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

Sicherheitsrichtlinie "Drucker, Kopierer und Multifunktionsgeräte"

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 | ISMS300035 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Drucker, Kopierer und Multifunktionsgeräte" | [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](#_Toc81037053)

[Dokumentenhistorie 3](#_Toc81037054)

[Inhaltsverzeichnis 4](#_Toc81037055)

[Allgemeine Festlegungen 5](#_Toc81037056)

[Ziel / Zweck 5](#_Toc81037057)

[Geltungsbereich 5](#_Toc81037058)

[Zuständigkeiten 5](#_Toc81037059)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81037060)

[Aufbau des Dokuments 6](#_Toc81037061)

[Sicherheitsrichtlinie „Drucker, Kopierer und Multifunktionsgeräte" 7](#_Toc81037062)

[Basismaßnahmen 7](#_Toc81037063)

[Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A1) 7](#_Toc81037064)

[Geeignete Aufstellung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A2) 7](#_Toc81037065)

[Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln (SYS.4.1.A12) 7](#_Toc81037066)

[Ordnungsgemäße Entsorgung ausgedruckter Dokumente (SYS.4.1.A22) 7](#_Toc81037067)

[Standardmaßnahmen 8](#_Toc81037068)

[Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten (SYS.4.1A4) 8](#_Toc81037069)

[Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A5) 8](#_Toc81037070)

[Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (SYS.4.1.A7) 8](#_Toc81037071)

[Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A11) 8](#_Toc81037072)

[Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A15) 9](#_Toc81037073)

[Schutz von Nutz- und Metadaten (SYS.4.1.A17) 9](#_Toc81037074)

[Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A18) 9](#_Toc81037075)

[Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A19) 9](#_Toc81037076)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc81037077)

[Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A14 - CI) 10](#_Toc81037078)

[Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A16 - A) 10](#_Toc81037079)

[Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A20 - C) 10](#_Toc81037080)

[Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A21 - C) 11](#_Toc81037081)

# Allgemeine Festlegungen

## Ziel / Zweck

Moderne Drucker, Kopierer und Multifunktionsgeräte sind komplexe Geräte, die neben mechanische Komponenten eigene Betriebssysteme enthalten und Serverdienste und -funktionen bereitstellen. Drucker, Kopierer und Multifunktionsgeräte oft vertrauliche Informationen verarbeiten, bedeutet dies, dass diese sowie die gesamte Druck- und Scan-Infrastruktur der <Institution> geschützt werden muss.

Für einige wichtige Geschäftsprozesse der <Institution> wird noch Papier als Informationsträger benutzt. Damit sind Drucker, Kopierer oder Multifunktionsgeräte wichtige Komponenten in der IT-Infrastruktur der <Institution>. Fallen die Geräte aus oder werden verfälschte Dokumente ausgedruckt, könnte sich das mitunter auf kritische Prozesse auswirken und zu wirtschaftlichen Schäden führen.

Diese Sicherheitsrichtlinie beschreibt, wie sich Drucker, Kopierer und Multifunktionsgeräte sicher betreiben lassen, sodass weder Informationen über diese Geräte abfließen können noch durch sie die Sicherheit der übrigen internen IT-Infrastruktur beeinträchtigt wird. Für die Erstellung dieser Sicherheitsrichtlinie wurde auf die Vorgaben des BSI Bausteines SYS.4.1 "Drucker, Kopierer und Multifunktionsgeräte" 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 „Drucker, Kopierer und Multifunktionsgeräte“ 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 „Drucker, Kopierer und Multifunktionsgeräte"

## Basismaßnahmen

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

### Planung des Einsatzes von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A1)

Die <Institution> muss den sicheren Einsatz von Druckern, Kopierern und Multifunktionsgeräten planen. Bei der Planung sind auch Cloud-basierte Drucker zu berücksichtigen. Von besonderer Bedeutung im Rahmen der Planung ist, wo die Geräte aufgestellt werden dürfen. Außerdem ist festzulegen, wer auf die Drucker, Kopierer und Multifunktionsgeräte zugreifen darf. Die Ergebnisse sollten in einem Basiskonzept dokumentiert werden.

### Geeignete Aufstellung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A2)

Drucker, Kopierer und Multifunktionsgeräte sind so aufzustellen und abzusichern, dass nur befugte Benutzer die Geräte verwenden und auf verarbeitete Informationen zugreifen können. Außerdem ist sicherzustellen, dass nur berechtigte Mitarbeitende die Geräte administrieren, warten und reparieren können. Mit Dienstleistern (z. B. für die Wartung) sind schriftliche Vertraulichkeitsvereinbarungen zu treffen.

Drucker, Kopierer und Multifunktionsgeräte müssen mit Passwörtern für den administrativen Zugriff auf das Geräte versehen sein, um so den Zugriff per Webserver und Bedienfeld zu sperren. Die hinterlegten Passwörter müssen die internen Vorgaben erfüllen. Das Passwort darf nur berechtigten Mitarbeitenden bekannt sein.

### Ordnungsgemäße Entsorgung von Geräten und schützenswerten Betriebsmitteln (SYS.4.1.A12)

Vor der Außerbetriebnahme sind alle internen Speicher sicher zu löschen und/oder aus dem Gerät zu entferne. Alle auf dem Gerät befindlichen Aufkleber, die auf die Verwendung hinweisen, sind zu entfernen.

Alle zur Vernichtung vorgesehenen Geräte sind einem zertifizierten Unternehmen zu zuführen, welches für die Vernichtung verantwortlich ist.

### Ordnungsgemäße Entsorgung ausgedruckter Dokumente (SYS.4.1.A22)

Nicht benötigte, aber ausgedruckte Dokumente mit vertraulichen Informationen sind in geeigneter Weise zu vernichten, z. B. in geeigneten Papiercontainern oder Aktenvernichtern. Sind Homeoffice-Plätze mit Druckern, Kopierern oder Multifunktionsgeräten ausgestattet, sollte gewährleistet werden, dass die ausgedruckten Informationen auch direkt vor Ort geeignet vernichtet werden können.

## Standardmaßnahmen

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

### Erstellung eines Sicherheitskonzeptes für den Einsatz von Druckern, Kopieren und Multifunktionsgeräten (SYS.4.1A4)

Es sollte ein Sicherheitskonzept für Drucker, Kopierer und Multifunktionsgeräte entwickelt werden. Darin sollte geregelt werden, welche Anforderungen und Vorgaben an die Informationssicherheit der Geräte gestellt und wie diese erfüllt werden sollen. Es sollte auch festgelegt werden, welche Funktionen von welchen Mitarbeitenden unter welchen Bedingungen administriert beziehungsweise genutzt werden dürfen. Der Information Security Officer sollte auf Basis des Sicherheitskonzepts eine Administrationsrichtlinie ausarbeiten.

### Erstellung von Benutzerrichtlinien für den Umgang mit Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A5)

Für die Mitarbeitenden sollte der Information Security Officer ein Merkblatt erstellen, auf dem alle Sicherheitsvorgaben zum Umgang mit den Geräten übersichtlich und verständlich zusammengefasst sind. Das Merkblatt sollte allen Mitarbeitenden bekannt sein.

### Beschränkung der administrativen Fernzugriffe auf Drucker, Kopierer und Multifunktionsgeräte (SYS.4.1.A7)

Die Verantwortlichen für die Office-IT sollten sicherstellen, dass der administrative Fernzugriff auf Drucker, Kopierer und Multifunktionsgeräte nur einer klar definierten Gruppe an Administratoren und Servicetechnikern ermöglicht wird. Das sollte auch dann gewährleistet sein, wenn die <Institution> eine zentrale Geräteverwaltungssoftware einsetzt.

Es sollte festgelegt werden, ob die Anzeige des Bedienfelds über ein Datennetz eingesehen werden kann. Wenn dies gewünscht ist, sollte es nur an die Verantwortlichen für die Office-IT übertragen werden können.

### Einschränkung der Anbindung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A11)

Die Verantwortlichen für die Office-IT sollten sicherstellen, dass Netzdrucker und Multifunktionsgeräte nicht aus Fremdnetzen erreichbar sind. Wenn Multifunktionsgeräte an das Internet oder Mobilfunknetz oder Telefonnetz angeschlossen werden, sollte sichergestellt werden, dass keine unkontrollierten Datenverbindungen aufgebaut werden können. Netzdrucker und Multifunktionsgeräte sind in einem eigenen Netzsegment, das von den Clients und Servern der <Institution> getrennt ist, betrieben werden.

### Verschlüsselung von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A15)

Alle auf geräteinternen, nichtflüchtigen Speichermedien (z. B. Festplatten, SSDs) abgelegten Informationen sollten verschlüsselt werden. Auch die Druckaufträge selbst sollten möglichst verschlüsselt übertragen werden.

### Schutz von Nutz- und Metadaten (SYS.4.1.A17)

Nutz- und Metadaten von Scan- und Druckaufträgen und deren Dateien sollten nur so kurz wie möglich auf den Geräten gespeichert werden. Die Daten sollten nach einer vordefinierten Zeit automatisch gelöscht werden. Dateiserver in den Geräten und Funktionen wie „Scan in den Gerätespeicher" sollten von den Verantwortlichen für die Office-IT abgeschaltet werden. Die dafür benötigten Protokolle und Funktionen sollten gesperrt werden.

Generell sollte von den Verantwortlichen für die Office-IT sichergestellt werden, dass alle Metadaten bspw. von Druckaufträgen nicht für Unberechtigte sichtbar sind. Es sollte von der <Institution> geregelt werden, wie mit Metadaten versehene Ausdrucke an Dritte weitergegeben werden.

### Konfiguration von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A18)

Alle Drucker und Multifunktionsgeräte sollten geeignet von den Verantwortlichen für die Office-IT konfiguriert werden. Nicht benötigte Gerätefunktionen sind abzuschalten. Die Geräte sollten ausschließlich über verschlüsselte Protokolle wie HTTPS und SNMPv3 verwaltet werden. Sämtliche Protokolle, mit denen unverschlüsselt auf Drucker und Multifunktionsgeräte zugegriffen werden kann, sollten von den Verantwortlichen für die Office-IT durch verschlüsselte ersetzt oder abgeschaltet werden. Dies gilt insbesondere für Protokolle mit denen sich die Gerätekonfiguration verändern lässt, z. B. SNMP, Telnet und PJL. Der voreingestellte „SNMP Set Community Name" ist zu ändern.

### Sicheres Löschen von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A19)

Es ist sicherzustellen, dass gelöschte Daten nicht rekonstruierbar sind. Die Daten sollten automatisch mit Zufallswerten überschrieben werden. Alle nicht mehr benötigten kryptografischen Schlüssel und Zertifikate sind sicher zu löschen.

## 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).

### Authentisierung und Autorisierung bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A14 - CI)

Es sollten nur berechtigte Mitarbeitende auf die ausgedruckten oder kopierten Dokumente zugreifen können.

Es sollten möglichst nur zentrale Drucker, Kopierer und Multifunktionsgeräte eingesetzt werden, bei denen sich die Mitarbeitenden authentisieren müssen, bevor sie diese benutzen können. Es sollten nur die für die jeweiligen Mitarbeitenden notwendigen Funktionen freigeschaltet werden. Nachdem sich die Mitarbeitenden authentisiert haben, sollten ausschließlich die eigenen Druckaufträge sichtbar sein.

### Notfallvorsorge bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A16 - A)

Die Ausfallzeiten von Druckern, Kopierern und Multifunktionsgeräten sollte so gering wie möglich sein. Deshalb sollten im Rahmen der Notfallvorsorge mindestens in den Wartungsverträgen auf eine angemessene Reaktionszeit geachtet werden und zusätzlich unter Berücksichtigung der Notwendigkeit

* Ersatzgeräte bereitstehen,
* eine Liste mit Fachhändlern geführt werden, um schnell Ersatzgeräte oder -teile beschaffen zu können oder
* falls erforderlich, häufig benötigte Ersatzteile gelagert werden.

### Erweiterter Schutz von Informationen bei Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A20 - C)

Druckdateien mit vertraulichen Informationen sind verschlüsselt zu übertragen. Auch sollten auf dem Druckserver die Namen der Druckaufträge nur anonymisiert angezeigt werden.

Alle Schnittstellen für externe Speichermedien sollten gesperrt bzw. deaktiviert werden.

Geräteinterne Adressbücher sind zu deaktivieren und den Benutzern alternative Adressbücher (z. B. Adresssuche per LDAP) angeboten werden.

Bei Druckern und Multifunktionsgeräten mit E-Mail-Funktion ist sicherzustellen, dass E-Mails ausschließlich mit der E-Mail-Adresse eines authentisierten Mitarbeitenden versendet werden können. Auch sollten Dokumente nur an interne E-Mail-Adressen verschickt werden können.

Eingehende Fax-Dokumente sowie Sendeberichte sollten nur autorisierten Benutzern zugänglich sein.

### Erweiterte Absicherung von Druckern, Kopierern und Multifunktionsgeräten (SYS.4.1.A21 - C)

Die Sicherheitseinstellungen von Druckern, Kopierern und Multifunktionsgeräten sind regelmäßig zu kontrollieren. Sofern notwendig sind die Sicherheitseinstellungen zu korrigieren. Die Drucker, Kopierer und Multifunktionsgeräte sollten in ein automatisiertes Kontroll- und Korrektursystem eingefügt werden.

Die Sicherheitseinstellungen sollten einschränken, dass die Drucker, Kopierer und Multifunktionsgeräte über das Bootmenü auf die Werkseinstellungen zurückgestellt werden können. Es sollte ebenfalls sichergestellt sein, dass keine Firmware oder Zusatzsoftware in Druckern und Multifunktionsgeräten installiert werden kann, die nicht vom jeweiligen Hersteller verifiziert und freigegeben wurde.