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

Standard "Rollen und Gremien"

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 Dokumentenvertraulichkeit  offen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS200001 | [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](#_Toc75072992)

[Dokumentenhistorie 3](#_Toc75072993)

[Inhaltsverzeichnis 4](#_Toc75072994)

[Allgemeine Festlegungen 5](#_Toc75072995)

[Ziel / Zweck 5](#_Toc75072996)

[Geltungsbereich 5](#_Toc75072997)

[Zuständigkeiten 5](#_Toc75072998)

[Genehmigungs- und Änderungsverfahren 5](#_Toc75072999)

[Standard "Rollen und Gremien" 6](#_Toc75073000)

[Rollen im Informationssicherheitsmanagement 6](#_Toc75073001)

[Geschäftsführung 6](#_Toc75073002)

[<Information Security Officer> 6](#_Toc75073003)

[Informationssicherheitsmanagementteam 8](#_Toc75073004)

# Allgemeine Festlegungen

## Ziel / Zweck

Zur Entwicklung, Einführung, Weiterentwicklung und dem Betrieb des ISMS sowie zur Gewährleistung unserer Sicherheitsziele wird ein Sicherheitsmanagement eingesetzt. Das Sicherheitsmanagement wird in seiner Aufgabe durch die Geschäftsführung angemessen unterstützt.

Um den vielseitigen Ansprüchen unserer Sicherheitsziele zu entsprechen, setzt sich das Sicherheitsmanagement aus mehreren Rollen und Gremien zusammen. Der Standard „Rollen und Gremien“ legt die Rollen, deren Aufgaben und Befugnisse sowie die Gremien fest.

## 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 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

Der Standard Rollen und Gremien wird durch den <Informationssicherheitsbeauftragter> verantwortet. Die Pflege dieses Dokuments unterliegt dem <Bereich ???> vertreten durch den <Information Security Officer>. Änderungen werden ausschließlich von dieser Person oder seinem Stellvertreter vorgenommen. Eine Genehmigung und Freigabe erfolgt durch den <Information Security Officer>.

# Standard "Rollen und Gremien"

## Rollen im Informationssicherheitsmanagement

Für ein stabiles und langfristig wirksames Informationssicherheitsmanagementsystem (ISMS) besteht die Notwendigkeit, Rollen und Gremien zu definieren und zu etablieren. Dieses Dokument beschreibt die Aufgaben, Verantwortlichkeiten, Kompetenzen, und Qualifikationen der Rollen und Gremien innerhalb des ISMS der <Institution>.

Maßgeblich für den Erfolg der Anstrengungen ist, dass den Rollen und Gremien des ISMS ausreichende Ressourcen (sowohl zeitlich als auch personell) für ihre Aufgaben zur Verfügung gestellt werden. Dies gilt insbesondere für die erstmalige Einrichtung von Prozessen im ISMS. Bereits während der Planung werden je Rolle qualifizierte Stellvertreter benannt, die die Aufgaben und Verantwortlichkeiten im Vertretungsfall wahrnehmen.

Folgende Rollen und Gremien sind Bestandteil des ISMS:

* Rollen
  + Geschäftsführung
  + <Informationssicherheitsbeauftragter>
* Gremien
  + Informationssicherheitsmanagementteam
  + Externe Gremien

### Geschäftsführung

Sicherheit zu erreichen und aufrechtzuerhalten, ist Ziel aller Sicherheitsmaßnahmen der <Institution>.

Die Sicherheitsmaßnahmen leiten sich aus den gesetzlichen und regulatorischen Rahmenbedingungen (z. B. vertragliche Auflagen) ab und sind die Basis des Verständnisses von Verpflichtungen gegenüber den Mitarbeitenden und Anwendern.

Die Geschäftsführung verpflichtet sich daher, für die Wahrung der Sicherheit eine geeignete Vorsorge zu leisten. Er betrachtet Sicherheit als wichtiges Ziel und unterstützt die Tätigkeit der Rolleninhaber und Gremien zur Erfüllung ihrer Aufgaben.

Die Geschäftsführung stellt sicher, dass für die nachfolgend genannten Rollen und Gremien Personen und Stellvertreter benannt werden.

### <Information Security Officer>

#### Verantwortlichkeiten und Pflichten

Der Information Security Officer ist für die Entwicklung, Einführung, Weiterentwicklung und Betrieb des ISMS verantwortlich und verfügt über ein Mitsprache-, Weisungs- und Vetorecht bei allen Entscheidungen, die die Informationssicherheit betreffen. Seine Aufgabe ist es, die Einhaltung der gesetzten Sicherheitsziele zu gewährleisten. Darüber hinaus vertritt er die <Institution> im Bereich Informationssicherheitsmanagements in definierten internen und externen Gremien. Er informiert und berät die Geschäftsführung in allen grundsätzlichen und wichtigen Fragen der Informationssicherheit. Zu seinen Hauptaufgaben zählen:

* Die Beratung hinsichtlich der Informationssicherheit.
* Das Einführen, Migrieren und Erhalten eines ISMS nach BSI Standard 200-1 „ISMS“.
* Das Anwenden von Informationssicherheitsweisungsbefugnissen.
* Die Erstellung von Sicherheitsdokumentationen und Sicherheitsrichtlinien.
* Das Spezifizieren von Sicherheitsanforderungen an Infrastrukturen, IT-Systeme, IT-Komponenten, Netze und Anwendungen.
* Die Beratung und Begleitung von internen und externen Projekten zu Sicherheitsfragen.
* Die Sensibilisierung und Schulung von Mitarbeitenden und Externen hinsichtlich Sicherheitsfragen und der Sicherheitskultur.
* Die Kontrolle und Aufrechterhaltung eines geeigneten IT-Sicherheitsniveaus.
* Die Feststellung und Auswertung von Sicherheitsvorfällen.
* Die Erstellung von Management-Reporten zur Informationssicherheit.
* Die Leitung des Informationssicherheitsmanagementteams.

Er ist weiterhin zuständig für das Management von Informationssicherheitsrisiken. Der Information Security Officer pflegt einen Ansatz zur Risikoeinschätzung und führt Risikoanalysen gemäß des BSI Standards 200-3 „Risikomanagement“ durch. Die Ergebnisse berichtet er an die Geschäftsführung. Er wirkt darauf hin, dass Maßnahmen, die über das vorhandene Sicherheitsniveau hinausgehen, als notwendig erkannt, ergriffen und umgesetzt werden.

Er und sein Stellvertreter sind dauerhafte Mitglieder des Informations­sicherheits­management­teams.

#### Befugnisse

Der <Informationssicherheitsbeauftragter> ist in dieser Funktion organisatorisch <WEM??> unterstellt, handelt im Vertrauen der Geschäftsführung und verantwortet ihr gegenüber Maßnahmen, die er veranlasst hat. Er verfügt über ein direktes Vortragsrecht.

Der <Informationssicherheitsbeauftragter> ist gegenüber den Projektmanagern, den Systembetreuern, den Anwenderbetreuern sowie den Mitarbeitenden in Bezug auf die Informationssicherheit weisungsbefugt.

Er ist in Abstimmung mit der Geschäftsführung ermächtigt, Anwendungen ganz oder zeitweise einzustellen, wenn die Sicherheitsziele der <Institution> gefährdet sind. Im Falle einer Gefahr im Verzug, kann er auch ohne Abstimmung mit der Geschäftsführung eigenmächtig über die Abschaltung von Anwendungen verfügen. Diese Entscheidung ist anschließend zeitnah mit der Geschäftsführung zu überprüfen.

Der <Informationssicherheitsbeauftragter> ist ermächtigt Audits durchzuführen beziehungsweise zu veranlassen, die Aufschlüsse über den Stand der Informationssicherheit geben.

Der <Informationssicherheitsbeauftragter> ist zwingend in alle die Informationssicherheit tangierenden Projekte einzubinden.

Der <Informationssicherheitsbeauftragter> hat in Abstimmung mit der Geschäftsführung für die Erfüllung seines Aufgabenbereichs das jederzeitige Zutrittsrecht zu allen Stellen der <Institution>.

Der <Informationssicherheitsbeauftragter> ist befugt, sämtliche hierfür erforderlichen Regelungen, Konzepte und Maßnahmen zu entwickeln und einzuführen.

### Informationssicherheitsmanagementteam

#### Verantwortlichkeiten und Pflichten

Das Informationssicherheitsmanagementteam orientiert sich am BSI Standard 200-2 „IT-Grundschutz-Methodik“ und dient der Unterstützung des <Informationssicherheitsbeauftragter> bei der Koordinierung von Sicherheitsmaßnahmen, der Informationserhebung und den Kontrollaufgaben. Das Informationssicherheitsmanagementteam agiert nur im internen Umfeld der <Institution> und ist zuständig für die Informationssicherheitsaspekte der eigenen Informationssysteme und Verfahren, die für die Geschäftsprozesse und Leistungserbringung der <Institution> erforderlich sind. Kundenverfahren liegen somit nicht im Zuständigkeitsbereich des Informationssicherheitsmanagementteams. Das Informationssicherheitsmanagementteam trifft sich üblicherweise alle zwei Monate.

Das Informationssicherheitsmanagementteam hat die Aufgabe:

* Die Informationssicherheitsziele und -strategien zu bestimmen und die Leitlinie zur Informationssicherheit weiterzuentwickeln.
* Die Umsetzung der Sicherheitsrichtlinien zu überprüfen.
* Die Sicherheitsprozesse zu initiieren, steuern und kontrollieren.
* Die Beratung der Erstellung von Informationssicherheitskonzepten durchzuführen.
* Die Wirksamkeit und Eignung der in den Sicherheitskonzepten geplanten Sicherheitsmaßnahmen zu überprüfen.
* Die Sensibilisierungs- und Schulungsprogramme für die Informationssicherheit zu konzipieren.
* Die auftretenden Sicherheitsvorfälle zu behandeln.

Das Informationssicherheitsmanagementteam setzt sich aus geeigneten Personen zusammen, die über Informationssicherheits- und IT-Kenntnisse verfügen sowie Erfahrungen über die prozessuale Infrastruktur der <Institution> besitzen. Das Informationssicherheitsmanagementteam spiegelt die unterschiedlichen Aufgabenbereiche der <Institution> wieder. Es ist erforderlich, dass mindestens folgende Rollen im Informationssicherheitsmanagementteam bedient werden:

* <Informationssicherheitsbeauftragter>
* <Chief Technology Officer>
* ein Mitarbeitender

#### Befugnisse

Das Informationssicherheitsmanagementteam fungiert als Steuerungs- und Abstimmungsinstanz der <Institution>, um sicherheitsrelevante Themen strategisch zu entwickeln und optimal verwalten zu können. Dabei übernehmen die Gremium-Teilnehmer die Kommunikation für zuständige Segmente und nutzen zur Verfügung stehende Ressourcen, wodurch Informationssicherheitsthemen begünstigt werden. Das Informationssicherheitsmanagementteam trägt dazu bei, die bestehende Sicherheitskultur der <Institution> zu fördern.