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

Sicherheitsrichtlinie "Standardsoftware"

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 Dokumentenvertraulichkeitoffen, intern, vertraulich, streng vertraulich] |
| Dokumen­tenkennung | ISMS300004 | [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](#_Toc78731740)

[Dokumentenhistorie 3](#_Toc78731741)

[Inhaltsverzeichnis 4](#_Toc78731742)

[Allgemeine Festlegungen 5](#_Toc78731743)

[Ziel / Zweck 5](#_Toc78731744)

[Geltungsbereich 5](#_Toc78731745)

[Zuständigkeiten 5](#_Toc78731746)

[Genehmigungs- und Änderungsverfahren 6](#_Toc78731747)

[Aufbau des Dokuments 6](#_Toc78731748)

[Sicherheitsrichtlinie "Standardsoftware" 7](#_Toc78731749)

[Basismaßnahmen 7](#_Toc78731750)

[Sicherstellen der Integrität von Standardsoftware (CON.4.A1) 7](#_Toc78731751)

[Entwicklung der Installationsanweisung für Standardsoftware (CON.4.A2) 7](#_Toc78731752)

[Sichere Installation und Konfiguration von Standardsoftware (CON.4.A3) 7](#_Toc78731753)

[Standardmaßnahmen 7](#_Toc78731754)

[Festlegung der Verantwortlichkeiten im Bereich Standardsoftware (CON.4.A4) 7](#_Toc78731755)

[Erstellung eines Anforderungskatalogs für Standardsoftware (CON.4.A5) 8](#_Toc78731756)

[Auswahl einer geeigneten Standardsoftware (CON.4.A6) 8](#_Toc78731757)

[Überprüfung der Lieferung von Standardsoftware (CON.4.A7) 8](#_Toc78731758)

[Lizenzverwaltung und Versionskontrolle von Standardsoftware (CON.4.A8) 8](#_Toc78731759)

[Deinstallation von Standardsoftware (CON.4.A9) 8](#_Toc78731760)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc78731761)

[Implementierung zusätzlicher Sicherheitsfunktionen (CON.4.A10 - CIA) 9](#_Toc78731762)

[Nutzung zertifizierter Standardsoftware (CON.4.A11 - CIA) 9](#_Toc78731763)

[Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen (CON.4.A12 - CI) 9](#_Toc78731764)

# Allgemeine Festlegungen

## Ziel / Zweck

Unter Standardsoftware wird innerhalb der <Institution> Software die auf dem Markt angeboten und meistens über Kataloge oder Onlineportale erworben werden kann verstanden. Die Software zeichnet sich dadurch aus, dass diese durch die <Institution> selbst installiert und mit einem angemessenen Aufwand an die betrieblichen und sicherheitstechnischen Bedürfnisse der <Institution> angepasst werden kann.

In dieser Sicherheitsrichtlinie wird unter Berücksichtigung der Vorgaben aus dem BSI Baustein CON.4"Auswahl und Einsatz von Standardsoftware" dargestellt, wie die <Institution> unter Sicherheitsgesichtspunkten mit Standardsoftware umgehen wird. Es werden sowohl organisatorische als auch technische Maßnahmen definiert, die zum Aufbau und Aufrechterhaltung eines angemessenen Sicherheitsniveaus notwendig sind.

## 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

Das Dokument "Sicherheitsrichtlinie Standardsoftware“ 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 "Standardsoftware"

## Basismaßnahmen

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

### Sicherstellen der Integrität von Standardsoftware (CON.4.A1)

Es wird sichergestellt, dass nur originale und unveränderte Software installiert wird. Die Installation erfolgt ausschließlich von Originaldatenträgern oder von geprüften identischen Kopien des originalen Installationsmediums. Der Zugriff auf die Installationsroutinen ist auf einen bestimmten Mitarbeiterkreis beschränkt. Alle Installationsprogramme werden auf Schadsoftware überprüft. Von den Installationsdateien werden Sicherungskopien angelegt. Diese sollten im Anschluss ebenfalls geprüft werden.

### Entwicklung der Installationsanweisung für Standardsoftware (CON.4.A2)

Für ausgewählte Standardsoftware wird eine Installationsanweisung bzw. ein Workflow für die Installation erstellt. Sofern benötigt werden geeignete Parameter für die Konfiguration sowie organisatorische Rahmenbedingungen für die Installation der Software vorgegeben.

### Sichere Installation und Konfiguration von Standardsoftware (CON.4.A3)

Die Installation und Konfiguration freigegebener Standardsoftware folgt den innerhalb der <Institution> definierten Installationsanweisungen. Alle Abweichungen von den Installationsanweisungen sind durch den fachliche Produktverantwortlichen und dem Information Security Officer zu genehmigen. Alle Installationen werden durch die hierfür Verantwortlichen durchgeführt. Dabei wird sichergestellt, dass nur die benötigten Funktionen der Software installiert werden.

Die Programme werden so konfiguriert, dass sie die Sicherheitsvorgaben der <Institution> erfüllen. Nicht benötigte Dienste und Funktionen werden im Rahmen der Software-Installation nicht mit installiert. Ist dies nicht möglich, sollten die Funktionen durch zentrale Management-Tools abgeschaltet werden. Jeweils vor und nach der Software-Installation werden von allen IT-Systemen ab hohen Schutzbedarf Datensicherungen durchgeführt.

## Standardmaßnahmen

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

### Festlegung der Verantwortlichkeiten im Bereich Standardsoftware (CON.4.A4)

Für die Einführung einer Standardsoftware werden Verantwortliche benannt. Unter anderem wird festgelegt wer:

* einen Anforderungskatalog erstellt,
* das Produkt auswählt,
* das Produkt testet,
* das Produkt freigibt und
* für die Installation verantwortlich ist.

Hierzu wird zusätzlich ein Einführungs- und Freigabeprozess definiert. Für den Betrieb von Standardsoftware werden technische und fachliche Produktverantwortliche benannt.

### Erstellung eines Anforderungskatalogs für Standardsoftware (CON.4.A5)

Vor der Software-Beschaffung wird ein Anforderungskatalog erstellt. Dieser beinhaltet neben den funktionalen auch Sicherheitsanforderungen. Dazu werden auch die Programmanforderungen der Anwender erhoben. Der fertige Anforderungskatalog wird mit allen betroffenen Abteilungen abgestimmt.

### Auswahl einer geeigneten Standardsoftware (CON.4.A6)

Anhand des Anforderungskatalogs sollten die am Markt erhältlichen Produkte gesichtet und mithilfe einer Bewertungsskala miteinander verglichen werden. Anschließend sollte untersucht werden, ob die Produkte aus der engeren Wahl die Anforderungen der <Institution> wirklich erfüllen. Sofern es mehrere Produktalternativen gibt, sollten auch zusätzliche Aufwände bspw. für Schulungen oder für die Migrationen berücksichtigt werden. Letztlich sollten die Anfordernden und Bertiebsverantwortlichen anhand der Bewertungen und Testergebnissen ein geeignetes Softwareprodukt auswählen.

### Überprüfung der Lieferung von Standardsoftware (CON.4.A7)

Es ist zu überprüfen, ob neue Softwareprodukte vollständig und korrekt geliefert wurden. Dabei ist mindestens zu kontrollieren, ob die Lieferung bestellt wurde, für wen sie bestimmt ist und ob alle notwendigen Komponenten vorhanden sind. Auch reine Download-Software ist inklusive zugehöriger Lizenzdateien oder -schlüsseln entsprechend zu prüfen. Die Ergebnisse der Überprüfung sollten dokumentiert werden. Anschließend sind alle gelieferten Produkte und Lizenzinformationen mit eindeutigen Identifizierungsmerkmalen zu versehen und in ein Bestandsverzeichnis zu übernehmen.

### Lizenzverwaltung und Versionskontrolle von Standardsoftware (CON.4.A8)

Alle lizenzpflichtigen Standardsoftware-Produkte, die auf IT-Systemen der <Institution> eingesetzt werden, sind zu lizenzieren. Mittels entsprechender Werkzeuge sollten regelmäßige Kontrollen der installierten Programmversionen und der Lizenzen stattfinden. Die Bestandslisten für die Lizenzen sind stets aktuell zu halten. Darüber hinaus sollten die verschiedenen Konfigurationen der installierten Standardsoftware dokumentiert werden.

### Deinstallation von Standardsoftware (CON.4.A9)

Bei der Deinstallation von Standardsoftware sind alle Dateien zu entfernen, die für den Betrieb der Software auf dem IT-System der <Institution> angelegt worden sind. Auch sind alle Einträge in Systemdateien zu löschen, die für die Standardsoftware vorgenommen wurden. Um Standardsoftware wieder vollständig deinstallieren zu können, sollten die während der Installation durchgeführten Systemänderungen entweder manuell oder mit entsprechenden Programmen dokumentiert 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).

### Implementierung zusätzlicher Sicherheitsfunktionen (CON.4.A10 - CIA)

Es ist zu prüfen, ob sich die Sicherheitsfunktionen der betriebenen Standardsoftware für einen erhöhten Schutzbedarf eignen. Ist das nicht der Fall, sollten geeignete Funktionen implementiert werden, um den Betrieb abzusichern.

Grundsätzlich ist ein erhöhter Schutzbedarf jedoch bereits zu beachten, wenn die Anforderungen definiert werden und das Produkt ausgewählt wird.

### Nutzung zertifizierter Standardsoftware (CON.4.A11 - CIA)

Bei der Beschaffung von Standardsoftware ist festzulegen, ob eine Zusicherung des Herstellers, Vertreibers oder Anbieters über implementierte Sicherheitsfunktionen als ausreichend vertrauenswürdig anerkannt werden kann. Ist dies nicht der Fall, sollte eine Zertifizierung der Standardsoftware nach Common Criteria als Entscheidungskriterium in Betracht gezogen werden. Stehen mehrere Produkte zur Auswahl sind Sicherheitsmerkmale insbesondere dann zu berücksichtigen, wenn der evaluierte Funktionsumfang die Mindestfunktionalität (weitestgehend) umfasst und die Mechanismenstärke dem Schutzbedarf entspricht. Gibt es auf dem Markt kein geeignetes und zertifiziertes Produkt ist die Einsatzumgebung entsprechend eines hohen Schutzbedarfes abzusichern.

### Einsatz von Verschlüsselung, Checksummen oder digitalen Signaturen (CON.4.A12 - CI)

Sofern Daten mit erhöhtem Schutzbedarf übertragen oder gespeichert werden, sind diese vorher zu verschlüsseln. Gibt es in einer Standardsoftware eine integrierte Verschlüsselungsfunktion, sollte geprüft werden, ob diese ausreichend sicher ist. Die Mitarbeiter sind im Umgang mit den Verschlüsselungsfunktionen zu schulen und sensibilisieren.