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

Sicherheitsrichtlinie "Mobile Endgeräte und Datenträger"

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 | ISMS300033 | [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](#_Toc81034670)

[Dokumentenhistorie 3](#_Toc81034671)

[Inhaltsverzeichnis 4](#_Toc81034672)

[Allgemeine Festlegungen 5](#_Toc81034673)

[Ziel / Zweck 5](#_Toc81034674)

[Geltungsbereich 6](#_Toc81034675)

[Zuständigkeiten 6](#_Toc81034676)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81034677)

[Aufbau des Dokuments 6](#_Toc81034678)

[Sicherheitsrichtlinie „Mobile Endgeräte und Datenträger" 8](#_Toc81034679)

[Basismaßnahmen 8](#_Toc81034680)

[Mobiletelefon 8](#_Toc81034681)

[Allgemeine Smartphones und Tablets 8](#_Toc81034682)

[iOS (for Enterprise) 10](#_Toc81034683)

[Android 11](#_Toc81034684)

[Wechseldatenträger 11](#_Toc81034685)

[Standardmaßnahmen 12](#_Toc81034686)

[Mobiletelefon 12](#_Toc81034687)

[Allgemeine Smartphones und Tablets 13](#_Toc81034688)

[iOS (for Enterprise) 15](#_Toc81034689)

[Android 17](#_Toc81034690)

[Wechseldatenträger 18](#_Toc81034691)

[Maßnahmen bei erhöhtem Schutzbedarf 19](#_Toc81034692)

[Mobiletelefon 19](#_Toc81034693)

[Allgemeine Smartphones und Tablets 20](#_Toc81034694)

[iOS (for Enterprise) 21](#_Toc81034695)

[Android 22](#_Toc81034696)

[Wechseldatenträger 22](#_Toc81034697)

# Allgemeine Festlegungen

## Ziel / Zweck

Mobiltelefone, Smartphones, Tablets und Phablets sind durch eine international eindeutige Seriennummer (International Mobile Equipment Identity, IMEI) gekennzeichnet. Die Identifizierung der Benutzer mit ihren Geräten im Mobilfunknetz erfolgt durch die SIM-Karte, die bei Vertragsabschluss vom Mobilfunkanbieter zugeteilt wurde.

Die in diesem Dokument betrachteten Mobiltelefone („Feature-Phones“ oder „Dumbphones“) besitzen weniger Eigenschaften als ein typisches Smartphone, bieten aber mehr Funktionen als nur die reine Telefonfunktion. So können Mobiltelefone zusätzlich mit einer Kamera für Videos und Fotos, einem Terminplaner, E-Mail-Programmen, Spielen, einem MP3-Player oder einem Radioempfänger ausgestattet sein. „Klassische“ Mobiltelefone verfügen in der Regel nicht über einen Touchscreen und ein Betriebssystem, auf das zusätzliche Apps installiert werden können. Diese fehlenden Funktionen unterscheidet das Mobiltelefon von einem Smartphone.

Smartphones hingegen sind Mobiltelefone, die mit einem großen, üblicherweise berührungsempfindlichen Touch-Display ausgestattet sind. Ein Smartphone vereint neben den klassischen Funktionen eines Mobiltelefons Media-Player, Personal Information Manager (PIM) und Digitalkamera in einem Gerät und bieten den Benutzern darüber hinaus viele weitere Anwendungen und Funktionen, wie Web-Browser, E-Mail-Client oder GPS. Zudem sind sie mit Mobilfunk-, WLAN- und Bluetooth-Schnittstellen ausgestattet. Verallgemeinert sind Tablets Smartphones mit großem Formfaktor, mit denen in der Regel nicht über das Mobilfunknetz telefoniert werden kann. Phablets sind im eigentlichen Sinne Hybridgeräte aus Smartphone und Tablet. Phablets werden in dieser Sicherheitsrichtlinie nicht gesondert hervorgehoben.

Wechseldatenträger werden eingesetzt, um Daten zu transportieren, zu speichern oder um mobil auf sie zugreifen zu können. Zu Wechseldatenträger gehören externe Festplatten, CD-ROMs, DVDs, BluRays, Speicherkarten und USB-Sticks. Die Eingruppierung in Klassen von Datenträgen unterscheidet, ob die Datenträger nur lesbar, einmalig beschreibbar oder wiederbeschreibbar sind.

Ziel dieser Sicherheitsrichtlinie ist es, den Verantwortlichen für die Sicherheit und dem Betrieb Informationen zu den typischen Gefährdungen für Smartphones, Tablets und Wechseldatenträgern zu geben. Außerdem sollen den Verantwortlichen Ansätze aufgezeigt werden, um schutzbedarfsgerechte Konfigurationsprofile zu erstellen.

Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben der BSI Bausteine SYS.3.3 "Mobiltelefon", SYS.3.2.1 "Allgemeine Smartphones und Tablets", SYS.3.2.3 "iOS (for Enterprise)" und SYS.3.2.4 "Android" und SYS.4.5 "Wechseldatenträger" 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

Die Sicherheitsrichtlinie „Mobile Endgeräte und Datenträger“ 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 „Mobile Endgeräte und Datenträger"

## Basismaßnahmen

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

### Mobiletelefon

#### Sperrmaßnahmen bei Verlust eins Mobiltelefons (SYS.3.3.A2)

Bei Verlust eines Mobiltelefons ist die verwendete SIM-Karte zeitnah zu sperren. Falls möglich, sollten vorhandene Mechanismen zum Diebstahlschutz, wie Fernlöschung oder -sperrung, genutzt werden. Alle notwendigen Informationen zur Sperrung von SIM-Karte und Mobiltelefon sind für die Verantwortlichen unmittelbar griffbereit zu sein.

#### Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen (SYS.3.3.A3)

Die Mitarbeitenden mit einem dienstlichen Mobiltelefon sind über die besonderen Gefährdungen der Informationssicherheit zu sensibilisieren. Die Mitarbeitenden müssen die Sicherheitsfunktion der Mobiltelefone falls erforderlich eingewiesen werden. Den Mitarbeitenden mit einem Mobiltelefon muss der Prozess bekannt sein, durch den die Mobiltelefone gesperrt werden können. Die Mitarbeitenden mit einem Mobiltelefon müssen darauf hingewiesen werden, wie das Mobiltelefon sicher und korrekt aufbewahrt werden sollte.

#### Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und darin verwendeter Speicherkarten (SYS.3.3.A4)

Dienstliche Mobiltelefone sind vor der Entsorgung von den Mitarbeitenden auf den Werkszustand zurückzusetzen. Im muss verifiziert werden, ob tatsächlich der Werkszustand aktiv ist und alle bisher vorhandenen Daten und Datenträger (Speicherkarten) gelöscht wurden. Im Rahmen der Entsorgung ist ebenfalls sicherzustellen, dass die dienstlichen Mobiltelefone und eventuell darin verwendete Speicherkarten ordnungsgemäß entsorgt werden. Falls die Mobiltelefone und Speicherkarten erst zu einem späteren Zeitpunkt beziehungsweise in größerer Anzahl entsorgt werden, sind die alle gesammelten Mobiltelefone und alle Speicherkarten vor unberechtigtem Zugriff zu schützen.

### Allgemeine Smartphones und Tablets

#### Festlegung einer Strategie für Smartphones und Tablets (SYS.3.2.1.bd.A1)

Bevor Smartphons oder Tablets den Mitarbeitenden zur Verfügung gestellt, betrieben oder eingesetzt werden, ist die generelle Strategie im Hinblick auf die Nutzung und Kontrolle der Endgeräte festzulegen. In diesem Zusammenhang ist zu regeln, wer auf welche Informationen zugreifen darf. Hierbei sind die Vorgaben des Standards „Klassifizierung von Informationen“ zu beachten.

#### Festlegung einer Strategie für den Cloud-Einsatz (SYS.3.2.1.A2)

Die <Institution> definiert für mobile Endgeräte eine generelle Strategie für die Cloud-Nutzung, Informationskontrolle und den Schutz der Informationen. Der Zugriff und die Nutzung von Cloud-Diensten durch die Mitarbeitenden und Externen ist zu klären und festzulegen. Die Mitarbeitenden sind regelmäßig hinsichtlich des Einsatzes von Cloud-Diensten zu schulen.

#### Sichere Grundkonfiguration für mobile Endgeräte (SYS.3.2.1.A3)

Alle mobilen Endgeräte sind so zu konfigurieren, dass die Smartphones und Tablets das erforderliche Schutzniveau angemessen erfüllen. Hierfür ist eine passende Grundkonfiguration der Sicherheitsmechanismen und -einstellungen zusammenzustellen und zu dokumentieren. Nicht benötigte Funktionen sollten deaktiviert werden. Die Freischaltung von Kommunikationsschnittstellen ist zu regeln und muss auf das dienstlich notwendige Maß reduziert werden.

Bei der sicheren Grundkonfiguration sind die Vorgaben der Sicherheitsrichtlinie "Mobile Device Management (MDM)" zu berücksichtigten. Bei der Übergabe des Smartphones oder Tablets an den Mitarbeitenden muss bereits der MDM-Client installiert sein.

#### Verwendung eines Zugriffschutzes (SYS.3.2.1.A4)

Alle Smartphones und Tablets der <Institution> sind mit einem angemessen komplexen Gerätesperrcode zu schützen. Die Mitarbeitenden sind verpflichtet die Bildschirmsperre einzusetzen. Die Anzeige von vertraulichen Informationen auf dem Sperrbildschirm ist zum Schutz von vertraulichen Informationen zu deaktivieren. Alle Smartphones und Tablets sind so zu konfigurieren, dass nach wenigen Minuten Inaktivität des Gerätes eine automatische Bildschirmsperre erfolgt. Die Zeitspanne bis die Bildschirmsperre aktiv wird, ist angemessen in Abhängigkeit vom Use-Case und dem Schutzbedarf der Daten auf dem Smartphone oder Tablet festzulegen.

Nach einer definierten Anzahl von fehlgeschlagenen Anmeldeversuchen am gesperrten Smartphone oder Tablet erfolgt eine Zurücksetzung auf den Werkzustand. Im Zuge des Zurücksetzens auf den Werkszustand sind die Daten der <Institution> sowie alle Einstellungsparameter und Verschlüsselungsschlüssel sicher zu vernichten.

Die Mitarbeitenden sollten bei einem Passwortwechsel Kennworte nutzen, die der Empfehlung "Umgang mit Passwörtern" entsprechen. Die Anzahl der Kennwörter, nachdem sich ein Passwort wiederholen darf, sind vom Sicherheitsmanagement der <Institution> festzulegen.

#### Updates von Betriebssystem und Apps (SYS.3.2.1.A5)

In der Sicherheitsrichtlinie "Patch- und Änderungsmanagement" wird der Umgang mit Patchen und Updates übergreifend für die <Institution> und deren Töchter dokumentiert. Für Smartphones und Tablets ist ein Prozess für die Aktualisierung der Betriebssysteme und der eingesetzten Apps zu etablieren. Aktualisierungen sind vor der produktiven Freigabe geeignet zu testen. Nach der Freigabe sind die Aktualisierungen zeitnah auszurollen.

Bei der Auswahl von zu beschaffenden Smartphones und Tablets sind für die anvisierte Nutzungsdauer die Supportzeiträume der Hersteller bereits in der Auswahl zu berücksichtigen. Ebenfalls ist bei der Auswahl von zu beschaffenden Smartphones und Tablets der benötigte Supportaufwand für die Bereitstellung von Betriebssystem und App-Aktualisierungen zu berücksichtigen.

Ältere Endgeräte, für die keine aktuellen Versionen der Betriebssysteme und Apps mehr bereitgestellt werden, sind auszusondern und durch geeignete Geräte zu ersetzen.

#### Datenschutzeinstellungen (SYS.3.2.1.A6)

Der Zugriff von Apps und dem Betriebssystem auf Daten und Schnittstellen des Smartphones und Tablets ist angemessen einzuschränken. Die Datenschutzeinstellungen sind unter der Berücksichtigung der Benutzbarkeit und dem zugrundeliegenden Use-Case so restriktiv wie möglich zu konfigurieren. Insbesondere der Zugriff auf Kameras, Mikrofone und Geodaten ist konform mit den gesetzlichen und organisationsinterne Datenschutz- und Sicherheitsvorgaben zu konfigurieren.

#### Verhaltensregeln bei Sicherheitsvorfällen (SYS.3.2.1.A7)

Generell sind alle Sicherheitsvorfälle entsprechend den Regelungen der <Institution> zu melden und werden auf Basis den Vorgaben aus der Sicherheitsrichtlinie "Behandlung von Sicherheitsvorfällen" behandelt. Gehen Smartphones oder Tablets verloren oder werden unberechtigte Änderungen am Gerät und Software festgestellt, sind durch die Verantwortlichen sofort geeignete Gegenmaßnahmen einzuleiten.

Die möglichen Konsequenzen sicherheitskritischer Ereignisse sind zeitnah zu untersuchen. Es sind grundsätzlich alle erforderlichen Schutzmaßnahmen zu ergreifen, damit nicht auf vertrauliche und geschäftskritische Informationen zugegriffen werden kann.

#### Keine Installation von Apps aus unsicheren Quellen (SYS.3.2.1.A8)

Es ist technisch zu unterbinden, dass sich auf dem Smartphone oder Tablet Apps aus alternativen App-Stores oder aus dem Dateisystem oder aus Dateianhängen installieren lassen.

### iOS (for Enterprise)

#### Strategie für die iOS-Nutzung (SYS.3.2.3.A1)

Die Strategie der <Institution> für die Nutzung iPhones und iPads im Enterprise-Umfeld basiert auf einer zentralen Mobile Device Management (MDM) Lösung. Die zentral verwalteten iPhones und iPads sind mittels dem Apple Device Enrollment Program (DEP) über den Apple Business Manager in die MDM-Infrastruktur zu integrieren.

Für eine kleine einstellige Anzahl von iPhones oder iPads besteht die Möglichkeit, bei entsprechender Begründung von einer zentralen MDM-basierten Verwaltung abzuweichen.

Die Strategie zur Nutzung von iPhones und iPads sieht eine geeignete Geräteauswahl inklusive Proof of Concept (PoC) vor. Sofern die vom iPhone oder iPad verarbeiteten Daten nicht zentral gespeichert werden, ist eine Datensicherung gemäß Sicherheitsrichtlinie "Datensicherung" zu etablieren.

Zusätzliche Apps von Drittanbietern sind ausschließlich nach Tests und Freigaben im Rahmen von Volumenlizenzen (VPP) über das MDM zum Download anzubieten.

#### Planung des Einsatzes von iCloud-Diensten (SYS.3.2.3.A2)

Da die iOS-basierten Endgeräte eng mit den iCloud-Diensten des Herstellers Apple verzahnt sind definiert die [Institutionsname] folgende Regelungen zur Nutzung von Cloud-Diensten bei mobilen Endgeräten:

* Auf die Aktivierung der Endgeräte mit einer persönlichen Apple ID ist zu verzichten, indem das Apple-Programm zur Endgeräteregistrierung (Device Enrollment Program, DEP) genutzt wird.
* Auf die Nutzung der Aktivierungssperre ist zu verzichten, um die Verknüpfung der Cloud-Dienste mit der personalisierten Apple ID zu vermeiden.
* Es ist mit dem <Informationssicherheitsbeauftragter> und <Datenschutzbeauftragter> abzustimmen, welche Cloud-Services in welchem Umfang durch die Mitarbeitenden genutzt werden können.

#### Verhinderung des unautorisierten Löschens von Konfigurationsprofilen (SYS.3.2.3.A7)

Es sind durch die Verantwortlichen für den Betrieb des MDM der <Institution> geeignete Regelungen zur Vermeidung der unautorisierten Löschung von Konfigurationsprofilen zu treffen und zu etablieren. Im Rahmen von Schulungen sind die Mitarbeitenden mit geschäftlichen iPhones und iPads über den Zweck der etablierten Sicherheitsmaßnahmen zu sensibilisieren.

### Android

#### Auswahl von Android-basierten Geräten (SYS.3.2.4.A1)

Bei der Auswahl von Smartphones und Tablets mit dem Betriebssystem Android ist sicherzustellen, dass der Hersteller regelmäßig Sicherheitsupdates für dieses Gerät bereitstellt und sich der Supportzeitraum der von der <Institution> angedachten Nutzungsdauer annähert sowie, dass die Geräte durch ein MDM verwertbar ist.

Das Smartphone oder Tablet ist direkt mit einer aktuellen Version von Android zu beschaffen oder im Rahmen der Inbetriebnahme auf die neueste intern freigegebene Version von Android zu aktualisieren.

### Wechseldatenträger

#### Sensibilisierung der Mitarbeiter zum sicheren Umgang mit Wechseldatenträgern (SYS.4.5.A1)

Alle Mitarbeitenden sind im Rahmen des etablierten Schulungsprogramms für den sicheren Umgang mit Wechseldatenträgern sensibilisieren und zu informieren, dass keine Wechseldatenträger aus unbekannten Quellen an die übergebenen Geräte der <Institution> angeschlossen werden dürfen.

Ein weiteres Thema für die Schulung der Mitarbeitenden ist das Verhalten im Umgang mit den Wechseldatenträgern, um einem Verlust oder Diebstahl vorzubeugen und eine lange Lebensdauer zu gewährleisten.

#### Verlust- bzw. Manipulationsmeldung (SYS.4.5.A2)

Der Verlust oder Diebstahl der von der <Institution> bereitgestellten Wechseldatenträger oder der Verdacht einer Manipulation ist unverzüglich an den <Informationssicherheitsbeauftragter> und <Datenschutzbeauftragter> sowie an den Service Desk zu melden und durch den <Informationssicherheitsbeauftragter> als Sicherheitsvorfall weiter zu bearbeiten.

Der Mitarbeitende muss bei seiner Meldung angeben, welche Informationen auf dem Wechseldatenträger gespeichert waren.

#### Schutz vor Schadsoftware (SYS.4.5.A12)

Zur Vermeidung, dass durch Wechseldatenträger der <Institution> Schadsoftware verbreitet wird, dürfen nur auf Malware überprüfte Daten auf den Wechseldatenträger übertragen werden. Bevor Daten von Wechseldatenträgern verarbeitet bzw. auf andere Systeme kopiert werden, sind die Daten ebenfalls auf Schadsoftware zu überprüfen.

## Standardmaßnahmen

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

### Mobiletelefon

#### Nutzung der Sicherheitsmechanismen von Mobiltelefonen (SYS:3.3.A5)

Die verfügbaren Sicherheitsmechanismen auf den dienstlichen Mobiltelefonen sollten genutzt und vorkonfiguriert werden. Die SIM-Karte sollte durch eine PIN geschützt werden. Das dienstliche Mobiltelefon sollte durch einen Zugangscode geschützt werden. Sofern möglich, sollte mittels SIM-Lock das dienstliche Mobiltelefon an die SIM-Karte gebunden werden. Die Mitarbeitenden mit einem dienstlichen Mobiltelefon sind über die aktivierten Sicherheitsmechanismen zu informieren.

#### Updates von Mobiltelefonen (SYS.3.3.A6)

Die Mitarbeitenden müssen regelmäßig prüfen, ob es Softwareupdates für das dienstliche Mobiltelefon gibt. Sofern seitens des Verantwortlichen für die Sicherheit und den Betrieb keine anders lautenden Empfehlungen gibt, sollen die Mitarbeitenden die Updates für das dienstliche Mobiltelefon selber installieren.

#### Beschaffung von Mobiltelefonen (SYS.3.3.A7)

Bevor dienstliche Mobiltelefone beschafft werden, sollte eine Anforderungsliste erstellt werden. Anhand der Anforderungsliste sind die am Markt erhältlichen Produkte zu bewerten und auszuwählen. Seitens des Herstellers oder eines vertraglich gebundenen Dienstleisters sollte gewährleistet werden, dass Ersatzteile wie Akkus und Ladegeräte in ausreichender Qualität für den vorgesehenen Lebenszyklus nachbeschafft werden können.

#### Nutzung drahtloser Schnittstellen von Mobiltelefonen (SYS.3.3.A8)

Die drahtlosen Schnittstellen (IrDA, WLAN und Bluetooth) der dienstlichen Mobiltelefone sollten sofern nicht benötigt deaktiviert werden.

#### Sicherstellung der Energieversorgung von Mobiltelefonen (SYS.3.3.A9)

Es sollten seitens der Mitarbeitenden angemessene Maßnahmen getroffen werden, um die Energieversorgung der dienstlichen Mobiltelefone sicherzustellen. Als Vorsorge kann bei Bedarf der Einsatz von Wechselakkus oder Powerbanks geprüft werden.

#### Sichere Datenübertragung über Mobiltelefone (SYS.3.3.A10)

Die zu übertragenden Daten sind mittels den von der <Institution> freigegebenen Verschlüsselungsprotokollen abzusichern.

#### Ausfallvorsorge bei Mobiltelefonen (SYS.3.3.A11)

Die auf einem dienstlichen Mobiltelefon gespeicherten Daten sollten in regelmäßigen Abständen auf einem externen Medium gesichert werden. Sofern ein defektes Mobiltelefon repariert werden muss, sind zuvor alle Daten zu löschen und das Mobiltelefon auf den Werkszustand zurückzusetzen. Um ein defektes Mobiltelefon kurzfristig zu ersetzen, sollten Seitens der <Institution> Ersatzgeräte vorgehalten werden.

#### Einrichtung eines Mobiltelefon-Pools (SYS.3.3.A12)

Bei häufig wechselnden Benutzern der dienstlichen Mobiltelefone sollte eine Mobiltelefon-Pool eingerichtet werden. Die Ausgabe und Rücknahme von Mobiltelefonen und Zubehör sollte dokumentiert werden. Vor der Ausgabe sollte sichergestellt werden, dass die Mobiltelefone aufgeladen und mit den nötigen Programmen und Daten für den neuen Benutzer ausgestattet sind. Bei der Ausgabe sollte der Mitarbeitende informiert werden, wie die Mobiltelefone aufzubewahren sind. Zudem sollte der Mitarbeiter auf die Einhaltung der Sicherheitsvorgaben der <Institution> hingewiesen werden. Nachdem das Mobiltelefon vom Mitarbeitenden wieder zurückgegeben wurden, sollten alle Daten gelöscht und das Mobiltelefon auf den Werkszustand zurückgesetzt werden.

### Allgemeine Smartphones und Tablets

#### Restriktive Nutzung von funktionalen Erweiterungen (SYS.3.2.1.A9)

Funktionale Erweiterungen sollten ausschließlich restriktiv genutzt werden. Sofern funktionalen Erweiterungen eingesetzt werden, sind automatische Zugriffe auf schützenswerte Informationen zu unterbinden. Die festgelegten Grundkonfiguration dürfen durch die funktionalen Erweiterungen auf dem Smartphone oder Tablet nicht umgangen oder abgeändert werden.

#### Richtlinie für Mitarbeiter zur Benutzung von mobilen Endgeräten (SYS.3.2.1.A10)

Im Standard „Benutzer“ werden übergreifende Vorgaben für die Mitarbeitenden der <Institution> festgelegt. Die Inhalte dieser Richtlinie erweitern den Kontext um die Thematik Smartphones, Tablets und Wechseldatenträger. Dadurch wird garantiert, dass die Smartphones und Tablets wie gewünscht durch die Mitarbeitenden genutzt und gepflegt werden. Regelungen zur Aufbewahrung und Verlustmeldungen sind für alle Smartphones, Tablets und Datenträger gleichermaßen festzulegen. Die installierte Verwaltungssoftware auf dem Smartphone und Tablet darf durch den Mitarbeitenden nicht deinstalliert werden und das eigenmächtige „rooten“ des Smartphones oder Tablets ist untersagt.

#### Verschlüsselung des Speichers (SYS.3.2.1.A11)

Der nichtflüchtige Speicher der Smartphones und Tablets sowie eventuell vorhandene SD-Karten sind zu verschlüsseln. Hierbei ist zu beachten, dass nur die intern freigegebenen kryptographischen Verfahren und deren Protokolle und Werte angewendet werden.

#### Verwendung nicht personalisierter Endgerätenamen (SYS.3.2.1.A12)

Wird ein Smartphone oder Tablet zum Laden mit einem Notebook oder einer Workstation gekoppelt oder ein öffentliches WiFi-Netz genutzt oder die Ortungsdienste für eine WebApp freigegeben wird automatisch der Gerätename angezeigt bzw. übertragen. Dies ermöglicht so Rückschlüsse auf den Besitzer des Smartphones oder Tablets. Um zu verhindern, dass unter Umständen der Benutzer und der Passcode des Gerätes erraten werden können und um die Anforderungen aus dem Datenschutz zu erfüllen, darf der Name des Smartphones oder Tablets keine persönlichen Namens- oder <Institution>-Merkmale enthalten sondern besteht aus der sechsstelligen <Institution>-Inventarnummer.

#### Regelungen zum Screensharing und Casting (SYS.3.2.1.A13)

Screensharing oder Casting können seitens der Mitarbeitenden und den von der <Institution> freigegeben Apps je nach Anforderungslage eingesetzt werden. Beim Screensharing oder Casting ist durch den Mitarbeitenden die Vertraulichkeit der Informationen des geteilten Dokumentes und der Inhalte des Gespräches zu beachten. Dies gilt insbesondere, wenn Videokonferenzen aufgezeichnet werden und somit potentiell durch den Videokonferenzbetreiber ausgewertet werden können.

#### Schutz vor Phishing und Schadprogrammen im Browser (SYS.3.2.1.A14)

Alle Smartphones und Tablets sind unter Berücksichtigung der Anforderungen aus der Sicherheitsrichtlinie „Schutz vor Schadprogrammen“ in die etablierte Malware-Detection und Prevention Infrastruktur der <Institution> zu integrieren. Sofern die vorhandenen Browser auf dem Smartphone oder Tablet die Funktion "Safe Browsing" anbieten sollte ist diese zu aktivieren bzw. alternative Funktion zur Warnung vor schädlichen Inhalten zu aktivieren.

#### Deaktivierung von Download-Boostern (SYS.3.2.1.A15)

Download-Booster in Apps auf dem Smartphone oder Tablet, welche die Daten beim Download über die Server des Download-Booster-Herstellers leiten, sind zu deaktivieren.

#### Deaktivierung nicht benutzter Kommunikationsschnittstellen (SYS.3.2.1.A16)

Kommunikationsschnittstellen der Smartphones und Tablets sollten nur bei Bedarf und nur in geeigneten Umgebungen aktiviert werden. Sofern der Schutzbedarf der Informationen auf dem Smartphone oder Tablet oder deren Umgebung es erfordert, sind die Kommunikationsschnittstellen zentral über das MDM der <Institution> zu verwalten.

#### Verwendung der SIM-Karten-PIN (SYS.3.2.1.A17)

Die Nutzung der von der <Institution> gestellten SIM-Karte wird durch eine PIN geschützt. Die Super-PIN/PUK wird ausschließlich im Rahmen der definierten Anwendungsfälle von den Mitarbeitenden benutzt.

#### Verwendung biometrischer Authentisierung (SYS.3.2.1.A18)

Die Nutzung von biometrischen Verfahren zur Authentisierung (z. B. Fingerabdrucksensor oder Gesichtserkennung) bei Smartphones und Tablets, ist je Gerättyp und Betriebssystem unter Beachtung des Use-Cases, der Benutzbarkeit und des tatsächlich benötigten Schutzbedarfes zu prüfen. Insbesondere ist zu prüfen, ob ein ähnlicher oder höherer Schutz als mit dem klassischen Gerätepasswort erzielt werden kann. Im Zweifelsfall oder bei einem schlechteren Schutz sind biometrische Verfahren zentral unter Verwendung des MDM der <Institution> zu verhindern. Die Mitarbeitenden sollten für die Fälschbarkeit von biometrischen Merkmalen sensibilisiert werden.

#### Verwendung eines Sprachassistenten (SYS.3.2.1.A19)

Da Sprachassistenten alle Informationen auf die Server des Herstellers übertragen, sollten Sprachassistenten nur eingesetzt werden, wenn diese zwingend notwendig sind. Andernfalls sollten die Sprachassistenten deaktiviert werden. Sofern das Smartphone oder Tablet gesperrt ist, sollte der Sprachassistent nicht genutzt werden können. Dies wird idealerweise durch das MDM der <Institution> technisch unterstützt.

#### Auswahl und Freigabe von Apps (SYS.3.2.1.A20)

Apps aus öffentlichen App-Stores sowie WebApps sind durch die Verantwortlichen innerhalb der <Institution> zu prüfen und erst nach bestandener Prüfung freizugeben. Im etablierten Freigabeprozess sind geeignete Bewertungskriterien für die App-Freigaben zu definieren. Alle freigegebenen Apps sind intern in einem Standardkatalog zu veröffentlichen.

#### Definition der erlaubten Informationen und Applikationen auf mobilen Endgeräten (SYS.3.2.1.A21)

Die Mitarbeitenden sollten bei der Übergabe Smartphone oder Tablets erläutert bekommen, welche Informationen der Mitarbeiter auf dem Smartphone oder Tablet speichern oder bearbeiten darf. Die Grundlage für die Regelung bilden die Sicherheitsrichtlinie „Klassifikation von Informationen“, der Standard „Benutzer“ und diese Richtlinie.

Die Mitarbeitenden dürfen nur freigegebene und geprüfte Apps aus als sicher klassifizierten Quellen installieren. Die freigegebenen Apps sind durch das MDM der <Institution> im Rahmen der zentralen Verwaltung bereitzustellen.

#### Einbindung der Endgeräte in die interne Infrastruktur via VPN (SYS.3.2.1.A22)

Sofern Smartphones oder Tablets Zugriff auf interne Infrastrukturen der <Institution> benötigen, erfolgt dies nur mittels kryptographisch abgesicherter Protokolle (VPNs). Vorgaben zum Einsatz von VPN gehen aus der Sicherheitsrichtlinie „VPN“ hervor. Die Authentisierung ist bevorzugt durch Zertifikate statt durch den Einsatz klassischer Passworten zu implementieren und zu betreiben.

#### Verwendung der Filteroption für Webseiten (SYS.3.2.1.A28)

Sofern ein Reputationsdienst oder ein Proxy-Server verwendet, sollte dieser als globaler HTTP-Proxy für alle installierten Browser auf dem Smartphone oder Tablet hinterlegt werden. Ist der etablierte Proxy nur im internen Netz erreichbar, ist Smartphone oder Tablet des Mitarbeitenden über eine VPN-Verbindung wahlweise permanent oder Apps basierend geeignet einzubinden.

Können die Smartphones oder Tablets nicht in eine vorhandene Proxy- oder Reputations-Infrastruktur eingebunden werden, sind für die Filteroptionen der installierten Web-Browser auf Basis von Whitelists oder Blacklists oder Inhaltsfilter Dritter zu aktivieren und zu verwenden.

### iOS (for Enterprise)

#### Verwendung biometrischer Authentisierung (SYS.3.2.3.A10)

Bei Geräten der Firma Apple mit Funktionen zur biometrischen Authentisierung ist zur Erhöhung der Benutzbarkeit alternativ zur Entsperrung des Smartphones oder Tablets die „Touch ID“ oder „Face ID“ freizugeben, wenn gleichzeitig technisch sichergestellt ist, dass die Mitarbeitenden komplexere Gerätecodes verwenden. Einhergehend mit der Aktivierung von „Touch ID“ oder „Face ID“ sollten die Mitarbeitenden für die Fälschbarkeit von biometrischen Merkmalen sensibilisiert werden.

#### Verwendung nicht personalisierter Gerätenamen (SYS.3.2.3.A11)

Um zu verhindern, dass unter Umständen der Benutzer und der Passcode des Gerätes erraten werden können und um die Anforderungen aus dem Datenschutz zu erfüllen, darf der Name des Smartphones oder Tablets keine persönlichen Namens- oder <Institution>-Merkmale enthalten, sondern besteht aus der sechsstelligen <Institution>-Inventarnummer.

#### Verwendung von Apple-IDs (SYS.3.2.3.A12)

In den allgemeinen Geschäftsbedingungen schließt die Firma Apple die Möglichkeit der Übertragung der Apple-ID an einen anderen Mitarbeitenden aus. Zum Zwecke der Notfallvorsorge vor Verlust geschäftlicher Daten, die auf dem Smartphone oder Tablet selbst oder in der iCloud gespeichert sind und der Möglichkeit der Weiterverwendung von bereits bezahlten App's sind <Institution>-bezogene Apple-IDs zu verwenden. Hierzu ist es erforderlich, dass das Smartphone mittels des Apple Business Managers in DEP und VPP aufgenommen und an das MDM der <Institution> angebunden wird.

#### Verwendung der Konfigurationsoption "Einschränkungen unter iOS" (SYS.3.2.3.A13)

Um die Vertraulichkeit und Integrität der verarbeiteten bzw. auf dem Smartphone oder Tablet gespeicherten Daten sicherzustellen, sind alle nicht benötigten oder nicht erlaubten Funktionen oder Dienste zu deaktivieren.

Für mindestens den Sperrbildschirm, die Unified Communication, Siri, das Hintergrundbild, die Verbindung mit Host-Systemen und die Diagnose- und Nutzungsdaten ist basierend auf dem Einsatzzweck und dem Schutzbedarf der Daten auf dem Smartphone oder Tablet zu entscheiden, ob der Dienst oder die Funktion eingeschränkt oder komplett deaktiviert werden muss.

#### Verwendung der iCloud-Infrastruktur (SYS.3.2.3.A14)

Durch die Firma Apple wird allen Mitarbeitenden mit einer Apple-ID die iCloud-Infrastruktur zur Verfügung gestellt. So besteht zum Beispiel die Möglichkeit, über die iCloud-Infrastruktur Dokumente und Fotos zu teilen oder macOS-basierte und iOS-basierte Endgeräte um Continuity-Funktionen zu erweitern.

Die Freigabe der umfänglichen oder selektiven Nutzung der iCloud-Infrastruktur ist anhand der Vereinbarkeit der allgemeinen Geschäftsbedingungen der Firma Apple mit den internen Richtlinien hinsichtlich Verfügbarkeit, Vertraulichkeit, Integrität und Datenschutz zu bewerten. Sofern die Nutzung der iCloud-Infrastruktur für Smartphones und Tablets freigegeben wird, muss die Authentisierung am iCloud-Webservice durch eine Zwei-Faktor-Authentisierung erfolgen. Durch die Verwendung verwalteter Apps kann die iCloud-Nutzung für einen rein dienstlichen Bedarf zusätzlich auf ein geringes Maß reduziert oder komplett ausgeschlossen werden.

#### Verwendung der Continuity-Funktionen (SYS.3.2.3.A15)

Sofern die Nutzung der iCloud-Infrastruktur nicht grundsätzlich untersagt ist, erfolgt eine Einzelfallbewertung der Vereinbarkeit der Continuity-Funktionen (AirDrop und Handoff) mit den internen Richtlinien unter Berücksichtigung der Aspekte Vertraulichkeit und Integrität. Auf Basis der Bewertungsergebnisse wird geregelt, inwieweit diese Funktionen technisch einzuschränken.

#### Verwendung der Endgerätecode-Historie (SYS.3.2.3.A17)

Um die Vertraulichkeit des verwendeten Passcodes zu wahren und zu schnelle Wiederholungen vom Mitarbeitenden verwendete Passcode zu verhindern, ist im Konfigurationsprofil die Anzahl der eindeutigen Codes bis zur ersten Wiederholung festzulegen. Der zu konfigurierende Wert folgt den Empfehlungen aus dem Dokument „Umgang mit Passwörtern“.

#### Verwendung der Konfigurationsoption für den Browser Safari (SYS.3.2.3.A18)

Der Browser "Safari" ist in iOS tief integriert und besitzt gegenüber den aus dem App-Store installierten Browsern anderer Anbieter teils höhere Rechte. Daher sind technische und organisatorische Maßnahmen zu etablieren, um den benötigten Schutz der Daten auf dem Smartphone oder Tablet sicherstellen zu können. Um den Mitarbeitenden der <Institution> ein einheitliches Benutzerempfinden garantieren zu können sollten die Einstellungen der Browser auf Workstations bzw. Notebooks adaptiert werden.

#### Einbindung der Endgeräte in die interne Infrastruktur via VPN (SYS.3.2.3.A20)

Um die Vertraulichkeit und Integrität der Daten auf dem Smartphone oder Tablet zu wahren, sind diese mittels VPN in die Infrastruktur zu integrieren.

In Abhängigkeit von Schutzbedarf, Zweck und technischen Möglichkeiten des VPN-Servers ist eine VPN-Verbindung auf Basis der Technologien IPSec mit IKEv2 oder TLS unter Berücksichtigung der intern freigegeben Parameter zu realisieren. Die Authentisierung ist bevorzugt durch Zertifikate statt durch den Einsatz klassischer Passwörter zu implementieren und zu betreiben.

#### Freigabe von Apps und Einbindung des Apple App Stores (SYS.3.2.3.A21)

Sofern zusätzliche Apps von den Mitarbeitenden auf ihrem Smartphone oder Tablet benötigt werden, wird durch die Verantwortlichen des internen Software-Freigabeprozess dies unterstützt. Im Rahmen der Validierung und Freigabe von Anwendungen wird hierzu bevorzugt auf Apps aus dem VPP zurückgegriffen. Alle freigegebenen Anwendungen werden intern in einem Standardkatalog veröffentlicht und den Mitarbeitenden mittels des <Institution> MDM zur Verfügung gestellt.

Die Zahlungsbestätigung von Apps im App-Store erfolgen ausschließlich über den Apple-Business-Manager für alle in die MDM Infrastruktur integrierten Smartphones und Tablets. Sofern ein Apple-Device nicht in die MDM Infrastruktur integriert ist, sollte die Freigabe der Bezahlung im App-Store nicht durch ein biometrisches Merkmal "Touch ID" oder "Face ID" erfolgen.

### Android

#### Deaktivieren der Entwickler-Optionen (SYS.3.2.4.A2)

Die Entwickleroptionen ist in allen Smartphones und Tablets mit dem Betriebssystem Android zu deaktivieren.

#### Einsatz des Multi-User- und Gäste-Modus (SYS.3.2.4.A3)

Jedes Benutzerkonto auf dem Smartphone oder Tablet muss einer natürlichen Person entsprechen. Sofern das Smartphone oder Tablet nicht als Pool-Gerät bzw. Team Gerät genutzt wird, sollte der Multi-User- und Gäste-Modus nicht verwendet werden.

#### Regelung und Konfiguration von Cloud-Print (SYS.3.2.4.A4)

Der Google Beta-Service Cloud-Print wurde zum 31.12.2020 eingestellt. Daher wird dieser Service nicht freigegeben.

#### Erweiterte Sicherheitseinstellungen (SYS.3.2.4.A5)

Es dürfen sich nur freigegebene Sicherheits-Apps als Geräteadministrator oder „Trust Agents“ eintragen lassen. Dies sollte durch die Verantwortlichen für das MDM und die Mitarbeitenden regelmäßig überprüft werden.

Über die Einstellungen für "Zugriff auf Nutzungsdaten und Zugriff auf Benachrichtigungen" sind nur erlaubten Apps der Zugriff auf schützenswerte Daten zu ermöglichen/freizugeben.

### Wechseldatenträger

#### Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern (SYS.4.5.A4)

Im Umgang mit Wechseldatenträgern sind folgende grundlegende Aspekte zu berücksichtigen.

* Die Mitarbeitenden können alle von der <Institution> ausgegebenen Wechseldatenträger nutzen.
* Vertrauliche interne Daten und alle Kundendaten dürfen auf einen verschlüsselten Wechseldatenträger gespeichert werden bzw. sind bei einem unverschlüsselten Wechseldatenträger zuvor Datei- oder Ordner-basiert mittels AES-256 zu verschlüsseln,
* Vertrauliche Daten auf den Wechseldatenträgern sind sicher und nicht wiederverstellbar zu löschen.
* Private Wechseldatenträger sollten nicht genutzt werden. Sofern die aktuelle Situation dies jedoch erfordert, ist der private Wechseldatenträger zu verschlüsseln bzw. sind bei einem unverschlüsselten Wechseldatenträger zuvor die Datei oder der Ordner mittels AES-256 zu verschlüsseln.
* Mit externen Mitarbeitenden oder Dienstleistern dürfen vertrauliche Daten nur mittels eines vollverschlüsselten Datenträgers ausgetauscht werden.
* Sofern Daten per Kurier oder einem anderen öffentlichen Versender verschickt werden müssen, ist zuvor sicherzustellen, dass der Wechseldatenträger voll verschlüsselt ist bzw. bei einem unverschlüsselten Wechseldatenträger zuvor die Datei oder der Ordner mittels AES-256 verschlüsselt wurden. Die Haftung bei Verlust des Wechseldatenträger muss vertraglich an das Versandunternehmen bzw. dem Empfänger übergeben werden.
* Wechseldatenträgern sind entsprechend den Herstellerangaben zu verwenden und im Technikraum der <Institution> zu lagern.

Die Einhaltung der Sicherheitsvorgaben für den Umgang mit Wechseldatenträgern sind im Rahmen von internen Audits zu überprüfen und bei Bedarf die Vorgaben auf die aktuellen Bedürfnisse anzupassen.

#### Regelung zur Mitnahme von Wechseldatenträgern (SYS.4.5.A5)

Sofern es das mobile Arbeiten oder der Austausch von Daten vor Ort beim Kunden oder Dienstleister erfordert, kann jeder Mitarbeitende die von der <Institution> ausgegebenen Wechseldatenträger mitnehmen. Beim Umgang mit dem zur Verfügung gestellten Datenträger sind die Anforderungen aus dem vorherigen Abschnitt "Erstellung einer Richtlinie zum sicheren Umgang mit Wechseldatenträgern" zu beachten.

#### Datenträgerverwaltung (SYS.4.5.A6)

Im Rahmen der Datenträgerverwaltung ist zu gewährleisten, dass Wechseldatenträger sachgerecht behandelt, aufbewahrt sowie ordnungsgemäß eingesetzt und transportiert werden. Ebenso ist die sichere Löschung und Vernichtung der Datenträger über die Sicherheitsrichtlinie „Löschen und Vernichten von Informationen“ zu regeln.

#### Sicheres Löschen der Datenträger vor und nach der Verwendung (SYS.4.5.A7)

Bevor Datenträger weitergegeben, wiederverwendet oder ausgesondert werden, sind diese in geeigneter Weise sicher zu löschen.

#### Angemessene Kennzeichnung der Datenträger beim Versand (SYS.4.5.A13)

Sofern Datenträger durch Mitarbeitende versendet werden, sind die Datenträger so zu kennzeichnen, dass der Absender und Empfänger sofort zu identifizieren ist. Die Kennzeichnung der Datenträger bzw. deren Verpackung muss für den Empfänger eindeutig sein. Die Kennzeichnung von Datenträgern mit vertraulichen Daten darf für Außenstehende keine Rückschlüsse auf Art und Inhalte der Informationen zulassen.

## 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).

### Mobiletelefon

#### Schutz vor der Erstellung von Bewegungsprofilen bei der Mobilfunk-Nutzung (SYS.3.3.A13 - C)

Es sollte durch die <Institution> geklärt werden, ob sich die Erstellung von Bewegungsprofilen ihrer Mitarbeitenden durch Dritte negativ auf die <Institution> auswirken kann bzw. als Problem angesehen wird. Sofern dies der Fall ist, sollten Funktion zur Ortung bspw. mittels GPS, WiFi abgeschaltet bzw. APP's mit Tracking-Funktionen verboten werden. Wenn eine Ortung über das Mobilfunknetz verhindert werden soll, sollte das Mobiltelefon abgeschaltet sofern dies nicht ausreichend ist der Akku entfernt oder das Mobiltelefon in einen empfangshindernden Behältnis aufbewahrt werden.

#### Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung (SYS.3.3.A14 - C)

Um zu verhindern, dass die verwendeten Rufnummern bestimmten Mitarbeitenden zugeordnet werden können, sollten Rufnummern für ausgehende Anrufe unterdrückt werden. Außerdem sollten keine SMS und Nachrichten mit der Rufnummer als Identifier versendet werden. Rufnummern von Mobiltelefonen sollten nicht veröffentlicht oder an unbefugte Dritte weitergegeben werden.

#### Schutz vor Abhören der Raumgespräche über Mobiltelefone (SYS.3.3.A15 - C)

Sofern der Schutzbedarf von geschäftskritischen Informationen sehr hoch ist, sollte dafür gesorgt werden, dass keine Mobiltelefone zu vertraulichen Besprechungen und Gesprächen in die entsprechenden Besprechungsräume mitgenommen werden. Die organisatorische Anforderung kann bei Bedarf durch die Implementierung von Mobilfunk-Detektoren technisch unterstützt werden.

### Allgemeine Smartphones und Tablets

#### Zusätzliche Authentisierung für vertrauliche Anwendungen (SYS.3.2.1.A23 - C)

Alle Anwendungen mit vertraulichen Daten sind durch einen zusätzlichen Mechanismus auf Basis von 2FA zu schützen.

#### Einsatz einer geschlossenen Benutzergruppe (SYS.3.2.1.A24 - C)

Das Passwort für den Zugangspunkt (Access Point Name, APN) einer geschlossenen Benutzergruppe sollte komplex sein und im Vorfeld mit dem Mobilfunkanbieter die Anforderungen abgestimmt werden. Die Authentisierung am APN sollte das CHAP-Protokoll nutzen. Sofern nicht CHAP sondern wie im Default PAP genutzt wird, kann die Aushandlung durch Dritte abgehört werden und die Benutzergruppe kann nicht mehr als geschlossen angesehen werden.

#### Nutzung von getrennten Arbeitsumgebungen (SYS.3.2.1.A25 - CIA)

Ist es den Mitarbeitenden erlaubt, dienstliche Geräte auch privat zu nutzen, sind Lösungen für getrennte Arbeitsumgebungen (Container oder Virtualisierung) auf dem Smartphone und Tablet einzusetzen werden. Die zu etablierende Lösung sollte bspw. nach Common Criteria (CC) oder einen CC kompatiblen Standard zertifiziert sein. Dienstliche Daten der <Institution> müssen ausschließlich in der dienstlichen Umgebung verbleiben und verarbeitet werden.

#### Nutzung von PIM-Containern (SYS.3.2.1.A26 - CI)

Informationen auf Smartphone und Tablet sind durch einen PIM-Container zu kapseln. Zusätzlich sollten die Daten durch eine separate Authentisierung und eine vom Betriebssystem unabhängige Daten- und Transportverschlüsselung abgesichert werden.

#### Einsatz besonders abgesicherter Endgeräte (SYS.3.2.1.A27 - CIA)

Sofern der Schutzbedarf der Informationen auf dem Smartphone oder Tablet oder der Use-Case es erfordert, setzt die <Institution> Geräte ein, die für die Verarbeitung von Informationen nach gesetzlichen Informationsschutz-Klassifizierungen zertifiziert sind.

#### Verwendung eines institutionsbezogenen APN (SYS.3.2.1.A29 - C)

Bei Verwendung eines <Institution> spezifischen APNs bildet dieser die Grundlage zur Eingrenzung des erlaubten Geräte-Pools. Alle Smartphones und Tablets, die diesen APN verwenden, erhalten vom Mobilfunk-Provider einen mit der <Institution> abgestimmten IP-Adressenbereich. Zur Vermeidung von Sicherheitsvorfällen, die durch zu kurze Passwörter für die Authentisierung verursacht werden, sind ausschließlich komplexe Passworte mit maximal 64 Stellen mit dem Mobilfunk-Provider zu vereinbaren. Beim Einsatz des <Institution> spezifischen APN ist die Authentisierung auf Basis des Protokolls CHAP zu realisieren.

#### Einschränkung der App-Installation mittels Whitelist (SYS.3.2.1.A30 - CIA)

Bei erhöhtem Schutzbedarf dürfen die Mitarbeitenden nur freigegebene und geprüfte Apps auf den zur Verfügung gestellten Smartphones und Tablets installieren. Die Bereitstellung von Apps muss durch das MDM der <Institution> erfolgen bzw. muss das MDM unbefugt installierte Apps sofort wieder entfernt.

### iOS (for Enterprise)

#### Verwendung der automatischen Konfigurationsprofillöschung (SYS.3.2.3.A23 - CI)

Durch die Verwendung der automatischen Konfigurationsprofillöschung soll sichergestellt werden, dass auch nicht permanent online erreichbare Smartphones oder Tablets ohne Zutun der IT-Verantwortlichen den bisher gewährten Zugang zur Infrastruktur der <Institution> nach Ablauf eines definierten Zeitraums oder an einem bestimmten Tag verlieren. Um sicherzustellen, dass der Mitarbeitende noch im Besitz des übergebenden Smartphones oder Tablets ist, kann diese Methodik bei Bedarf präventiv angewendet werden, da nur ein Zugriff durch das MDM der <Institution> eine Aktualisierung des Löschdatums ermöglicht.

#### Verwendung der Konfigurationsoption für AirPrint (SYS.3.2.3.A25 - CA)

Seitens der Firma Apple wurde die AirPrint-Funktionalität fest in das Betriebssystem eingebaut. Diese Funktion lässt sich nicht grundsätzlich einschalten oder abschalten.

Freigegebene AirPrint-Drucker sind durch ein Konfigurationsprofil dem Mitarbeitenden bereitzustellen. Um zu vermeiden, dass Informationen auf nicht vertrauenswürdigen Druckern durch den Mitarbeitenden ausgedruckt werden können, ist bei sehr hohem Schutzbedarf der Daten sicherzustellen, dass stets alle Kommunikationsverbindungen über die Infrastruktursysteme der <Institution> geführt werden.

#### Keine Verbindung mit Host-Systemen (SYS.3.2.3.A26 - CIA)

Um zu vermeiden, dass Smartphones oder Tablets unautorisiert mit Notebooks, PCs oder ähnlichen IT-Systemen verbunden werden, sollten die Mitarbeitenden ihr Smartphone oder Tablet ausschließlich mit dem MDM der <Institution> verbinden können. Dadurch wird garantiert, dass keine lokalen Datensicherungen mittels iTunes, Finder oder ähnlichen Programmen erstellt werden können. Zusätzlich werden hierdurch Angriffe unter Zuhilfenahme forensischer Mittel stark erschwert oder komplett verhindert.

### Android

#### Einsatz eines Produkts zum Schutz vor Schadsoftware (SYS.3.2.4.A6 - CA)

Alle Smartphones und Tablets mit dem Betriebssystem Android sind in die etablierten Malware-Protection Infrastrukturen der <Institution> zu integrieren.

Sofern unter bestimmten Umständen dies nicht möglich ist, ist sicherzustellen, dass zum Schutz vor Schadsoftware auf diesem Gerät eine entsprechende Anwendung installiert wurde. Es sollte eine Software eingesetzt werden, die in unabhängigen Tests als „sehr gut“ bewertet wurde. Die lokal auf dem Gerät installierte Software ist gemäß dem etablierten Patch- und Änderungsmanagement immer auf dem aktuellen Stand gehalten.

#### Verwendung einer Firewall (SYS.3.2.4.A7 - CA)

Auf allen Smartphones und Tablets mit dem Betriebssystem Android und einem erhöhtem Schutzbedarf ist eine Firewall zu installieren und zu aktivieren bzw. das Gerät permanent in die bereits etablierten Security Infrastrukturen (Firewall, Intrusion Detection System, Intrusion Prevention System, etc.) zu integrieren.

### Wechseldatenträger

#### Datenträgerverschlüsselung (SYS.4.5.A10 - CI)

Sofern auf dem Wechseldatenträger Daten mit vertraulichen Informationen oder Kundendaten gespeichert werden, ist der Datenträger vollständig zu verschlüsseln. Es sind hierfür die intern freigegebenen Verschlüsselungsverfahren zu verwenden.

#### Integritätsschutz durch Checksummen oder digitale Signaturen (SYS.4.5.A11 - I)

Um beim Datenaustausch mittels Wechseldatenträger die Integrität von vertraulichen Informationen sicherzustellen, sind Verfahren zum Schutz gegen zufällige oder vorsätzliche Veränderungen einzusetzen. Dies ist bspw. möglich mittels Checksummen-Verfahren, fehlerkorrigierende Codes, Message Authentication Code (MAC) oder digitale Signaturen. Die Verfahren zum Schutz vor Veränderungen sind auf dem aktuellen Stand der Technik zu halten.

#### Sichere Versandart und Verpackung (SYS.4.5.A14 - C)

Die <Institution> sollte überprüfen, wie vertrauliche Informationen bei einem Versand angemessen geschützt werden können. Sofern Datenträger durch Mitarbeitende versendet werden, sind die Datenträger so zu kennzeichnen, dass der Absender und Empfänger sofort zu identifizieren ist. Die Kennzeichnung der Datenträger bzw. deren Verpackung muss für den Empfänger eindeutig sein. Die Kennzeichnung von Datenträgern mit vertraulichen Daten darf für Außenstehende keine Rückschlüsse auf Art und Inhalte der Informationen zulassen. Die Mitarbeitenden sollten Versandmaterial verwenden, welche es dem Empfänger erleichtert eine Manipulation zu erkennen.

#### Zertifizierte Produkte (SYS.4.5.A15 - CI)

Sofern vertraglich mit Kunden vereinbart, verwendet die <Institution> nur zertifizierte Wechseldatenträger. Bei der Beschaffung von zertifizierten Wechseldatenträgern ist darauf zu achten, dass eine integere Datenerhaltung sowie eine möglicherweise vorhandene Verschlüsselung berücksichtigt sind.

#### Nutzung dedizierter Systeme zur Datenprüfung (SYS.4.5.A16 - CI)

Sofern vertraglich mit Kunden vereinbart, sollte die <Institution> dedizierte Systeme als Datenschleuse verwenden, bei denen Daten von einem Wechseldatenträger auf einen anderen übertragen werden und dabei auf Schadsoftware untersucht werden.