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

Sicherheitsrichtlinie "Mobile Device Management (MDM)"

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 | ISMS300032 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Mobile Device Management (MDM)" | [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](#_Toc80768057)

[Dokumentenhistorie 3](#_Toc80768058)

[Inhaltsverzeichnis 4](#_Toc80768059)

[Allgemeine Festlegungen 5](#_Toc80768060)

[Ziel / Zweck 5](#_Toc80768061)

[Geltungsbereich 5](#_Toc80768062)

[Zuständigkeiten 5](#_Toc80768063)

[Genehmigungs- und Änderungsverfahren 6](#_Toc80768064)

[Aufbau des Dokuments 6](#_Toc80768065)

[Sicherheitsrichtlinie „Mobile Device Management (MDM)" 7](#_Toc80768066)

[Basismaßnahmen 7](#_Toc80768067)

[Festlegung einer Strategie für das Mobile Device Management (SYS.3.2.2.A1) 7](#_Toc80768068)

[Festlegen erlaubter mobiler Endgeräte (SYS.3.2.2.A2) 7](#_Toc80768069)

[Auswahl eines MDM-Produkts (SYS.3.2.2.A3) 8](#_Toc80768070)

[Verteilung der Grundkonfiguration auf mobile Endgeräte (SYS.3.2.2.A4) 8](#_Toc80768071)

[Sichere Grundkonfiguration für mobile Endgeräte (SYS.3.2.2.A5) 8](#_Toc80768072)

[Protokollierung und Gerätestatus (SYS.3.2.2.A6) 8](#_Toc80768073)

[Regelmäßige Überprüfung des MDM (SYS.3.2.2.A20) 9](#_Toc80768074)

[Standardmaßnahmen 9](#_Toc80768075)

[Auswahl und Freigabe von Apps (SYS.3.2.2.A7) 9](#_Toc80768076)

[Festlegung erlaubter Informationen auf mobilen Endgeräten (SYS.3.2.2.A8) 9](#_Toc80768077)

[Auswahl von Sicherheits-Apps (SYS.3.2.2.A9) 9](#_Toc80768078)

[Sichere Anbindung der mobilen Endgeräte an die Institution (SYS.3.2.2.A10) 9](#_Toc80768079)

[Berechtigungsmanagement im MDM (SYS.3.2.2.A11) 10](#_Toc80768080)

[Absicherung der MDM-Betriebsumgebung (SYS.3.2.2.A12) 10](#_Toc80768081)

[Verwaltung von Zertifikaten (SYS.3.2.2.A21) 10](#_Toc80768082)

[Fernlöschung und Außerbetriebnahme von Endgeräten (SYS.3.2.2.A22) 10](#_Toc80768083)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc80768084)

[Benutzung externer Reputation-Services für Apps (SYS.3.2.2.A14 - CIA) 11](#_Toc80768085)

[Kontrolle der Nutzung von mobilen Endgeräten (SYS.3.2.2.A17 - CI) 11](#_Toc80768086)

[Geofencing (SYS.3.2.2.A19 - CI) 11](#_Toc80768087)

[Durchsetzung von Compliance-Anforderungen (SYS.3.2.2.A23 - CIA) 11](#_Toc80768088)

# Allgemeine Festlegungen

## Ziel / Zweck

Smartphones, Tablets und Phablets sind für die Mitarbeitenden der <Institution> ein nicht mehr wegzudenkender Teil ihrer Arbeit. Die verantwortlichen Administratoren müssen jedoch immer mehr Smartphones und Tablets in vielen unterschiedlichen Ausführungen bereitstellen und dabei gleichzeitig für eine angemessene Sicherheit Geräte-Hersteller-übergreifen sorgen. Hinzu kommt, dass mobile Endgeräte (Mobile Devices) besonderen Gefahren ausgesetzt sind und sich die Administration von Smartphones und Tablets in grundlegenden Punkten von anderen klassischen IT-Systemen unterscheidet.

Aus diesem Grunde ist ein Mobile Device Management (MDM) für die zentrale Verwaltung, dem sicheren Betrieb der Clients sowie in Notfall-Situationen für die <Institution> unabdingbar.

Diese Sicherheitsrichtlinie zeigt auf, wie mit einem MDM mobile Endgeräte sicher von der <Institution> genutzt und wie das MDM selber sicher betrieben werden kann. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines SYS.3.2.2 "Mobile Device Management (MDM)" 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 Device Management (MDM)“ 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 Device Management (MDM)"

## Basismaßnahmen

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

### Festlegung einer Strategie für das Mobile Device Management (SYS.3.2.2.A1)

In den folgenden Dokumenten „Standard Benutzer“, „Standard IT-Administration“ und „Sicherheitsrichtlinie mobile Geräte und Datenträger“ definiert die <Institution> Strategien und Regelungen zur sicheren Benutzung mobilen Clients durch Mitarbeitende und Externe sowie die Integration der Clients in die internen IT-Strukturen. Die Grundlage für die geltenden Strategien und Regelungen ist dabei der ermittelte bzw. geerbte Schutzbedarf der zu verarbeitenden Informationen.

Unter der Berücksichtigung der Cloud-Strategie der <Institution>, sind in dieser Sicherheitsrichtlinie die speziellen Vorgaben für den Betrieb eines Mobile Device Managements (MDM) festgelegt.

Die MDM-Strategie der <Institution> deckt mindestens folgende Aspekte ab:

* Das MDM der <Institution> kann als Cloud-Dienst betreiben werden.
* Die Verfügbarkeit des Cloud-Dienstes soll bei 99,99% pro Monat betragen.
* Die MDM-Infrastruktur soll nicht durch die <Institution> selbst betrieben werden.
* Das Data-Center in dem die MDM-Infrastruktur betrieben wird, muss konform zu den Standards der <Institution> sein.
* Es sind nur die geschäftlich notwendigen Cloud-Dienste einzubinden und dabei die Anforderungen des Dokumenten-Managements mit einzubeziehen.
* Es gelten die Compliance-Anforderungen der <Institution>.
* Ausschließlich evaluierte, getestete und freigegebene mobile Endgeräte und Betriebssysteme sind zu verwenden.
* Es sollte eine mandantenfähige MDM-Lösung eingesetzt werden.
* Das MDM sollte auch Peripherie-Geräte einbinden und verwalten können.

Als Betriebsmodell sind für interne Mitarbeitenden ausschließlich personalisierte Endgeräte, die sich im Eigentum der <Institution> befinden, vorgesehen. Nicht personalisierte Endgeräte kommen nicht zum Einsatz. Private Endgeräte (Bring Your Own Device) dürfen nur in das MDM zur Bereitstellung von 2FA-Apps eingebunden werden.

### Festlegen erlaubter mobiler Endgeräte (SYS.3.2.2.A2)

Es ist festzulegen, welche mobilen Endgeräte und Betriebssysteme für die Verwaltung durch das MDM zugelassen sind. Alle erlaubten Geräte und Betriebssysteme müssen den Anforderungen der MDM-Strategie genügen und die technischen Sicherheitsanforderungen der <Institution> vollständig erfüllen.

Das MDM ist so zu konfigurieren, dass nur mit freigegebenen Clients auf Informationen der <Institution> zugegriffen werden kann. Neue mobile Clients sind gemäß der Liste der zugelassenen Endgeräte zu beschaffen. Ganz neue Produkte sollten erst Anhand von Anforderungslisten und mittels Proof of Concept (PoC) geprüft und nach Freigabe in die Liste der zugelassenen Clients aufgenommen werden.

### Auswahl eines MDM-Produkts (SYS.3.2.2.A3)

Im Rahmen der Beschaffung einer MDM-Lösung ist sicherzustellen, dass sich mit der MDM-Lösung alle in der MDM-Strategie festgelegten Anforderungen erfüllen lassen. Die MDM-Lösung muss auch sämtliche technischen und organisatorischen Sicherheitsmaßnahmen umsetzen können und alle zugelassenen mobilen Endgeräte unterstützen.

### Verteilung der Grundkonfiguration auf mobile Endgeräte (SYS.3.2.2.A4)

Alle mobilen Clients sind so schnell wie möglich in das MDM zu integrieren, damit diese nach den Richtlinien der <Institution> zentral konfiguriert und verwaltet werden können. Wenn die Clients die Grundkonfiguration über das MDM erhalten, müssen diese im Rahmen des On-Boardings sich im Werkszustand befinden. Bei bereits benutzten Clients muss entschieden werden, ob vorher alle Business-bezogenen Daten gelöscht werden. Ein nicht über das MDM konfiguriertes Endgerät darf nicht ohne Freigabe durch den <Datenschutzbeauftragter> und dem <Informationssicherheitsbeauftragter> auf sensible Informationen der <Institution> zugreifen können.

### Sichere Grundkonfiguration für mobile Endgeräte (SYS.3.2.2.A5)

Alle mobilen Clients sind so zu konfigurieren, dass die Clients den zuvor definierten Schutzbedarf angemessen erfüllen. Zur Erreichung eines angemessenen Schutzes der Informationen auf dem Client, sind durch die Verantwortlichen für das MDM-Management passende Grundkonfiguration zusammenzustellen und zu dokumentieren. Wenn mobile Endgeräte an Mitarbeitende übergeben werden, muss darauf bereits der MDM-Client installiert sein bzw. im Rahmen des On-Boarding muss es den Mitarbeitenden selbst möglich sein, den MDM-Client zu installieren.

### Protokollierung und Gerätestatus (SYS.3.2.2.A6)

Zum Zwecke einer übergreifenden Auswertung von Ereignissen muss die Zeit-Synchronisation mit den freigegebenen Zeitquellen bzw. Zeitzonen der <Institution> erfolgen.

Die MDM-Lösung muss alle sicherheitsrelevanten Ereignisse und Konfigurationsänderungen protokollieren. Die erhobenen Protokolldaten dürfen nicht von unbefugten Personen eingesehen werden und müssen unveränderbar gespeichert werden. Auch müssen bei der Protokollierung gesetzliche und interne Regelungen der <Institution> eingehalten werden. Die von MDM-Lösung erzeugten Protokolle müssen regelmäßig auf ungewöhnliche Einträge überprüft werden. Der Lebenszyklus einschließlich der Konfigurationshistorie eines mobilen Clients sollte ausreichend protokolliert und zentral abrufbar sein. Bei Bedarf sollte der aktuelle Status der verwalteten Endgeräte durch den verantwortlichen Administrator ermittelt werden können (Device Audit).

### Regelmäßige Überprüfung des MDM (SYS.3.2.2.A20)

Die Sicherheitseinstellungen der MDM-Lösung sind regelmäßig zu überprüfen. Bei neuen Betriebssystemversionen der mobilen Clients ist vorab zu prüfen, ob die MDM-Lösung diese vollständig unterstützt und die Konfigurationsprofile und Sicherheitseinstellungen weiterhin wirksam und ausreichend sind. Erkannte Abweichungen sind zeitnah zu korrigieren bzw. in das Risikomanagement aufzunehmen. Die zugeteilten Berechtigungen für Mitarbeitende (Benutzer) und Administratoren sind regelmäßig daraufhin zu überprüfen, ob die Berechtigungen weiterhin entsprechend des Need-to-know-Prinzip angemessen sind.

## Standardmaßnahmen

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

### Auswahl und Freigabe von Apps (SYS.3.2.2.A7)

Apps aus öffentlichen App-Stores werden durch die Verantwortlichen für die MDM-Lösung geprüft und mittels des etablierten Freigabeprozesses bereitgestellt. Die Freigaben erfolgen ausschließlich nach den definierten Bewertungskriterien. Alle freigegebenen Apps werden intern in einem Standardkatalog veröffentlicht und dort für die Mitarbeitenden zur Verfügung gestellt. Apps werden gemäß den Anforderungen des geplanten Einsatzszenarios über die MDM-Lösung installiert, deinstalliert und aktualisiert. Das MDM erzwingt die Installation, Deinstallation und Aktualisierung, sobald eine Verbindung zum mobilen Client besteht.

### Festlegung erlaubter Informationen auf mobilen Endgeräten (SYS.3.2.2.A8)

Es ist festzulegen, welche Informationen die mobilen Clients unter welchen Bedingungen verarbeiten dürfen. Die Grundlagen für diese Regelungen sind die Klassifikationen und Schutzbedarf der Informationen sowie die exakten Verarbeitungsbedingungen auf dem mobilen Client (zum Beispiel in abgeschotteten Containern oder verwaltete Apps). Die Verantwortlichen für die MDM-Lösung konfigurieren das MDM auf Basis dieser Richtlinie und hinsichtlich der Durchsetzbarkeit der Anforderungen auf allen mobilen Clients.

Den Mitarbeitern werden die notwendigen Regelungen zum Umgang mit den mobilen Clients und den MDM Funktionen in geeigneter Weise bekannt gemacht.

### Auswahl von Sicherheits-Apps (SYS.3.2.2.A9)

Um das erforderliche Sicherheitsniveau durchzusetzen, sind für die mobilen Clients geeignete Sicherheits-Apps auszuwählen. Die Sicherheits-Apps sind durch die MDM-Lösung automatisch zu installieren.

### Sichere Anbindung der mobilen Endgeräte an die Institution (SYS.3.2.2.A10)

Die Verbindung der mobilen Clients zur MDM-Lösung muss angemessen abgesichert werden. Die Verbindung der mobilen Clients ins Netz der <Institution> oder den von der <Institution> genutzten Cloud-Services oder WebApps muss angemessen abgesichert werden. Sofern Daten zwischen den mobilen Clients und dem IT-Netz der <Institution> übertragen werden, sollte durch geeignete Maßnahmen (z. B. IPSec- oder TLS-VPNs) verhindert werden, dass Unbefugte diese Daten verändern oder einsehen können.

### Berechtigungsmanagement im MDM (SYS.3.2.2.A11)

Für das MDM-Lösung sollte ein Berechtigungskonzept erstellt, dokumentiert und angewendet werden. Bei der Erstellung des Berechtigungskonzeptes sind ebenfalls die notwendigen Infrastrukturen für ein Zero-Touch-Deployment mit einzubeziehen. Sofern Client der Firma Apple durch die MDM-Lösung zentral verwaltet werden, sind auch die Berechtigungen für die Nutzung der Apple ID zu integrieren. Den Benutzergruppen und Administratoren sind für die MDM-Lösung nur so viele Berechtigungen einzuräumen wie für die Aufgabenerfüllung notwendig sind. Es sollte regelmäßig überprüft werden, ob die zugeteilten Rechte noch angemessen sind.

### Absicherung der MDM-Betriebsumgebung (SYS.3.2.2.A12)

Die MDM-Lösung selbst ist durch technische Maßnahmen abzusichern, um dem Schutzbedarf der hinterlegten oder verarbeiteten Informationen zu genügen. Das zugrundeliegende Betriebssystem sollte gehärtet werden. Alle notwendigen Patches sollten eingespielt werden. Zugriffsberechtigungen und -wege sollten gemäß dem festgelegten Sicherheitskonzept konfiguriert werden.

### Verwaltung von Zertifikaten (SYS.3.2.2.A21)

Zertifikate zur Nutzung von Diensten auf dem mobilen Client sollten zentral über die MDM-Lösung installiert, deinstalliert und aktualisiert werden. Die Installation von nicht vertrauenswürdigen und nicht verifizierbaren (Root-) Zertifikaten durch den Mitarbeitenden sollte durch die MDM-Lösung unterbunden werden. Die MDM-Lösung sollte Mechanismen unterstützen, um die Gültigkeit von Zertifikaten zu überprüfen.

### Fernlöschung und Außerbetriebnahme von Endgeräten (SYS.3.2.2.A22)

Die MDM-Lösung sollte sicherstellen, dass sämtliche Daten auf dem mobilen Client aus der Ferne gelöscht werden können (Remote Wipe), sofern eine Kommunikationsverbindung besteht. Werden in dem mobilen Client austauschbare externe Speicher genutzt, ist zu verifizieren, dass diese Speichermedien bei einem Remote Wipe ebenfalls gelöscht werden.

Der Prozess zur Außerbetriebnahme des mobilen Endgerätes muss sicherstellen, dass keine schutzbedürftigen Daten der <Institution> auf dem mobilen Client oder eingebundenen Speichermedien verbleiben. Dies muss insbesondere dann etabliert sein, wenn das Löschen und die Außerbetriebnahme aus der Ferne ausgeführt wird.

## 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).

### Benutzung externer Reputation-Services für Apps (SYS.3.2.2.A14 - CIA)

Wenn die verantwortlichen Administratoren der MDM-Lösung die erlaubten Apps nicht selbst auswählen können und Benutzer selbstständig Apps auf ihren Geräten installieren dürfen, muss ein sogenannter Reputation-Service eingesetzt werden. Die MDM-Lösung muss dann mithilfe dieser Informationen aus dem Reputation-Service die Installation von Apps zumindest einschränken.

### Kontrolle der Nutzung von mobilen Endgeräten (SYS.3.2.2.A17 - CI)

Es sollten angemessene Kriterien definiert werden, aufgrund derer die mobilen Clients zu überwachen sind, ohne gegen gesetzliche oder interne Regelungen der <Institution> zu verstoßen.

Die angemessenen Kriterien für die Protokollierung und Überwachung der mobilen Clients sind als integraler Bestandteil der sicherheitstechnischen und datenschutzrelevanten Dokumentation des Sicherheitsmanagement und der Betriebsdokumentation aufzunehmen.

### Geofencing (SYS.3.2.2.A19 - CI)

Durch die Hinterlegung einer Geofencing-Richtlinie soll sichergestellt werden, dass mobile Clients mit sehr schutzbedürftigen Informationen/Daten nicht außerhalb eines zuvor festgelegten geografischen Bereichs verwenden können. Wird der zuvor freigegebene geografische Bereich verlassen, sollte eine selektive Löschung der klassifizierten Informationen oder eine vollständige Löschung des Geräts erfolgen. Bevor das Gerät selektiv oder vollständig gelöscht wird, sollten die verantwortlichen Administratoren und das Sicherheitsmanagement die von diesen Einstellungen betroffenen Mitarbeitenden informieren. Die Löschung sollte erst mit einer angemessenen zeitlichen Verzögerung erfolgen.

Unter zur Hilfenahme der Möglichkeit einer Schutzbedarfsanalyse sollen Bereiche identifiziert werden, an denen diese zusätzlichen Geofencing-Maßnahmen notwendig sind.

Alle angewendeten Geofencing-Richtlinien sind unter Beachtung der gesetzlichen und internen Regelungen der <Institution> umzusetzen.

### Durchsetzung von Compliance-Anforderungen (SYS.3.2.2.A23 - CIA)

Seitens der <Institution> sollte eine vom MDM-Anbieter bereitgestellte Lösung verwendet werden, um Verstöße gegen die internen Regelungen oder sogar eine Manipulation des Betriebssystems zu erkennen. Die folgenden Aktionen sollten durch die entsprechenden MDM Funktionen bei Verdacht auf Verstoß gegen Regelungen oder Manipulation des Betriebssystems ausgeführt:

* Selbständiges Versenden von Warnhinweisen
* Selbständiges Sperren des mobilen Clients
* Löschen der vertraulichen Informationen auf dem mobilen Client
* Löschen des kompletten mobilen Clients
* Verhindern des Zugangs zu Apps des mobilen Clients
* Verhindern des Zugangs zu den Systemen, Services und Informationen der <Institution>

Bei Verdacht auf einen Verstoß oder eine Manipulation wird ein Alarm an die verantwortlichen Administratoren, den <Datenschutzbeauftragter>und den <Informationssicherheitsbeauftragter> gesandt.