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

Sicherheitsrichtlinie "Mobiles Arbeiten"

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 | ISMS300062 | [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](#_Toc83809668)

[Dokumentenhistorie 3](#_Toc83809669)

[Inhaltsverzeichnis 4](#_Toc83809670)

[Allgemeine Festlegungen 5](#_Toc83809671)

[Ziel / Zweck 5](#_Toc83809672)

[Geltungsbereich 5](#_Toc83809673)

[Zuständigkeiten 5](#_Toc83809674)

[Genehmigungs- und Änderungsverfahren 6](#_Toc83809675)

[Aufbau des Dokuments 6](#_Toc83809676)

[Sicherheitsrichtlinie „Mobiles Arbeiten" 7](#_Toc83809677)

[Basismaßnahmen 7](#_Toc83809678)

[Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes (INF.9.A1) 7](#_Toc83809679)

[Regelungen für mobile Arbeitsplätze (INF.9.A2) 7](#_Toc83809680)

[Zutritts- und Zugriffsschutz (INF.9.A3) 8](#_Toc83809681)

[Arbeiten mit fremden IT-Systemen (INF.9.A4) 8](#_Toc83809682)

[Standardmaßnahmen 8](#_Toc83809683)

[Zeitnahe Verlustmeldung (INF.9.A5) 8](#_Toc83809684)

[Entsorgung von vertraulichen Informationen (INF.9.A6) 9](#_Toc83809685)

[Rechtliche Rahmenbedingungen für das mobile Arbeiten (INF.9.A7) 9](#_Toc83809686)

[Verschlüsselung tragbarer IT-Systeme und Datenträger (INF.9.A9) 9](#_Toc83809687)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc83809688)

[Einsatz von Diebstahlsicherungen (INF.9.A10 - A) 9](#_Toc83809689)

[Verbot der Nutzung unsicherer Umgebungen (INF.9.A11 - CIA) 10](#_Toc83809690)

# Allgemeine Festlegungen

## Ziel / Zweck

Sofern eine gleichbleibend schnelle Internet-Anbindung bzw. Netzabdeckung am Standort besteht sowie leistungsfähige Notebooks, Smartphones oder Tablets den Mitarbeitenden bereitgestellt werden, können die Mitarbeitenden nahezu an jedem Platz bzw. von überall arbeiten. Das bedeutet, dass geschäftliche Aufgaben häufig nicht mehr nur in den Räumen und Gebäuden der <Institution> erfüllt werden müssen, sondern an wechselnden Arbeitsplätzen in unterschiedlichen Umgebungen (bspw. zu Hause, im Zug oder bei Dienstleistern) möglich ist. Unabhängig von der aktuellen Arbeitsumgebung müssen die Informationen der <Institution> angemessen geschützt werden.

Das mobile Arbeiten verändert einerseits die Dauer, Lage und Verteilung der Arbeitszeiten. Andererseits erhöht es die Anforderungen an die Informationssicherheit, da in mobilen Arbeitsplatz-Umgebungen nicht eine sichere IT-Infrastruktur vorausgesetzt werden kann.

Diese Sicherheitsrichtlinie definiert Sicherheitsanforderungen an mobile Arbeitsplätze. Ziel ist es, für solche Arbeitsplätze eine mit einem Büroraum vergleichbare Sicherheitssituation zu schaffen. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines INF.9 "Mobiler Arbeitsplatz" 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

Die Sicherheitsrichtlinie „Mobiles Arbeiten“ 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 „Mobiles Arbeiten"

## Basismaßnahmen

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

### Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes (INF.9.A1)

Die <Institution> ermöglicht es ihren Mitarbeitenden die Nutzung von mobilen Arbeitsplätzen sofern sichergestellt ist, dass mindestens diese Anforderungen von dem Mitarbeitenden erfüllt sind:

* Eine permanente Stromversorgung ist gegeben.
* Eine permanente Netzanbindung mit mindestens 16 Mbit/s im Download und 1.024 Kbit/s im Upload im asynchronen Modus oder 5Mbit/s im synchronen Modus alleinig besteht.
* Der Mitarbeitende den Bildschirm vor ungewollter Einsicht Dritter schützt.
* Durch den Mitarbeitenden gewährleistet ist, dass Unbefugte zu keiner Zeit den mobilen Arbeitsplatz betreten und auf geschäftliche IT und Unterlagen zugreifen können. Diese Maßnahmen sind in sinnvoller Art und sinnvollen zeitlichen Abständen, mindestens aber bei einer Änderung der mobilen Arbeitsplatz Verhältnisse zu überprüfen.
* Alle unternehmensrelevanten Informationen durch den Mitarbeitenden grundsätzlich auf den dafür vorgesehenen Netzwerklaufwerken, Cloud-Speichern oder Webanwendungen der <Institution> gespeichert werden.
* Der Mitarbeitende nicht die etablierten Sicherheitseinstellungen auf dem zur Verfügung gestellten IT-Equipment umgeht oder privates IT-Equipment zur Erfüllung seiner Tätigkeit einsetzt.
* Informationen der <Institution> dürfen vom Firmen-Notebook nicht auf betriebsfremde, insbesondere private IT-Systeme übertragen werden. Ausnahmen müssen schriftlich durch die disziplinarischen Vorgesetzten und dem <Informationssicherheitsbeauftragter> genehmigt werden.
* Der Mitarbeitende Verlust, Diebstahl und erkannte potentielle Sicherheitsvorfälle unverzüglich den Verantwortlichen bei der <Institution> meldet.

### Regelungen für mobile Arbeitsplätze (INF.9.A2)

Außerhalb der Räumlichkeiten der <Institution> müssen alle digitalen Daten in verschlüsselter Form transportiert und dürfen nur durch berechtigte Mitarbeitende bearbeitet werden. Die Mitarbeitenden müssen sich dazu verpflichten, die etablierten Sicherheitseinstellungen auf dem zur Verfügung gestellten IT-Equipment nicht zu umgehen oder ein privates IT-Equipment zur Erfüllung der Tätigkeit einzusetzen.

Für den Zugriff auf die Daten der <Institution> in Webanwendungen oder die Einwahl auf die Infrastrukturen der <Institution> müssen die bereitgestellten Zugänge genutzt werden. Die Mitbenutzung bzw. das Einschleusen von privaten VPNs oder Anonymisierungstools für die Anmeldung an Webanwendungen oder Infrastrukturen der <Institution> darf durch den Mitarbeitenden nicht erfolgen. Sofern die Nutzung solcher Tools erkannt wird, darf die <Institution> dieses technisch verhindern.

Die Mitarbeitenden dürfen die von der <Institution> bereitgestellten IT-Komponenten und Datenträgern für das mobile Arbeiten verwenden. Sofern Mitarbeitende nicht auf Sie persönlich registrierte Komponenten mit außer Haus nehmen möchten, muss dies mit dem disziplinarischen Vorgesetzten abgestimmt und schriftlich dokumentiert werden. In das Dokument müssen einfließen, von wem, was, von wann, bis wann außerhalb der Räumlichkeiten der <Institution> eingesetzt wird.

Geschäftliche Unterlagen und Datenträger müssen im mobilen Umfeld so aufbewahrt, dass kein Unbefugter darauf zugreifen kann. Dies bedeutet, dass jeder Mitarbeitende seinen mobilen Arbeitsplatz aufgeräumt hinterlässt und sicherstellt, dass keine vertraulichen Informationen frei zugänglich sind (CleanDesk-Policy).

Im Rahmen des etablierten Schulungsprogramms müssen die Mitarbeitenden für den Wert mobiler IT-Systeme und den Wert der darauf gespeicherten Informationen sensibilisiert werden.

### Zutritts- und Zugriffsschutz (INF.9.A3)

Den Mitarbeitenden muss bekannt gegeben werden, welche Regelungen und Maßnahmen zum Einbruch- und Zutrittsschutz am mobilen Arbeitsplatz zu beachten sind. Insbesondere muss darauf hingewiesen werden, dass wenn der Mitarbeiter nicht am mobilen Arbeitsplatz ist, sind die Fenster zu schließen und Türen abzuschließen. Sofern die Räumlichkeiten mit mehreren Personen geteilt werden, gilt dies adäquat. Ist dies nicht möglich, z. B. im Zug, müssen die Mitarbeitenden alle Unterlagen und IT-Systeme an sicherer Stelle verwahren, wenn sie abwesend sind. Es muss sichergestellt werden, dass Unbefugte zu keiner Zeit auf IT der <Institution> und deren Unterlagen zugreifen können.

Werden die Räume vom Mitarbeitenden nur kurz verlassen, müssen die eingesetzten IT-Systeme gesperrt oder heruntergefahren werden, sodass die IT-Systeme nur nach erfolgreicher Authentisierung wieder benutzt werden können und alle Daten durch die etablierte Festplattenverschlüsselung geschützt sind.

### Arbeiten mit fremden IT-Systemen (INF.9.A4)

Da sich das Schutzniveau fremder IT-Systeme von dem der <Institution> stark unterscheiden kann, muss jeder mobile Mitarbeitende über die Gefahren fremder IT-Systeme sensibilisiert werden.

## Standardmaßnahmen

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

### Zeitnahe Verlustmeldung (INF.9.A5)

Die Mitarbeitenden müssen umgehend melden, wenn Informationen, Notebooks, Smartphones, Tablets oder (Wechsel)Datenträger verloren gegangen sind oder gestohlen wurden. Bei potentiellen Sicherheitsvorfällen, verlorenen oder gestohlenen Notebooks, Smartphones, Tablets oder (Wechsel)Datenträger sollte zusätzlich der <Datenschutzbeauftragter> und der <Informationssicherheitsbeauftragter> informiert werden.

### Entsorgung von vertraulichen Informationen (INF.9.A6)

Vertrauliche Informationen müssen auch im Rahmen des mobilen Arbeitens sicher entsorgt werden. Bevor ausgediente oder defekte Datenträger und Papierdokumente weggeworfen (entsorgt) werden, muss überprüft werden, ob diese vertraulichen Informationen enthalten. Ist dies der Fall, müssen die Datenträger und Papierdokumente wieder mit zurück in die Standorte der <Institution> transportiert werden und auf den etablierten internen Wegen und Prozessen entsorgt bzw. vernichtet werden.

### Rechtliche Rahmenbedingungen für das mobile Arbeiten (INF.9.A7)

Für das mobile Arbeiten sollten arbeitsrechtliche und arbeitsschutzrechtliche Rahmenbedingungen beachtet und geregelt werden. Alle relevanten Punkte sollten entweder durch Betriebsvereinbarungen oder durch zusätzlich zum Arbeitsvertrag getroffene individuelle Vereinbarungen zwischen dem mobilen Mitarbeitenden und der <Institution> geregelt werden.

### Verschlüsselung tragbarer IT-Systeme und Datenträger (INF.9.A9)

Es sollte sichergestellt werden, dass schützenswerte Informationen nicht durch unberechtigte Dritte, entsprechend den internen Richtlinien der <Institution>, eingesehen werden können. Mobile Datenträger und Clients sollten verschlüsselt werden. Dabei müssen die kryptografischen Schlüssel getrennt vom verschlüsselten Gerät bspw. im bereitgestellten Passwort-Manager aufbewahrt werden.

## 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).

### Einsatz von Diebstahlsicherungen (INF.9.A10 - A)

Bietet das verwendete IT-System an eine Diebstahlsicherung zu verwenden, sollte die Diebstahlsicherung durch den Mitarbeitenden benutzt werden. Die Diebstahlsicherung sollte stets dort eingesetzt werden, wo ein erhöhter Publikumsverkehr herrscht oder die Fluktuation sehr hoch ist. Dabei sollten die Mitarbeitenden immer beachten, dass der Schutz der auf den IT-Systemen gespeicherten Informationen meist einen höheren Wert besitzt als die Wiederanschaffungskosten des IT-Systems betragen. Die Beschaffungs- und Einsatzkriterien für Diebstahlsicherungen sollten an die Prozesse der <Institution> angepasst und dokumentiert werden.

### Verbot der Nutzung unsicherer Umgebungen (INF.9.A11 - CIA)

Sofern der Mitarbeitende die Mindestkriterien aus dem Abschnitt "Geeignete Auswahl und Nutzung eines mobilen Arbeitsplatzes" dieser Sicherheitsrichtlinie nicht erfüllen kann, sollte mobiles Arbeiten für diesen Mitarbeiter nicht freigegeben.