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

Sicherheitsrichtlinie "Telearbeit"

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 | ISMS300019 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Telearbeit" | [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](#_Toc79908553)

[Dokumentenhistorie 3](#_Toc79908554)

[Inhaltsverzeichnis 4](#_Toc79908555)

[Allgemeine Festlegungen 5](#_Toc79908556)

[Ziel / Zweck 5](#_Toc79908557)

[Geltungsbereich 5](#_Toc79908558)

[Zuständigkeiten 5](#_Toc79908559)

[Genehmigungs- und Änderungsverfahren 6](#_Toc79908560)

[Aufbau des Dokuments 6](#_Toc79908561)

[Sicherheitsrichtlinie „Telearbeit" 7](#_Toc79908562)

[Basismaßnahmen 7](#_Toc79908563)

[Regelungen für Telearbeit (OPS.1.2.4.A1) 7](#_Toc79908564)

[Sicherheitstechnische Anforderungen an den Telearbeitsrechner (OPS.1.2.4.A2) 7](#_Toc79908565)

[Sicherheitstechnische Anforderungen an die Kommunikationsverbindung (OPS.1.2.4.A3) 7](#_Toc79908566)

[Datensicherung bei der Telearbeit (OPS.1.2.4.A4) 7](#_Toc79908567)

[Sensibilisierung und Schulung der Telearbeiter (OPS.1.2.4.A5) 7](#_Toc79908568)

[Standardmaßnahmen 8](#_Toc79908569)

[Erstellen eines Sicherheitskonzeptes für Telearbeit (OPS.1.2.4.A6) 8](#_Toc79908570)

[Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (OPS.1.2.4.A7) 8](#_Toc79908571)

[Informationsfluss zwischen Telearbeiter und Institution (OPS.1.2.4.A8) 8](#_Toc79908572)

[Betreuungs- und Wartungskonzept für Telearbeitsplätze (OPS.1.2.4.A9) 8](#_Toc79908573)

[Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (OPS.1.2.4.A10) 9](#_Toc79908574)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc79908575)

# Allgemeine Festlegungen

## Ziel / Zweck

Unter Telearbeit wird innerhalb der <Institution> jede auf die Informations- und Kommunikationstechnik gestützte Tätigkeit verstanden, die ganz oder in Teilen außerhalb der Gebäude und Räume der <Institution> durchgeführt wird.

Bei Telearbeit aus dem Homeoffice arbeiten die Mitarbeitenden regelmäßig tages- oder stundenweise abwechselnd an ihrem festen oder wechselnden Arbeitsplatz in den Räumlichkeiten der <Institution> und im Homeoffice.

Ziel dieser Sicherheitsrichtlinie ist der Schutz von Informationen der <Institution>, die während der Telearbeit gespeichert, verarbeitet und übertragen werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Baustein OPS.1.2.4 "Telearbeit" 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 Telearbeit“ 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 „Telearbeit"

## Basismaßnahmen

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

### Regelungen für Telearbeit (OPS.1.2.4.A1)

Alle relevanten Aspekte der Telearbeit werden im Einklang mit den bereits vorhandenen internen Vorgaben abgestimmt und erkannte zusätzlich benötigte Reglungen werden mit aufgenommen. Mit Hilfe eines Merkblattes werden alle Regelungen für die Telearbeit Mitarbeitenden ausgehändigt.

Aufbauend auf der bereits etablierten Vertreterregelung sind für jeden Telearbeiter ein Vertreter zu benennen. Die Vertretungsregelung sollte regelmäßig geprüft werden. Alle freigegebenen Regelungen zur Telearbeit sind regelmäßig zu überprüfen und bei Bedarf zu aktualisieren.

### Sicherheitstechnische Anforderungen an den Telearbeitsrechner (OPS.1.2.4.A2)

Es sind sicherheitstechnischen Anforderungen festzulegen, die ein IT-System für die Telearbeit erfüllen muss. Die Anforderungen sollten hierbei im Einklang mit den bereits dokumentierten Anforderungen an mobile Endgeräte sein. Unter Anwendung des Need-to-know-Prinzips sind alle Zugangsmöglichkeiten auf Informationen und IT-Systeme der <Institution> auf das notwendige Mindestmaß zu beschränken.

Es ist sicherzustellen, dass nur autorisierte Mitarbeitende Zugang zu den mobilen Endgeräten (Telearbeitsrechnern) erlangen können. Darüber hinaus ist sicherzustellen, dass der Telearbeitsrechner so abgesichert ist, dass dieser nur für autorisierte Zwecke benutzt werden kann.

### Sicherheitstechnische Anforderungen an die Kommunikationsverbindung (OPS.1.2.4.A3)

Alle eingesetzten Kommunikationsprotokolle und Sicherheitsmechanismen müssen den intern freigegebenen Verfahren und deren kryptographischer Absicherung entsprechen.

### Datensicherung bei der Telearbeit (OPS.1.2.4.A4)

Alle Daten, die bei der Telearbeit durch die Mitarbeitenden erstellt und bearbeitet werden, sind zeitnah auf den von der <Institution> bereitgestellten Lösungen zu sichern.

Für einen reibungslosen Prozessablauf sind bei der Datensicherung möglichst wenige Aktionen vom Mitarbeitenden auszugehen.

### Sensibilisierung und Schulung der Telearbeiter (OPS.1.2.4.A5)

Im Rahmen der etablierten Schulungsprogramme sind die Mitarbeitenden für die Gefahren zu sensibilisieren. Im Rahmen der Sensibilisierung sollten ebenfalls die hinterlegten und aktiven Sicherheitsmaßnahmen aufgezeigt und deren Umgang mitgeschult werden.

## Standardmaßnahmen

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

### Erstellen eines Sicherheitskonzeptes für Telearbeit (OPS.1.2.4.A6)

Für die Telearbeit sollte ein Sicherheitskonzept erstellt werden. Das Sicherheitskonzept muss die Sicherheitsziele, die Schutzbedarfe (Vertraulichkeit, Integrität und Verfügbarkeit), die abgestimmten Sicherheitsanforderungen, die erkannten und betrachteten Risiken sowie bei Bedarf einen Maßnahmenbehandlungsplan beinhalten. Das Sicherheitskonzept ist in den etablierten Dokumentenmanagementprozess aufzunehmen und regelmäßig auf Aktualität zu prüfen und bei einem erkannten Verbesserungsbedarf zu aktualisieren.

### Regelung der Nutzung von Kommunikationsmöglichkeiten bei Telearbeit (OPS.1.2.4.A7)

Es sollte klar geregelt werden, welche Kommunikationsmöglichkeiten bei der Telearbeit unter welchen Rahmenbedingungen von den Mitarbeitenden der <Institution> genutzt werden dürfen. Die private Nutzung von Internetdiensten bei der Telearbeit sollte unter Berücksichtigung der <Institution>-weiten Vorgaben zur privaten Nutzung auch für die Telearbeit angewandt werden.

### Informationsfluss zwischen Telearbeiter und Institution (OPS.1.2.4.A8)

Es sollte ein regelmäßiger innerbetrieblicher Informationsaustausch zwischen den Mitarbeitenden der <Institution> gewährleistet sein. Alle Telearbeiter sind zeitnah über geänderte Sicherheitsanforderungen und andere sicherheitsrelevante Aspekte zu informieren. Allen Teammitgliedern des jeweiligen Telearbeiters sollte bekannt sein, wann, wie und wo dieser erreicht werden kann. Technische und organisatorische Telearbeitsregelungen zur Aufgabenbewältigung, zu Sicherheitsvorfällen und sonstigen Problemen sind zu regeln und an den Telearbeiter zu kommunizieren.

### Betreuungs- und Wartungskonzept für Telearbeitsplätze (OPS.1.2.4.A9)

Für die Telearbeitsplätze der <Institution> sollte ein spezielles Betreuungs- und Wartungskonzept erstellt bzw. alternativ in die bereits bestehenden Konzepte die Aspekte für die Telearbeitsplätze mit aufgenommen werden. Grundsätzlich sind folgende Aspekte zu regeln: die Ansprechpartner für den Benutzerservice, die Wartungstermine, die Fernwartung und der Transport der IT-Systeme. Die Ansprechpartner für Hard- und Softwareprobleme sind den Telearbeitern zu benennen.

### Durchführung einer Anforderungsanalyse für den Telearbeitsplatz (OPS.1.2.4.A10)

Bevor ein Telearbeitsplatz eingerichtet wird, sollte eine Anforderungsanalyse durchgeführt werden. Aus der Anforderungsanalyse sollte mindestens hervorgehen, welche Hard- und Software-Komponenten für den Telearbeitsplatz benötigt werden. Die Anforderungen an den jeweiligen Telearbeitsplatz sind mit den IT-Verantwortlichen abzustimmen. Es muss immer festgestellt und dokumentiert werden, welchen Schutzbedarf die am Telearbeitsplatz verarbeiteten Informationen haben.

## Maßnahmen bei erhöhtem Schutzbedarf

Für diese Sicherheitsrichtlinie sind keine Anforderungen für einen erhöhten Schutzbedarf definiert.