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

Sicherheitsrichtlinie "Personal"

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 | ISMS300007 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Personal" | [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](#_Toc78819768)

[Dokumentenhistorie 3](#_Toc78819769)

[Inhaltsverzeichnis 4](#_Toc78819770)

[Allgemeine Festlegungen 5](#_Toc78819771)

[Ziel / Zweck 5](#_Toc78819772)

[Geltungsbereich 5](#_Toc78819773)

[Zuständigkeiten 5](#_Toc78819774)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78819775)

[Aufbau des Dokuments 6](#_Toc78819776)

[Sicherheitsrichtlinie „Personal" 7](#_Toc78819777)

[Basismaßnahmen 7](#_Toc78819778)

[Geregelte Einarbeitung neuer Mitarbeitenden (ORP.2.A1) 7](#_Toc78819779)

[Geregelte Verfahrensweise beim Weggang von Mitarbeitenden (ORP.2.A2) 7](#_Toc78819780)

[Vertretungsregelungen (ORP.2.A3) 7](#_Toc78819781)

[Regelungen für den Einsatz von Fremdpersonal (ORP.2.A4) 8](#_Toc78819782)

[Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (ORP.2.A5) 8](#_Toc78819783)

[Standardmaßnahmen 8](#_Toc78819784)

[Überprüfung von Kandidaten bei der Auswahl von Personal (ORP.2.A6) 8](#_Toc78819785)

[Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (ORP.2.A7) 8](#_Toc78819786)

[Aufgaben und Zuständigkeiten von Mitarbeitenden (ORP.2.A8) 9](#_Toc78819787)

[Schulung von Mitarbeitenden (ORP.2.A9) 9](#_Toc78819788)

[Vermeidung von Störungen des Betriebsklimas (ORP.2.A10) 9](#_Toc78819789)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc78819790)

[Analyse der Sicherheitskultur (ORP.2.A11 - CA) 9](#_Toc78819791)

[Benennung einer Vertrauensperson (ORP.2.A12 - C) 10](#_Toc78819792)

[Sicherheitsüberprüfung (ORP.2.A13 - CA) 10](#_Toc78819793)

# Allgemeine Festlegungen

## Ziel / Zweck

Die Mitarbeitenden der <Institution> haben einen entscheidenden Anteil am Erfolg oder Misserfolg unserer Strategien, Lösungen und der Umsetzung der Informationssicherheit. Es können die aufwendigsten Sicherheitsvorkehrungen ins Leere laufen, wenn diese Vorkehrungen im Arbeitsalltag nicht gelebt werden. Die elementare Bedeutung von Informationssicherheit für die <Institution> sowie deren Geschäftsprozesse muss daher für die Mitarbeitenden (Personal) transparent und nachvollziehbar aufbereitet sein.

Ziel dieser Sicherheitsrichtlinie ist es aufzuzeigen, welche „personellen“ Sicherheitsmaßnahmen die Personalabteilung oder Vorgesetzten ergreifen müssen, damit die Mitarbeitenden der <Institution> verantwortungsbewusst mit den Informationen umgehen und sich so gemäß den Vorgaben verhalten. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines ORP.2 "Personal" beachtet.

## 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 Personal“ 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 „Personal"

## Basismaßnahmen

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

### Geregelte Einarbeitung neuer Mitarbeitenden (ORP.2.A1)

Neben der Personalabteilung sind die Vorgesetzten für eine angemessene Einarbeitung der Mitarbeitenden verantwortlich. Mittels Onboarding-Sessions und Checklisten sollten die Mitarbeitenden über bestehende Regelungen, Gepflogenheiten und Verfahrensweisen im Allgemeinen und im Umfeld der Informationssicherheit informiert werden.

Des Weiteren wird mit etablierten Prozessen dafür gesorgt, Mitarbeitende über Veränderungen und deren Auswirkungen auf Geschäftsprozesses bzw. des jeweiligen Arbeitsfeldes zu informieren.

Alle Mitarbeitende sind darauf verpflichtet einschlägige Gesetze, Vorschriften und interne Regelungen einzuhalten. Alle Mitarbeitende sind darauf hingewiesen, dass alle während der Arbeit erhaltenen Informationen ausschließlich zum internen Gebrauch bestimmt sind, solange sie nicht anders gekennzeichnet wurden.

### Geregelte Verfahrensweise beim Weggang von Mitarbeitenden (ORP.2.A2)

Um eine erfolgreiche Übergabe an den Nachfolger ermöglichen zu können, wird vor dem Ausscheiden eines Mitarbeitenden dessen Nachfolge rechtzeitig geregelt. Ist dies in Ausnahmefällen nicht möglich, erstellt der ausscheidende Mitarbeitende eine vollständige Dokumentation der bis zum Ausscheiden durchgeführten Aufgaben.

Alle Gegenstände (Unterlagen, Schlüssel, Ausweise, Token) werden, im Abgleich mit der Ausgabeliste, eingezogen. Die Deaktivierung bzw. Löschung aller Zugriffs- und Zutrittsrechte ist sicherzustellen.

Dem Ausscheidenden wird explizit die Verschwiegenheitsverpflichtung in Erinnerung gerufen.

Alle relevanten Stellen sind über das Ausscheiden informiert.

Ist der ausscheidende Mitarbeitende namentlich in Ablaufplänen, Notfallplänen oder Ähnlichem genannt, sind diese Pläne zu überarbeiten.

### Vertretungsregelungen (ORP.2.A3)

Die Vorgesetzten sind verantwortlich für die Einführung und Aufrechterhaltung von Vertretungsregelungen. Dabei sind alle Geschäftsprozesse zu berücksichtigen und die Aufgaben der Vertretung sind klar zu regeln. Darüber hinaus ist sicherzustellen, dass der Vertretende über das notwendige Fachwissen verfügt.

Ist es im Ausnahmefall nicht möglich für einzelne Mitarbeitende einen kompetenten Vertreter zu benennen oder zu schulen, muss frühzeitig entschieden werden, ob externes Personal dafür hinzugezogen werden kann.

### Regelungen für den Einsatz von Fremdpersonal (ORP.2.A4)

Wird externes Personal seitens der <Institution> beschäftigt, muss dieses grundsätzlich wie alle eigenen Mitarbeitenden dazu verpflichtet werden, geltende Gesetze, Vorschriften und interne Regelungen einzuhalten. Externes Personal, das kurzfristig oder einmalig eingesetzt wird, sollte in sicherheitsrelevanten Bereichen beaufsichtigt werden. Bei längerfristig beschäftigtem externem Personal muss dieses wie die eigenen Mitarbeitenden in seine Aufgaben eingewiesen werden. Auch für diese Mitarbeitenden muss eine Vertretungsregelung eingeführt werden.

Verlässt das Fremdpersonal die <Institution> müssen Arbeitsergebnisse wie bei eigenem Personal geregelt übergeben und eventuell ausgehändigte Zugangsberechtigungen zurückgegeben werden.

### Vertraulichkeitsvereinbarungen für den Einsatz von Fremdpersonal (ORP.2.A5)

Bevor externes Personal Zugang und Zugriff zu vertraulichen Informationen erhält, muss eine Vertraulichkeitsvereinbarung abgeschlossen werden. In dieser Vertraulichkeitsvereinbarung müssen alle wichtigen Aspekte zum Schutz von internen und kundenspezifischen Informationen berücksichtigt werden.

## Standardmaßnahmen

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

### Überprüfung von Kandidaten bei der Auswahl von Personal (ORP.2.A6)

Bei der Auswahl neuer Mitarbeitende liegt eine genau formulierte Beschreibung der Qualifikation und der Fähigkeiten vor. Die formulierten Qualifikationen sind mit den Kandidaten im Bewerbungsgespräch in geeigneter Form abzugleichen bzw. zu prüfen.

Um bei einem zukünftigen Stellenwechsel Interessenkonflikte zu vermeiden, sollten Konkurrenzverbote oder Karenzzeiten vereinbart werden.

### Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden (ORP.2.A7)

Neue Mitarbeitende sollten bevor sie eingestellt werden, auf ihre Vertrauenswürdigkeit hin überprüft werden. Deshalb sollten alle an der Personalauswahl Beteiligten soweit möglich kontrollieren, ob die Angaben der Bewerberinnen und Bewerber, die relevant für die Einschätzung ihrer Vertrauenswürdigkeit sind, glaubhaft sind. Insbesondere sollte kritisch geprüft werden, ob der vorgelegte Lebenslauf korrekt, plausibel und vollständig ist. Dabei sollten kritisch erscheinende Informationen überprüft werden, etwa indem dezidiert nachgefragt wird oder weitere Nachweise (bspw. praktische Übungen vor Ort) verlangt werden.

Vor der Einstellung erfolgt die Einsicht in ein amtliches Dokument mit Bild, zur Sicherstellung, dass es sich um den richtigen Kandidaten handelt.

### Aufgaben und Zuständigkeiten von Mitarbeitenden (ORP.2.A8)

Alle Aufgaben und Zuständigkeiten sind durch den Arbeitsvertrag und/oder durch entsprechende Vereinbarungen dokumentiert. Insbesondere sollte vereinbart sein, dass jeder Mitarbeitende auch außerhalb der Arbeitszeit für die Einhaltung der Informationssicherheit zuständig ist.

### Schulung von Mitarbeitenden (ORP.2.A9)

Durch regelmäßige Schulungen der Mitarbeitenden wird gewährleistet, dass alle Tätigkeiten mit einem Wissenstand, welcher dem Stand der Technik entspricht, erledigt werden. Bei größerem Schulungsbedarf sollten einzelne Mitarbeitende gesondert geschult und innerhalb des Tätigkeitsbereichs als Multiplikatoren für die übrigen Mitarbeitenden eingesetzt werden.

Alle Mitarbeitenden sind in die Geräte, Anwendungen und Aktivitäten eingewiesen, werden regelmäßig im Bereich der Informationssicherheit geschult und über alltägliche Risiken und mögliche Gegenmaßnahmen unterrichtet um diese im Arbeitstag ein- bzw. umzusetzen.

### Vermeidung von Störungen des Betriebsklimas (ORP.2.A10)

Es sollten auch aus Sicht der Informationssicherheit Maßnahmen ergriffen werden, um für ein positives Betriebsklima zu sorgen.

## 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).

### Analyse der Sicherheitskultur (ORP.2.A11 - CA)

Zur Aufrechterhaltung des hohen Sicherheitsstandards werden, unter Berücksichtigung der rechtlichen Rahmenbedingungen, Analysen zum Verhalten der Mitarbeitenden durchgeführt und ausgewertet. Aufgedeckte Potentiale zur Verbesserung der personellen und organisatorischen Sicherheit werden genutzt.

### Benennung einer Vertrauensperson (ORP.2.A12 - C)

Für die Mitarbeitende sollte eine Vertrauensperson als Ansprechpartner benannt werden.

### Sicherheitsüberprüfung (ORP.2.A13 - CA)

Im Hochsicherheitsbereich sollte eine zusätzliche Sicherheitsüberprüfung zusätzlich zur grundlegenden Überprüfung der Vertrauenswürdigkeit von Mitarbeitenden durchgeführt werden.

Überprüft werden jedoch nur die Mitarbeitende, die eine Tätigkeit ausüben sollen, bei den diese Zugang zu geheimhaltungsbedürftigen Angelegenheiten erhalten oder sich verschaffen können und ihrer Sicherheitsüberprüfung zugestimmt haben. Hierzu gehören zum Beispiel Bearbeiter von Verschlusssachen des Geheimhaltungsgrades VS-VERTRAULICH oder höher.