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

Sicherheitsrichtlinie "Mobile Anwendungen (Apps)"

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 | ISMS300047 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Mobile Anwendungen (Apps)" | [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](#_Toc82204943)

[Dokumentenhistorie 3](#_Toc82204944)

[Inhaltsverzeichnis 4](#_Toc82204945)

[Allgemeine Festlegungen 5](#_Toc82204946)

[Ziel / Zweck 5](#_Toc82204947)

[Geltungsbereich 5](#_Toc82204948)

[Zuständigkeiten 5](#_Toc82204949)

[Genehmigungs- und Änderungsverfahren 6](#_Toc82204950)

[Aufbau des Dokuments 6](#_Toc82204951)

[Sicherheitsrichtlinie „Mobile Anwendungen (Apps)" 7](#_Toc82204952)

[Basismaßnahmen 7](#_Toc82204953)

[Anforderungsanalyse für die Nutzung von Apps (APP.1.4.A1) 7](#_Toc82204954)

[Regelungen für die Verwendung von mobilen Endgeräten und Apps (APP.1.4.A2) 7](#_Toc82204955)

[Verwendung sicherer Quellen für Apps (APP.1.4.A3) 7](#_Toc82204956)

[Test und Freigabe von Apps (APP.1.4.A4) 7](#_Toc82204957)

[Minimierung und Kontrolle von App-Berechtigungen (APP.1.4.A5) 8](#_Toc82204958)

[Patchmanagement für Apps (APP.1.4.A6) 8](#_Toc82204959)

[Sichere Speicherung lokaler App-Daten (APP.1.4.A7) 8](#_Toc82204960)

[Verhinderung von Datenabfluss (APP.1.4.A8) 8](#_Toc82204961)

[Standardmaßnahmen 9](#_Toc82204962)

[Zentrales Management von Apps (APP.1.4.A11) 9](#_Toc82204963)

[Sichere Deinstallation von Apps (APP.1.4.A12) 9](#_Toc82204964)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc82204965)

[Entwicklung von Fallback-Lösungen für Apps (APP.1.4.A13 - CIA) 9](#_Toc82204966)

[Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps (APP.1.4.A14 - CI) 10](#_Toc82204967)

[Durchführung von Penetrationstests für Apps (APP.1.4.A15 - CIA) 10](#_Toc82204968)

# Allgemeine Festlegungen

## Ziel / Zweck

Smartphones, Tablets und ähnliche Geräte sind heute ein typisches Arbeitsgerät und ermöglichen durch ihre typischen Einsatzszenarien ein mobiles Arbeiten unabhängig vom eigentlichen Büroarbeitsplatz und Standort.

Mobile Anwendungen (Apps) sind Application, die auf Betriebssystemen wie Apple iOS, Google Android, Microsoft Windows10/11 oder Google Chrom-OS auf entsprechenden Endgeräten installiert und ausgeführt werden. Apps werden üblicherweise aus sogenannten App Stores bezogen. Diese werden von den Herstellern der Betriebssysteme und Endgeräte betrieben und gepflegt. Im professionellen Umfeld ist es aber auch üblich, Apps selbst zu entwickeln und über zentrale Management-Lösungen auf den Endgeräten zu installieren und zu verwalten. Im Vergleich zu Anwendungen auf Desktop-Betriebssystemen unterliegen Apps unter iOS oder Android besonderen Rahmenbedingungen, wie etwa einem durch das Betriebssystem sichergestellten Berechtigungsmanagement.

Für die unterschiedlichen mobilen Betriebssysteme gibt es mittlerweile eine riesige Auswahl an verfügbaren Apps. Auch gibt es standardisierte Bibliotheken und Entwicklungsumgebungen, mit deren Hilfe sich Apps im Vergleich zu klassischen Anwendungen schnell selbst entwickeln lassen.

Diese Sicherheitsrichtlinie benennt Sicherheitsanforderungen für mobile Anwendungen (Apps), die auf Workstations und Notebooks sowie auf Tablets und Smartphones eingesetzt werden. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines APP.1.4 "Mobile Anwendungen (Apps)" 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 Anwendungen (Apps)“ 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 Anwendungen (Apps)"

## Basismaßnahmen

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

### Anforderungsanalyse für die Nutzung von Apps (APP.1.4.A1)

Bevor eine App installiert und genutzt wird, ist unter Einbeziehung der jeweiligen Fachverantwortlichen klar zu definieren, welche Geschäftsprozesse die App unterstützen und an welche IT-Komponenten der <Institution> die App angebunden werden soll. Ferner sind Sicherheitsanforderungen für die App festzulegen. Außerdem sind der vererbte bzw. benötigte Schutzbedarf und die rechtlichen Rahmenbedingungen der zu verarbeitenden Daten zu betrachten.

In der Anforderungsanalyse sind insbesondere Risiken zu betrachten, welche sich aus der mobilen Nutzung und der Strategie zur Cloud-Nutzung der <Institution> ergeben. Die <Institution> muss prüfen, ob ihre Kontroll- und Einflussmöglichkeiten auf die Betriebssystemumgebung, die Identitäts- und Berechtigungsverwaltung ausreichend sind, um die App sicher nutzen zu können.

### Regelungen für die Verwendung von mobilen Endgeräten und Apps (APP.1.4.A2)

Da oft nicht alle sicherheitsrelevanten Aspekte technisch gelöst werden können, muss für die Mitarbeitenden der <Institution> eine Richtlinie für die Nutzung von Apps erstellt werden und mindestens die folgenden Punkte adressieren:

* welche Informationen/Daten auf den Geräten mit den App’s verarbeitet werden dürfen,
* inwieweit eine private Nutzung der App’s und Geräte gestattet ist,
* durch wen welche Apps auf den Geräten installiert werden dürfen,
* wie sich Mitarbeitenden als Benutzer der App’s in öffentlichen Datennetzen verhalten sollen und
* was zu tun ist, wenn ein Gerät verloren geht.

Diese Vorgaben MÜSSEN mit den etablierten Regelungen der Institution abgestimmt werden.

### Verwendung sicherer Quellen für Apps (APP.1.4.A3)

Es ist sicherzustellen, dass Apps nur aus sicheren und vertrauenswürdigen Quellen bezogen werden können. Es sind nur vertrauenswürdige App Stores zu verwenden. Interne Apps der <Institution> und Apps, die schutzbedürftige Informationen verarbeiten, sollten über einen <Institution>-eigenen App Store oder via der etablierten zentralen Management-Lösung verteilt werden.

### Test und Freigabe von Apps (APP.1.4.A4)

Es ist sicherzustellen, dass sich die App in den vorhandenen Betrieb der <Institution> integrieren lässt und alle Anforderungen der fachlichen Bereiche, der Informationssicherheit, des Datenschutzes und des Notfallmanagements eingehalten werden. Bevor eine neue App bzw. eine neue Version einer App eingesetzt wird, sollte diese getestet und anschließend ausdrücklich freigegeben werden. Für alle Bereiche sollten entsprechende Tests entwickelt sowie Freigabekriterien definiert werden. Die Ergebnisse der Tests sollten dokumentiert werden und als Basis für die Freigabe der App dienen. Es ist insbesondere darauf zu achten, dass die Tests auf allen in der <Institution> verwendeten Gerätemodellen und Betriebssystemumgebungen durchgeführt werden. Die Freigabekriterien sollten bei allen erfüllt sein.

### Minimierung und Kontrolle von App-Berechtigungen (APP.1.4.A5)

Bevor eine App in der <Institution> eingeführt wird, ist sicherzustellen, dass die App nur die minimal benötigten App-Berechtigungen für ihre Funktion erhält. Nicht unbedingt notwendige Berechtigungen sind zu hinterfragen und sollten sofern möglich zentral unterbunden werden.

Sicherheitsrelevante Berechtigungseinstellungen sind zentral so zu hinterlegen, so dass diese Einstellungen nicht durch den Mitarbeitenden oder die App selbst geändert werden kann. Insofern dies technisch nicht möglich ist, sind organisatorischen Regelungen zu etablieren und die Berechtigungseinstellungen regelmäßig zu prüfen und bei Bedarf erneut zu setzen.

### Patchmanagement für Apps (APP.1.4.A6)

Updates sind aufbauend auf den bereits etablierten Patch- und Änderungsmanagement-Prozessen der <Institution> zeitnah einzuspielen. Insofern die <Institution> eine zentrale Management-Lösung einsetzt, sind die Bereitstellung von verfügbaren Updates hierüber zu steuern. Für jeden von der <Institution> bereitzustellenden Patch muss bewertet werden, wie er sich auf die Sicherheit des darunter liegenden Systems sowie auf die Infrastruktur der <Institution> selbst auswirkt. Basierend auf diesem Bewertungsergebnis sollte entsprechend priorisiert werden.

Sollten für öffentlich bekannte Schwachstellen der betriebenen App‘s keine Patches zur Verfügung stehen, sind geeignete Gegenmaßnahmen zu ergreifen. Ist dies nicht möglich, dürfen Apps mit bekannten offenen Schwachstellen nicht verwendet werden.

### Sichere Speicherung lokaler App-Daten (APP.1.4.A7)

Wenn Apps auf interne Dokumente der <Institution> zugreifen können, ist sicherzustellen, dass die lokale Datenhaltung der App auf dem Gerät angemessen abgesichert ist. Insbesondere sind App-Zugriffsschlüssel verschlüsselt abgelegt werden. Vertrauliche Daten dürfen vom Betriebssystem nicht eigenständig an anderen Ablageorten zwischengespeichert werden.

### Verhinderung von Datenabfluss (APP.1.4.A8)

Um zu verhindern, dass Apps ungewollt vertrauliche Daten versenden oder aus den gesendeten Daten Benutzerprofile erstellt werden, ist die App-Kommunikation geeignet einzuschränken. Die Kommunikation sollte im Rahmen des Test- und Freigabeverfahrens analysiert werden. Weiterhin sollte überprüft werden, ob eine App ungewollte Protokollierungs- oder Hilfsdateien schreibt, die möglicherweise vertrauliche Informationen enthalten.

## Standardmaßnahmen

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

### Zentrales Management von Apps (APP.1.4.A11)

Um das Thema strukturiert und nachhaltig in der <Institution> einzuführen, ist ein strategisches Management zu berücksichtigen. Dieses sollte sich aus den folgenden drei Modulen des Enterprise Mobility Managements (EMM) zusammensetzen:

* Mobile Information Management (MIM),
* Mobile Application Management (MAM) und
* Mobile Device Management (MDM).

Mittels des Moduls MAM sollte über Prüfmechanismen und Allow-Listen sichergestellt werden, dass nur geprüfte und freigegebene Apps verwendet werden können.

### Sichere Deinstallation von Apps (APP.1.4.A12)

Wenn Apps deinstalliert werden, sollten auch alle von der App generierten Dateien gelöscht werden. Dabei sollten ebenso vom Betriebssystem zwischengespeicherte Daten (bspw. Caches) mit Bezug zur App gelöscht werden. Zusätzlich sollten auch Daten auf externen Systemen (z. B. beim App-Anbieter gespeicherte Daten) gelöscht 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).

### Entwicklung von Fallback-Lösungen für Apps (APP.1.4.A13 - CIA)

Für alle mit Apps abgebildeten Geschäftsprozesse sind unter Berücksichtigung der maximal tolerierbaren Ausfallzeit (MTA) im Falle einer Störung oder bei anderen Problemen eine Alternative bereitzustellen. Für geschäftskritische Prozesse und deren App’s sind diese mit in die etablierten Prozesse des IT-Notfallmanagements aufzunehmen.

### Unterstützung zusätzlicher Authentisierungsmerkmale bei Apps (APP.1.4.A14 - CI)

Es ist für die Authentisierung der Benutzer in der App ein zweiter Faktor unter Berücksichtigung der von der <Institution> freigegeben Verfahren zu integrieren und zu verwenden. Hierbei sollte darauf geachtet werden, dass eventuell benötigte Sensoren oder Schnittstellen in allen von der <Institution> verwendeten Geräten vorhanden sind. Beim Einsatz von biometrischen Verfahren ist zu berücksichtigen, wie resistent die Authentisierung gegen mögliche Fälschungsversuche ist.

### Durchführung von Penetrationstests für Apps (APP.1.4.A15 - CIA)

Bevor eine App für den Einsatz freigegeben wird, sollte ein Penetrationstest unter Berücksichtigung der Empfehlungen der OWASP durchgeführt werden. Dabei sollten alle Kommunikationsschnittstellen zu Backend-Systemen sowie die lokale Speicherung von Daten auf mögliche Sicherheitslücken untersucht werden. Die Penetrationstests sollten regelmäßig und zusätzlich bei größeren Änderungen an der App wiederholt werden. Bei App’s, welche für die <Institution> selbst entwickelt wurden, sind Black- bzw. Whitebox Penetrationstests mindestens einmal im Jahr und bei bekannt werden von Sicherheitslücken bei den genutzten Frameworks und Komponenten der Infrastruktur durchzuführen.