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

Sicherheitsrichtlinie "Office-Produkte"

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 | ISMS300045 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Office-Produkte" | [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](#_Toc81759996)

[Dokumentenhistorie 3](#_Toc81759997)

[Inhaltsverzeichnis 4](#_Toc81759998)

[Allgemeine Festlegungen 5](#_Toc81759999)

[Ziel / Zweck 5](#_Toc81760000)

[Geltungsbereich 5](#_Toc81760001)

[Zuständigkeiten 5](#_Toc81760002)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81760003)

[Aufbau des Dokuments 6](#_Toc81760004)

[Sicherheitsrichtlinie „Office-Produkte" 7](#_Toc81760005)

[Basismaßnahmen 7](#_Toc81760006)

[Sicherstellen der Integrität von Office-Produkten (APP.1.1.A1) 7](#_Toc81760007)

[Einschränken von Aktiven Inhalten (APP.1.1.A2) 7](#_Toc81760008)

[Sicheres Öffnen von Dokumenten aus externen Quellen (APP.1.1.A3) 7](#_Toc81760009)

[Absichern des laufenden Betriebs von Office-Produkten (APP.1.1.A4) 7](#_Toc81760010)

[Standardmaßnahmen 8](#_Toc81760011)

[Auswahl geeigneter Office-Produkte (APP.1.1.A5) 8](#_Toc81760012)

[Testen neuer Versionen von Office-Produkten (APP.1.1.A6) 8](#_Toc81760013)

[Installation und sichere Standardkonfiguration von Office-Produkten (APP.1.1.A7) 8](#_Toc81760014)

[Regelmäßige Versionskontrolle von Office-Produkten (APP.1.1.A8) 9](#_Toc81760015)

[Beseitigung von Restinformationen vor Weitergabe von Dokumenten (APP.1.1.A9) 9](#_Toc81760016)

[Regelung der Software-Entwicklung durch Endbenutzer (APP.1.1.A10) 9](#_Toc81760017)

[Geregelter Einsatz von Erweiterungen für Office-Produkte (APP.1.1.A11) 9](#_Toc81760018)

[Verzicht auf Cloud-Speicherung (APP.1.1.A12) 10](#_Toc81760019)

[Verwendung von Viewer-Funktionen (APP.1.1.A13) 10](#_Toc81760020)

[Schutz gegen nachträgliche Veränderungen von Dokumenten (APP.1.1.A14) 10](#_Toc81760021)

[Maßnahmen bei erhöhtem Schutzbedarf 10](#_Toc81760022)

[Einsatz von Verschlüsselung und Digitalen Signaturen (APP.1.1.A15 - CI) 11](#_Toc81760023)

[Integritätsprüfung von Dokumenten (APP.1.1.A16 - I) 11](#_Toc81760024)

# Allgemeine Festlegungen

## Ziel / Zweck

Die Gruppe der Office-Produkte umfasst in erster Linie solche Anwendungen, die dazu dienen, Dokumente zu betrachten, zu bearbeiten oder zu erstellen. Dazu zählen unter anderem die freie Anwendung LibreOffice und die proprietäre Anwendung Microsoft Office, Google GSuite (Docs, Tabellen, Präsentationen) und Apple iWorks (Pages, Numbers, Keynote). Office-Produkte gehören für die <Institution> zur notwendigen IT-Grundausstattung. Sie umfassen unter anderem Programme zur Textverarbeitung, Tabellenkalkulation und Erstellung von Präsentationen sowie Zeichenprogramme. Die Nutzung von Office-Anwendungen ermöglicht und vereinfacht es, der <Institution> Informationen zu erheben und zu verarbeiten.

Ziel der vorliegenden Sicherheitsrichtlinie ist der Schutz der Informationen, die durch Office-Produkte verarbeitet und genutzt werden. Dazu werden spezielle Anforderungen an die Funktionsweise der Komponenten von Office-Produkten gestellt. Die Sicherheitsrichtlinie zeigt Anforderungen auf, die zur Absicherung von Office-Produkten vor spezifischen Gefährdungen umgesetzt werden sollten. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines APP.1.1 "Office-Produkte" beachtet.

## 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 „Office-Produkte“ 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 „Office-Produkte"

## Basismaßnahmen

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

### Sicherstellen der Integrität von Office-Produkten (APP.1.1.A1)

Bei der Installation von Office-Produkten ist sicherzustellen, dass ausschließlich unveränderte Kopien der freigegebenen Originalsoftware verwendet werden. Spätere Updates zur Behebung von Sicherheitslücken oder zur Erweiterung des Funktionsumfanges sind ausschließlich aus sicheren Quellen zu beziehen. Falls zu einem Office-Produkt Prüfsummen angeboten werden, sind diese vor der manuellen Installation bzw. Integration in die zentrale Software-Enrollment-Infrastruktur zu überprüfen. Falls zu einem Office-Produkt digitale Signaturen verfügbar sind, sollten diese vor der Installation des Pakets manuell oder automatisiert durch Einsatz von entsprechenden Audit-Tools überprüft werden. Im Rahmen des etablierten Schulungsprogramms, sollten die Administratoren über die Bedeutung und Aussagekraft von Prüfsummen und digitalen Signaturen informiert werden.

### Einschränken von Aktiven Inhalten (APP.1.1.A2)

Da Malware das automatische Ausführen von eingebetteten aktiven Inhalten (Makros oder ActiveX-Elementen) sehr häufig zur Infektion des Systems oder der kompletten Infrastruktur missbraucht, sind in den Einstellungen aller verwendeten Office-Produkte das automatische Anführen von Macros oder ActiveX-Elementen zu deaktiviert werden.

Wird das Ausführen Aktiver Inhalte für einen Geschäftsprozess benötigt, ist das Ausführen nur von vertrauenswürdigen Quellen im vertraulichen Bereich (Trusted Location) erlaubt.

Alle Mitarbeitenden sind im Rahmen von Schulungen bezüglich der Gefährdungen durch Aktive Inhalte zu sensibilisieren und in Bezug auf die Funktionen zum Einschränken Aktiver Inhalte einzuweisen.

### Sicheres Öffnen von Dokumenten aus externen Quellen (APP.1.1.A3)

Alle Dokumente, die aus externen Quellen bezogen werden, sind vor dem Öffnen auf Schadsoftware durch die etablierte Anti-Malware-Infrastruktur zu überprüfen. Alle als problematisch eingestuften und innerhalb der <Institution> nicht benötigten Dateiformate (bspw. \*.cpl, \*.dll, \*.ocx, \*.sys, \*.scr, \*.drv, \*.efi, \*.fon, \*.pif und zusätzlich \*.HLP, \*.LNK, \*.CHM, \*.BAT, \*.VBE) sind verboten.

Die Prüfung von Dokumenten aus externen Quellen sollte durch technische Maßnahmen erzwungen werden. Das automatische Öffneten von Dateien mit bekannten Dateiformat ist ebenfalls technisch zu unterbinden.

### Absichern des laufenden Betriebs von Office-Produkten (APP.1.1.A4)

Die Betriebsverantwortlichen für die Office-Produkte müssen sich aktiv über bekannt gewordene Schwachstellen informieren. Bekannt gewordene Schwachstellen für das betreute Produkt zeitnah in Abhängigkeit vom Schutzbedarf und der Kritikalität zu beheben bzw. zu mitigieren.

Die Einschätzung der Relevanz von Sicherheitsaktualisierungen oder sicherheitsrelevanten Änderungen erfolgt in Abstimmung mit dem <Informationssicherheitsbeauftragter>. Vorab sollte auf Testsystemen überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen sowie die vereinbarten Schutzbedürfnisse nicht reduzieren. Solange keine Patches für bekannte und relevante Schwachstellen verfügbar sind, müssen geeignete Maßnahmen getroffen werden, um die durch Office-Produkte verarbeiteten Informationen und die Infrastruktur der <Institution> zu schützen.

Die Mitarbeitenden werden im Rahmen der Schulungsprogramme über die Möglichkeiten und Grenzen von Sicherheitsfunktionen der eingesetzten Software und der genutzten Speicherformate informiert. Die Vorgaben für die sichere Nutzung von Office-Produkten sind in der Sicherheitsrichtlinie enthalten.

## Standardmaßnahmen

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

### Auswahl geeigneter Office-Produkte (APP.1.1.A5)

Vor der Beschaffung von Office-Anwendungen sollte ein Anforderungskatalog erstellt werden. Die Erhebung der Anforderungen sollte durch Schlüsselanwender und deren Scope in den einzelnen Fachbereichen erfolgen. Anhand des erstellten Anforderungskatalogs sollten die am Markt erhältlichen Produkte verglichen werden. Sofern mehrere Produkte in Frage kommen, sollten zusätzlich die Aufwände für das Enrollment, die Pflege, die Migration und Schulung sowie die Interoperabilität mit Kunden und anderen externen Ansprechpartnern berücksichtigt. Sollten das Office-Produkt selbst als Cloud-App oder darin ein festintegrierte Cloud-Speicherplatz angeboten werden, sind zusätzlich die gesetzlichen und internen Anforderungen aus dem Datenschutz mit zu berücksichtigen.

### Testen neuer Versionen von Office-Produkten (APP.1.1.A6)

Neue Versionen von Office-Produkten sollten vor dem produktiven Einsatz auf Kompatibilität mit etablierten Arbeitsmitteln wie Vorlagen oder Formularen geprüft werden. Zu diesem Zweck sollten Testmethoden für die Einzeltests (Testarten, -verfahren und -werkzeuge) entwickelt und freigegeben werden. Es sollte sichergestellt sein, dass wichtige Arbeitsmittel auch mit der neuen Software-Funktion einwandfrei funktionieren. Bei entdeckten Inkompatibilitäten sollte ein Migrationsplan für die betroffenen Dokumente erstellt werden.

### Installation und sichere Standardkonfiguration von Office-Produkten (APP.1.1.A7)

Für alle eingesetzten Office-Produkte ist eine am Bedarf der <Institution> angepasste Standardkonfiguration zu erstellen und zu nutzen. Diese Konfiguration sollte in einer Installations- und Konfigurationsanweisung dokumentiert werden. Bei der Entwicklung der Standardkonfiguration soll auf die Härtungsempfehlungen des Herstellers und Sicherheitsexperten geachtet werden.

Alle Abweichungen vom etablierten Konfigurationsstandard sind zu dokumentieren und durch geeignete Freigabeprozesse zu genehmigen. Pilot-Installationen werden durch die IT durchgeführt. Jeweils vor und nach der Installation werden von allen beteiligten IT-Systemen Datensicherungen erstellt. Im Falle von Pilot-Installationen gilt, dass die Pilot-Installation immer durch das für den späteren Betrieb verantwortliche Department begleitet werden sollte. Vor und nach den Installationen sollten Datensicherungen der Office-Produkte auf allen betroffenen IT-Systemen durchgeführt werden.

### Regelmäßige Versionskontrolle von Office-Produkten (APP.1.1.A8)

Die installierten Versionen von Office-Produkten sollten regelmäßig kontrolliert werden. Diese Bestandsführung der Software-Lizenzen ist bei jeder Installation oder Deinstallation zu aktualisieren.

### Beseitigung von Restinformationen vor Weitergabe von Dokumenten (APP.1.1.A9)

Werden Office-Dokumente von Mitarbeitenden an Dritte weitergegeben, sind zuvor alle nicht benötigten und alle vertraulichen Restinformationen im eigentlichen Text aus den Dokumenten zu entfernen. Ebenfalls sind die Metadaten der Office-Dokumente zu bereinigen. Im Rahmen der etablierten Schulungsprogramme sollten alle Mitarbeitenden bezüglich der Risiken durch Restinformationen in den eingesetzten Office-Produkten sensibilisiert werden, wie sie Restinformationen beseitigen können. Dokumente sollten in einem nicht veränderbaren Format bspw. als PDF übermittelt werden, wenn keine Bearbeitung durch den Empfänger erforderlich ist.

### Regelung der Software-Entwicklung durch Endbenutzer (APP.1.1.A10)

Es sollten verbindliche Regelungen für die Software-Entwicklung auf Basis von Office-Anwendungen, z. B. Makros oder Tabellenkalkulationen, durch Mitarbeitende oder Dienstleister zu treffen. Im ersten Schritt sollte die Grundsatzentscheidung getroffen werden, ob solche Eigenentwicklungen überhaupt erwünscht sind. Diese Entscheidung ist geeignet zu dokumentieren.

Sofern Eigenentwicklungen erlaubt werden, sind diese mit einer internen Zertifikatssignatur auszustatten und innerhalb des etablierten Freigabeprozesses in die relevanten produktiven Prozesse bzw. Workflows zu übergeben.

Alle Informationen über die erstellten Eigenentwicklungen sind zentral zu dokumentieren. Die aktuell gültige Version sind allen betroffenen Mitarbeitenden zeitnah zugänglich zu machen bzw. in das zentrale Softwaremanagement zu übergeben.

### Geregelter Einsatz von Erweiterungen für Office-Produkte (APP.1.1.A11)

Alle Erweiterungen von Office-Produkten sollten vor dem produktiven Einsatz analog zum Testvorgehen von neuen Versionen getestet werden. Die Tests sollten ausschließlich auf isolierten Testsystemen durchgeführt werden. Die Tests sollten prüfen, dass Erweiterungen keine negativen Auswirkungen auf die Office-Produkte und auf die Vertraulichkeit der Inhalte in den Dokumenten haben. Die Tests der eingesetzten Erweiterungen sollten einem definierten Testplan folgen, damit Dritte das Testvorgehen nachvollziehen zu können.

### Verzicht auf Cloud-Speicherung (APP.1.1.A12)

Die in den Office-Produkten bspw. der Firma Microsoft, Apple oder Google integrierten Cloud-Speicher-Funktionen sollten sofern nicht zwingend benötigt deaktiviert werden.

Alle Dokumente sollten bevorzugt durch die Mitarbeitenden auf zentral verwalteten File-Servern der <Institution> gespeichert werden. Sofern die Cloud-Speicher-Funktionen und Cloud-Laufwerke benötigt werden, ist zu regeln, wie dieses unter Einhaltung der sicherheitstechnischen und datenschutzrechtlichen Anforderungen umsetzbar ist.

Um Dokumente für Dritte freizugeben, sollten spezialisierte Anwendungen bzw. Datenräume eingesetzt werden, die über Sicherheitsfunktionen wie eine verschlüsselte Datenablage und -versendung sowie ein geeignetes System zur Benutzer- und Rechteverwaltung verfügen.

### Verwendung von Viewer-Funktionen (APP.1.1.A13)

Daten aus potenziell unsicheren Quellen wie dem Internet oder unverschlüsselte Anhänge von E-Mail-Nachrichten von unbekannten Absendern sollten automatisch in einem geschützten Modus geöffnet werden, in dem diese Daten oder Anhänge nicht unmittelbar bearbeitet werden können. Nur eine allgemeine Navigation sollte ermöglicht werden und nicht durch den Mitarbeitenden deaktiviert werden können. Sofern die Dokumente lediglich betrachtet werden sollen, sollten bevorzugt entsprechende Viewer-Anwendungen von den Mitarbeitenden verwendet werden. Zur Reduzierung des potentiellen Angriffsvektors, sollte eine Liste vertrauenswürdiger Orte definiert werden, von denen nicht erwartete Dokumente oder Dateianhänge unmittelbar geöffnet und bearbeitet werden können.

### Schutz gegen nachträgliche Veränderungen von Dokumenten (APP.1.1.A14)

Je nach geplantem Verwendungszweck von Dokumenten oder dem Eigentümer der Dokumente sollten die in Office-Produkten vorhandenen Sicherheitsmechanismen genutzt werden, um den weiteren Umgang bzw. die generelle Bearbeitung mit den erstellten Dateien einzuschränken. Die Mitarbeitenden sollten darauf hingewiesen werden, wie diese Sicherheitsmechanismen funktionieren und wie sie anzuwenden sind.

## 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).

### Einsatz von Verschlüsselung und Digitalen Signaturen (APP.1.1.A15 - CI)

Daten mit erhöhtem Schutzbedarf sind vor einer Übertragung oder Speicherung im Cloud-Speicher lokal auf dem Notebook, Smartphone oder Tablet zu verschlüsseln. Vor der Nutzung eines in ein Office-Produkt integrierten Verschlüsselungsverfahrens ist zu prüfen, ob das Verfahren einen ausreichenden Schutz bietet und ob die verwendeten kryptographischen Protokolle den Standards der <Institution> entsprechen. Die IT-Systeme von Absender und Empfänger sollten den Zugriffsschutz auf die verwendete Methode zur Verschlüsselung gewährleisten. Mitarbeitenden sollten im Umgang mit den Verschlüsselungsfunktionen sensibilisiert und geschult werden. Zusätzlich ist ein Verfahren zu etablieren, mit dem Makros und Dokumente digital signiert werden können. Die Gültigkeit der verwendeten Zertifikate sollte dem Schutzbedarf entsprechend zeitlich begrenzt werden.

### Integritätsprüfung von Dokumenten (APP.1.1.A16 - I)

Zum Schutz vor zufälliger Veränderung von Daten mit erhöhtem Schutzbedarf bei einer Übertragung sowie Speicherung sollten Prüfsummenverfahren eingesetzt werden. Es sollte ein Verfahren ausgewählt werden, das dazu in der Lage ist, die Daten selbstständig zu korrigieren. Zum Schutz vor Manipulation sind kryptografische Prüfsummenverfahren einzusetzen.