkeit vom Datenformat und Schutzbedarf identifiziert und implementiert die <Institution> angemessene Maßnahmen damit Daten nicht unbemerkt veröffentlicht werden können. Die <Institution> berücksichtigt dabei insbesondere den Einsatz von digitalen Signaturen oder anderen kryptografischen Verfahren, den Einsatz von Copyright-Vermerken oder den Einsatz von Dateiformaten, die eine nachträgliche Veränderung erschweren.

Die Mitarbeitenden werden dahingehend informiert, welche Sicherheitsmaßnahmen ergriffen wurden und wie diese von den Mitarbeitenden zu benutzen sind.

### Klassifizierung von Informationen (ORP.5.A10 - CIA)

Auf Basis des Schutzbedarfes ergeben sich für bestimmte Informationen Restriktionen im Umgang mit diesen Informationswerten, weshalb die <Institution> alle Informationen anhand ihres Schutzbedarfs klassifiziert und kennzeichnet. Die Mitarbeitenden werden in regelmäßigen Abständen bzgl. des sorgfältigen Umgangs mit Informationen und den Restriktionen im Umgang mit klassifizierten Daten sensibilisiert.

### Erhebung der rechtlichen Rahmenbedingungen für kryptografische Verfahren und Produkte (ORP.5.A11 - CI)

Die <Institution> identifiziert und dokumentiert die rechtlichen Rahmenbedingungen für den Einsatz von kryptografischen Verfahren und Produkte für alle Länder, in denen diese genutzt werden sollen.