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

Sicherheitsrichtlinie "Laptop"

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 | ISMS300034 | [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](#_Toc81035765)

[Dokumentenhistorie 3](#_Toc81035766)

[Inhaltsverzeichnis 4](#_Toc81035767)

[Allgemeine Festlegungen 5](#_Toc81035768)

[Ziel / Zweck 5](#_Toc81035769)

[Geltungsbereich 6](#_Toc81035770)

[Zuständigkeiten 6](#_Toc81035771)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81035772)

[Aufbau des Dokuments 6](#_Toc81035773)

[Sicherheitsrichtlinie „Laptop" 8](#_Toc81035774)

[Basismaßnahmen 8](#_Toc81035775)

[Regelungen zur mobilen Nutzung von Laptops (SYS.3.1.A1) 8](#_Toc81035776)

[Zugriffsschutz am Laptop (SYS.3.1.A2) 8](#_Toc81035777)

[Einsatz von Personal Firewalls (SYS.3.1.A3) 8](#_Toc81035778)

[Einsatz von Antivirenprogrammen (SYS.3.1.A4) 8](#_Toc81035779)

[Datensicherung (SYS.3.1A5) 9](#_Toc81035780)

[Standardmaßnahmen 9](#_Toc81035781)

[Geregelte Übergabe und Rücknahme eines Laptops (SYS.3.1.A7) 9](#_Toc81035782)

[Sicherer Anschluss von Laptops an Datennetze (SYS.3.1.A8) 9](#_Toc81035783)

[Sicherer Fernzugriff (SYS.3.1.A9) 9](#_Toc81035784)

[Abgleich der Datenbestände von Laptops (SYS.3.1.A10) 10](#_Toc81035785)

[Sicherstellung der Energieversorgung (SYS.3.1.A11) 10](#_Toc81035786)

[Verlustmeldung (SYS.3.1.A12) 10](#_Toc81035787)

[Verschlüsselung von Laptops (SYS.3.1.A13) 10](#_Toc81035788)

[Geeignete Aufbewahrung von Laptops (SYS.3.1.A14) 10](#_Toc81035789)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc81035790)

[Zentrale Administration von Laptops (SYS.3.1.A16 - CIA) 11](#_Toc81035791)

[Sammelaufbewahrung (SYS.3.1.A17 - CIA) 11](#_Toc81035792)

[Einsatz von Diebstahl-Sicherungen (SYS.3.1.A18 - CIA) 11](#_Toc81035793)

[Geeignete Auswahl von Laptops (SYS.3.1.bd.A1) 11](#_Toc81035794)

# Allgemeine Festlegungen

## Ziel / Zweck

Unter einem Laptop (oder auch Notebook) versteht die <Institution> einen PC, der mobil genutzt werden kann. Ein Laptop hat eine kompakte Bauform, integriert Peripheriegeräte wie Tastatur und Bildschirm, ist über Akkus zeitweise unabhängig von einer externen Stromversorgung und besteht oft aus speziell für den mobilen Einsatz konzipierten Hardware-Komponenten. Laptops können mit allen üblichen Betriebssystemen wie Microsoft Windows, Apple macOS oder Linux betrieben werden. Die Geräte sind in der <Institution> verbreitet und ersetzen den klassischen Desktop-PC.

Da Laptops meist mobil genutzt werden, sind Laptops nicht permanent am LAN der <Institution> angeschlossen. Stattdessen können die Laptops sich in der Regel per Virtual Private Network (VPN) über das Internet oder andere Datennetze verbinden, um so auf die Ressourcen des LANs oder den bereitgestellten Cloud-Ressourcen zuzugreifen. Auch die Infrastruktur einer klassischen Büroumgebung, wie kontrollierbare Umwelteinflüsse, eine stabile Stromversorgung oder zutrittsgeschützte Bereiche kann für den mobilen Einsatz von Laptops nicht vorausgesetzt werden.

Ziel der Sicherheitsrichtlinie ist es, einen sicheren Betrieb von Laptops zu ermöglichen sowie für die spezifischen Gefährdungen dieser Geräteklasse zu sensibilisieren. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines SYS.3.1 "Laptops" 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 „Laptop“ 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 „Laptop"

## Basismaßnahmen

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

### Regelungen zur mobilen Nutzung von Laptops (SYS.3.1.A1)

In der <Institution> sind Regelungen für die Mitnahme von Laptops zu definieren. Es ist zu regeln, welche Laptops außer Haus mitgenommen werden dürfen, welcher Mitarbeitende diese mitnehmen darf und welche Sicherheitsmaßnahmen dabei zu beachten sind. Alle Mitarbeitenden sind über Regelungen und Maßnahmen zur Mitnahme von Laptops zu unterrichten.

### Zugriffsschutz am Laptop (SYS.3.1.A2)

Um die Geräte vor unberechtigter Nutzung zu schützen, sind auf allen Laptops angemessene Zugriffschutzmaßnahmen zu etablieren. Ebenfalls ist zu prüfen, ob alle Mitarbeitenden mit dem eingerichteten Zugriffschutz richtig umgehen.

### Einsatz von Personal Firewalls (SYS.3.1.A3)

Auf Laptops ist eine Personal Firewall entsprechend der Gesamtstrategie „Betrieb einer mehrstufigen Firewall-Infrastruktur“ zu aktivieren. Die Filterregeln der Firewall sind so restriktiv wie möglich zu setzen und regelmäßig zu testen. Die Personal Firewall muss so konfiguriert werden, dass die Benutzer nicht durch Warnmeldungen belästigt werden, die sie nicht interpretieren können.

### Einsatz von Antivirenprogrammen (SYS.3.1.A4)

Abhängig vom installierten Betriebssystem (Windows, macOS und Linux) und anderen vorhandenen Schutzmechanismen ist auf allen Laptops der <Institution> eine Antivirenlösung zu installieren und zu aktivieren. Es muss sichergestellt sein, dass sowohl das Scan-Programm als auch die Signaturen stets auf dem aktuellen Stand sind. Die Mitarbeitenden sind über den Umgang mit der Antivirenlösung und On-Demand-Scans zu unterrichten.

Der gesamte Datenbestand der Laptops ist regelmäßig auf Schadprogramme zu prüfen. Wenn das Laptop infiziert ist, ist im Offlinebetrieb zu untersuchen, ob das gefundene Schadprogramm bereits vertrauliche Daten gesammelt, Schutzfunktionen deaktiviert oder Code aus dem Internet nachgeladen wurde. Da eine Offline Untersuchung nur möglich ist, wenn zuvor alle sich im Laptop befindlichen Datenspeicher entschlüsselt wurden, ist eine Cloud-basierte Antivirenlösungen der nächsten Generation mit erweiterter Endpoint-Detection-and-Response (EDR) zu etablieren.

Die Antivirenlösung muss zudem nach Schadsoftware suchen, wenn Dateien ausgetauscht oder übertragen werden. Auch müssen alle auf dem Laptop benutzten Internet-Dienste (HTTP, FTP) sowie verschlüsselte Daten ausreichend vor Schadprogrammen geschützt werden.

Es ist sicherzustellen, dass die Benutzer keine sicherheitsrelevanten Änderungen an den Einstellungen der Antivirenprogramme (BIOS/UEFI) vornehmen können.

### Datensicherung (SYS.3.1A5)

Alle lokal auf dem Laptop gespeicherten Daten sind regelmäßig zu sichern. Hierfür sind abhängig vom Volumen des Datenbestands geeignete Verfahren zur Datensicherung auszuwählen. Die Datensicherung muss weitgehend automatisiert werden, sodass die Mitarbeitenden möglichst wenig Aktionen selbst durchführen müssen.

## Standardmaßnahmen

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

### Geregelte Übergabe und Rücknahme eines Laptops (SYS.3.1.A7)

Sofern Laptops von verschiedenen Mitarbeitenden abwechselnd genutzt werden, ist zu regeln, wie Laptops sicher an Mitarbeitende übergeben werden können bzw. wie Laptops wieder sicher zurückzunehmen sind. Beim Benutzerwechsel eines Laptops sind eventuell vorhandene schützenswerte Daten sicher zu löschen. Falls der Laptop nach dem Benutzerwechsel nicht neu aufgesetzt wird, ist sicherzustellen, dass sich auf dem System bzw. allen damit verbundenen Datenträgern keine Schadsoftware befindet. Mit einem Laptop sollte den Mitarbeitenden ein Merkblatt für den sicheren Umgang mit dem Gerät ausgehändigt werden.

### Sicherer Anschluss von Laptops an Datennetze (SYS.3.1.A8)

Eine Anmeldung am produktiven Netz der <Institution> ist nur für zugelassene Laptops zu ermöglichen. Es sollte ferner geregelt werden, wie Laptops sicher an fremde Datennetze bspw. beim Kunden und an das Internet angeschlossen werden. Laptops sind wirksam vor Schadsoftware, Schadcode und vor Angriffen aus Fremdnetzen und aus dem Internet zu schützen. Dafür sollten das Betriebssystem und die installierte Software von Laptops immer auf dem aktuellen Stand sein. Nicht benötigte Schnittstellen sollten bei allen Laptops deaktiviert werden.

Nicht zugelassene Laptops, welche sich am produktiven Netz der <Institution> anmelden wollen, sind in ein sogenanntes Quarantäne-Netz automatisch zu überführen.

### Sicherer Fernzugriff (SYS.3.1.A9)

Daten welche im Rahmen der Wartung (Fernzugriff) übertragen werden, sind durch geeignete kryptographische und Authentisierungsmaßnahmen ausreichend zu schützen. Auch sollte der Laptop des Mitarbeitenden selbst abgesichert sein, wenn Daten mit anderen IT-Systemen ausgetauscht werden.

### Abgleich der Datenbestände von Laptops (SYS.3.1.A10)

Sofern die Mitarbeitenden nicht direkt auf den zur Verfügung gestellten Cloud-Services oder Servern arbeiten, soll sichergestellt sein, dass alle business-relevanten Datenbestände regelmäßig zwischen Laptop und <Institution>-Infrastruktur abgeglichen werden.

Über das eingesetzte Betriebssystem (Windows, macOS, Linux) auf dem Laptop wird ein Synchronisationstool benutzt, welches sicherstellt, dass

* Synchronisationskonflikte aufgelöst werden können und
* der Synchronisationsvorgang protokolliert wird.

Außerdem sollten die Mitarbeitenden sensibilisiert werden, die angefallenen Synchronisationsprotokolle stichprobenartig zu prüfen.

### Sicherstellung der Energieversorgung (SYS.3.1.A11)

Alle Benutzer von Laptops sind darüber zu informieren, wie sie die Energieversorgung von Laptops im mobilen Einsatz optimal sicherstellen. Falls für die Laptops Ersatz-Akkus verfügbar sind, sollten diese in entsprechenden Hüllen gelagert und transportiert werden.

### Verlustmeldung (SYS.3.1.A12)

Ein Verlust des Laptops ist umgehend der <Institution> zu melden. Hierfür sind Meldewege zu definieren. Tauchen verlorene Laptops wieder auf, sind diese auf eventuelle technische Manipulationen zu überprüfen. Ist dies aus wirtschaftlichen Gründen nicht möglich, sind die Laptops zu entsorgen. Ebenfalls sind ehemals verlorene Laptops vor einem erneuten Einsatz komplett zurückzusetzen und neu zu installieren.

### Verschlüsselung von Laptops (SYS.3.1.A13)

Die Festplatten eines Laptops sind zu verschlüsseln. Für die Verschlüsselung sind die durch die <Institution> freigegebenen Verschlüsselungsalgorithmen einzusetzen. Die Schlüssel sind zufällig zu erzeugen und geeignet auf zu bauen bewahren. Sofern das Verfahren ein Challenge and Response anbietet, sind die Laptops in ein zentrales Challenge and Response Verfahren zu integrieren.

### Geeignete Aufbewahrung von Laptops (SYS.3.1.A14)

Alle Benutzer von Laptops sollten darauf hingewiesen werden, wie Laptops außerhalb der Räumlichkeiten der <Institution> geeignet aufbewahrt werden. Sofern die Laptops auch außerhalb der klassischen Nutzungszeiten in den Räumen der <Institution> verbleiben, sollten die Laptops gegen Diebstahl gesichert bzw. verschlossen 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).

### Zentrale Administration von Laptops (SYS.3.1.A16 - CIA)

Es ist eine zentrale Vorgabe und Vorgehensweise für die Administration von Laptops einzuführen und zu betreiben. Das eingesetzte Laptop-Management Tool muss alle eingesetzten Betriebssysteme unterstützen.

### Sammelaufbewahrung (SYS.3.1.A17 - CIA)

Nicht benutzte Laptops sind in einem geeignet abgesicherten Raum auf zu bewahren.

### Einsatz von Diebstahl-Sicherungen (SYS.3.1.A18 - CIA)

Es sollte geregelt werden, welche Diebstahlsicherungen für Laptops eingesetzt werden sollen. Bei mechanischen Sicherungen sollte besonders auf ein gutes Schloss geachtet werden.

### Geeignete Auswahl von Laptops (SYS.3.1.bd.A1)

Vor Anschaffung neuer Laptops sollte von den Verantwortlichen für den IT-Betrieb eine Anforderungsanalyse durchgeführt werden. Dabei sind ebenfalls die benötigten Hardwarekomponenten wie z. B. Dockingstation und Monitore zu beachten. Die Bewertung und Beschaffung der infrage kommenden Geräte erfolgt anhand der erzielten Ergebnisse der Anforderungsanalyse.