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

Sicherheitsrichtlinie "Faxgeräte und Faxserver"

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 | ISMS300044 | [Die Dokumenten-Kennung wird von der Dokumentenlenkung vergeben] |
| Name des Dokuments | Sicherheitsrichtlinie "Faxgeräte und Faxserver" | [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](#_Toc81743504)

[Dokumentenhistorie 3](#_Toc81743505)

[Inhaltsverzeichnis 4](#_Toc81743506)

[Allgemeine Festlegungen 5](#_Toc81743507)

[Ziel / Zweck 5](#_Toc81743508)

[Geltungsbereich 5](#_Toc81743509)

[Zuständigkeiten 6](#_Toc81743510)

[Genehmigungs- und Änderungsverfahren 6](#_Toc81743511)

[Aufbau des Dokuments 6](#_Toc81743512)

[Sicherheitsrichtlinie „Faxgeräte und Faxserver" 7](#_Toc81743513)

[Basismaßnahmen 7](#_Toc81743514)

[Geeignete Aufstellung eines Faxgerätes (NET.4.3.A1) 7](#_Toc81743515)

[Informationen für alle Mitarbeitende über die Faxnutzung (NET.4.3.A2) 7](#_Toc81743516)

[Sicherer Betrieb eines Faxservers (NET.4.3.A3) 7](#_Toc81743517)

[Standardmaßnahmen 8](#_Toc81743518)

[Beschaffung geeigneter Faxgeräte und Faxserver (NET.4.3.A6) 8](#_Toc81743519)

[Geeignete Kennzeichnung ausgehender Faxsendungen (NET.4.3.A7) 8](#_Toc81743520)

[Geeignete Entsorgung von Fax-Verbrauchsgütern und –Ersatzteilen (NET.4.3.A8) 9](#_Toc81743521)

[Nutzung von Sende- und Empfangsprotokollen (NET.4.3.A9) 9](#_Toc81743522)

[Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten (NET.4.3.A10) 9](#_Toc81743523)

[Maßnahmen bei erhöhtem Schutzbedarf 9](#_Toc81743524)

[Schutz vor Überlastung des Faxgerätes (NET.4.3.A11 - A) 10](#_Toc81743525)

[Sperren bestimmter Faxempfänger-Rufnummern und Absender-Faxnummern (NET.4.3.A12 - CA) 10](#_Toc81743526)

[Festlegung berechtigter Faxbediener (NET.4.3.A13 - C) 10](#_Toc81743527)

[Fertigung von Kopien eingehender Fax-Sendungen (NET.4.3.A14 - A) 10](#_Toc81743528)

[Ankündigung und Rückversicherung im Umgang mit Fax-Sendungen (NET.4.3.A15 - C) 10](#_Toc81743529)

[Umgang mit Faxgeräten, die gleichzeitig einen Netzwerkanschluss haben (NET.4.3.b.d.A1 - CIA) 11](#_Toc81743530)

# Allgemeine Festlegungen

## Ziel / Zweck

In dieser Sicherheitsrichtlinie werden die Sicherheitsaspekte der Informationsübermittlung über marktübliche Faxgeräte sowie Faxserver für die <Institution> betrachtet. Die übermittelten Informationen werden als Fax (Kurzform von Telefax) oder seltener auch als Telefaksimile oder Fernkopie bezeichnet. Bei einem herkömmlichen Faxgerät werden von einer Vorlage die darauf aufgezeichneten Inhalte vom Sendegerät Punkt für Punkt abgetastet und zu einem Empfänger übertragen. Das Empfängergerät baut diese Inhalte wieder Punkt für Punkt auf und gibt sie in der Regel direkt auf Papier aus.

Ein Faxserver hingegen ist ein Dienst, der auf einem Server installiert wird und so anderen IT-Systemen in einem Datennetz ermöglicht, Faxe zu versenden und zu empfangen. Faxserver werden häufig in bereits bestehende E-Mail- oder Groupware-Systeme integriert. So ist es möglich, dass eingehende Fax-Dokumente durch den Faxserver per E-Mail an die Mitarbeitenden zugestellt werden. Abzusendende Dokumente werden entweder über eine Druckerwarteschlange oder per E-Mail an den Faxserver übergeben. In der Regel wird das Dokument zwischen Faxserver und den Clients im Datennetz als Bild-Datei gesendet oder empfangen. Die übermittelte Bild-Datei kann nicht unmittelbar in Textverarbeitungssystemen weiterverarbeitet werden. Hierzu ist in der Regel zunächst eine Texterkennung (OCR, Optical Character Recognition) erforderlich. Von einem Faxserver empfangene und verarbeitete Dokumente lassen sich für gewöhnlich einfach archivieren, beispielsweise durch den Faxserver-Dienst selber, durch Dokumentenmanagementsysteme oder durch die Groupware, die direkt an den Faxserver-Dienst angebunden sind.

Ein Ziel dieser Sicherheitsrichtlinie ist der Schutz der Informationen, die mithilfe von Faxsendungen übermittelt und verarbeitet werden. Ein weiteres Ziel ist der Schutz der Faxgeräte und Faxserver vor Manipulationen durch Unbefugte. Das Übertragungsmedium spielt bei der Anwendung dieser Sicherheitsrichtlinie keine Rolle, sodass die Anforderungen für Fax over IP (FoIP) mit umgesetzt werden sollten. Bei der Erstellung dieser Sicherheitsrichtlinie wurden die Vorgaben des BSI Bausteines NET.4.3 "Faxgeräte und Faxserver" 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 „Faxgeräte und Faxserver“ 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 „Faxgeräte und Faxserver"

## Basismaßnahmen

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

### Geeignete Aufstellung eines Faxgerätes (NET.4.3.A1)

Ein Faxgerät bzw. Multifunktionsgerät mit Fax-Funktion ist so aufzustellen, dass eingegangene Faxsendungen nicht von Unberechtigten eingesehen oder entnommen werden können. Um die Vertraulichkeit von eingehenden Fax-Nachrichten sicherstellen zu können, dürfen in frei öffentlich zugänglichen Bereichen der <Institution> keine Faxgeräte aufgestellt werden.

### Informationen für alle Mitarbeitende über die Faxnutzung (NET.4.3.A2)

Alle Mitarbeitende sind auf die Besonderheiten der Informationsübermittlung per Fax hinzuweisen und darüber zu informieren, dass die Rechtsverbindlichkeit einer Faxsendung stark eingeschränkt ist. Alle Benutzer erhalten eine Kurzanleitung zu folgenden Punkten.

* Wer Verantwortlich für das Fax ist und als Ansprechpartner bei Problemfällen zu kontaktieren ist.
* Welches einheitliche Deckblatt benutzt werden sollte.
* Dass der Sendenachweis bzw. Übertragungsprotokoll für die korrekte Übertragung zu kontrollieren ist und diese den Unterlagen beizufügen und bei Bedarf zu archivieren sind.
* Dass für das Dokumentenmanagement beim Einsatz eines Faxservers mit automatischer Eingangs-Fax- bzw. Ausgangs-Verteilung ein Ausdruck von Eingangs-Faxsendungen anzufertigen ist bzw. dieses bei Fax-To-Mail oder Mail-to-Fax elektronisch zu archivieren ist.
* Dass die Adressbücher und Verteillisten regelmäßig zu kontrollieren sind, damit die Faxe nicht versehentlich an falsche Empfänger gesendet werden.

Zudem liegen für die wichtigsten Funktionen des Faxgerätes eine kurze Bedienungsanleitung idealerweise am Gerät aus.

### Sicherer Betrieb eines Faxservers (NET.4.3.A3)

Für den sicheren Betrieb eines Faxservers ist sowohl die lokale Kommunikation als auch die Kommunikation aufseiten des öffentlichen Netzes abzusichern. Der Faxserver muss zudem sicherstellen, dass lokale Sendungen, d. h. senden von Faxen von einem Arbeitsplatz zu einem anderen innerhalb der <Institution>, nur intern und nicht über das öffentliche Netz weitergeleitet werden.

Zum sicheren Betrieb eines Faxservers ist es u. a. erforderlich, dass nach der Beschaffung und Installation die Konfiguration des Betriebssystems und der Faxserver-Applikation ausgiebig getestet wird. Zudem ist regelmäßig die Verbindung vom Faxserver zur TK-Anlage beziehungsweise dem öffentlichen Telefonnetz auf ihre Funktion zu prüfen.

Der Faxserver bietet ausschließlich Fax-Dienste an und darf nicht für weitere Dienste genutzt werden. Alle nicht benötigen Funktionen, Dienste und Zugänge der eingesetzten Kommunikationsschnittstellen sind zu deaktivieren. Der Faxserver muss alle eingehenden und ausgehenden Faxsendungen speichern. Es ist zu regeln, wo und in welchem Umfang die Fax-Daten zu archivieren sind.

## Standardmaßnahmen

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

### Beschaffung geeigneter Faxgeräte und Faxserver (NET.4.3.A6)

Für die Beschaffung geeigneter Faxgeräte und Fax-Server sollte eine Anforderungsliste erstellt werden. Anhand dieser Liste erfolgt eine Bewertung der infrage kommenden Systeme und Komponenten. In der Anforderungsliste sind ebenfalls die sicherheitsrelevanten Aspekte definiert wie

* Austausch einer Teilnehmererkennung,
* Ausgabe von Sendeberichten und
* Fehlerprotokollierung und Journalführung.

Ebenfalls wurden angemessene zusätzliche Sicherheitsfunktionen anhand des für die <Institution> zu erfüllenden Schutzbedarfs berücksichtigt.

Bei Fax-Servern sind alle Anforderungen an das IT-System einschließlich Betriebssystem, Kommunikationskomponenten und Applikationssoftware zu erheben und zu berücksichtigen. Zudem ist die mögliche Integration eines Fax-Servers in eine bestehende VoIP- und E-Mail-Infrastruktur in der aktuell von der <Institution> betriebenen Version zu berücksichtigen.

### Geeignete Kennzeichnung ausgehender Faxsendungen (NET.4.3.A7)

Grundsätzlich sind aus allen ausgehenden Faxsendungen sowohl der Sender als auch der gewünschte Empfänger ersichtlich. Sollten die Informationen aus dem versendeten Dokument nicht identifizierbar sein, ist ein standardisiertes Faxdeckblatt zu nutzen. Die einzutragenden Informationen sind im Voraus als Standard zu definieren. Das Faxdeckblatt für öffentliche Kommunikation sollte die folgenden Informationen beinhalten:

* den Firmennamen des Absenders,
* Ansprechpartner beim Absender,
* den Firmennamen des Empfängers,
* das Datum,
* die Seitenanzahl sowie
* einen Dringlichkeitsvermerk.

Für die Kommunikation innerhalb der <Institution> sollte zusätzlich noch der Schutzbedarf mit aufgenommen werden.

### Geeignete Entsorgung von Fax-Verbrauchsgütern und –Ersatzteilen (NET.4.3.A8)

Alle Fax-Verbrauchsgüter, aus denen Informationen über die versendeten und empfangenden Fax-Dokumente gewonnen werden können, sowie ausgetauschte informationstragende Ersatzteile, werden vor der Entsorgung sicher vernichtet oder durch eine zuverlässige Fachfirma sicher entsorgt.

Wartungsfirmen, die Faxgeräte innerhalb der <Institution> warten oder reparieren, werden auf eine entsprechende Verschwiegenheit verpflichtet.

### Nutzung von Sende- und Empfangsprotokollen (NET.4.3.A9)

Für herkömmliche Faxgeräte sollten listenmäßige Protokolle von Übertragungsvorgängen, die automatisch vom Faxgerät geführt werden (Kommunikationsjournal) regelmäßig ausgedruckt werden. Es ist festzulegen, wer diese Ausdrucke veranlasst, wo und wie lange sie aufbewahrt werden und in welcher Weise die Protokollausdrucke stichprobenartigen Prüfungen auf Unregelmäßigkeiten unterzogen werden.

Auch auf Fax-Servern sind die Übertragungsvorgänge zu protokollieren. Diese Protokolle sind regelmäßig auszuwerten und zu archivieren. Die Rahmenbedingungen und Zuständigkeiten für die Auswertung und Archivierung der Protokolle sind festzulegen.

Die manuelle Auswertung der Kommunikationsjournale darf nur im Beisein des <Informationssicherheitsbeauftragter> erfolgen. Über die Ergebnisse einer automatisierten Auswertung sind der <Informationssicherheitsbeauftragter> zu informieren. Auf die Erfordernisse des Datenschutzgesetzes (BDSGneu) ist Rücksicht zu nehmen. Insbesondere ist der Zugriff auf die Kommunikationsjournale durch Unbefugte zu verhindern.

### Kontrolle programmierbarer Zieladressen, Protokolle und Verteilerlisten (NET.4.3.A10)

Programmierbare Kurzwahltasten oder Zieladressenspeicherungen sind regelmäßig daraufhin zu überprüfen, ob die gewünschte mit der einprogrammierten Faxnummer übereinstimmt. Alle nicht mehr benötigten Faxnummern sind zu löschen. Die Aufnahme eines neuen Eintrags oder das Ändern einer Zielnummer ist über die etablierten Prozesse zu steuern und zu dokumentieren.

## 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).

### Schutz vor Überlastung des Faxgerätes (NET.4.3.A11 - A)

Zum Schutz vor Überlastung sind ausreichend Kommunikations-Leitungen bzw. Kanäle bereitzustellen. Bei den Fax-Servern wird das voraussichtliche Faxvolumen abgeschätzt und regelmäßig mit dem aktuellen abgeglichen und an die aktuellen Erfordernisse angepasst. Nicht mehr benötigte Fax-Daten werden zeitnah vom Faxserver gelöscht.

### Sperren bestimmter Faxempfänger-Rufnummern und Absender-Faxnummern (NET.4.3.A12 - CA)

Das zufällige oder absichtliche Versenden von Informationen oder Unterlagen per Fax an eine nicht gewünschte Empfängerrufnummer ist zu verhindern. Falls erforderlich, darf die Fax-Absenderkennung (Call Subscriber ID) zur Auswertung herangezogen werden. Sofern die Fax-Absenderkennung ausgewertet wird, ist sicherzustellen, dass der Fax-Absender die eigene Rufnummernübermittlung nicht unterdrücken und die übermittelte Rufnummer sowie die Absenderkennung nicht manipulieren kann.

### Festlegung berechtigter Faxbediener (NET.4.3.A13 - C)

Die Berechtigung zur Bedienung des Faxgerätes sind auf einen ausgewählten Kreis zuverlässiger Mitarbeitende zu beschränken. Die berechtigten Mitarbeitenden sind in die korrekte Handhabung einzuweisen sowie mit den erforderlichen Sicherheitsmaßnahmen vertraut zu machen. Jeder berechtigte Mitarbeitende ist darüber zu unterrichten, wer das Fax-Gerät bedienen darf und wer für das Fax verantwortlich ist.

### Fertigung von Kopien eingehender Fax-Sendungen (NET.4.3.A14 - A)

Auf Thermopapier gedruckte Fax-Sendungen, die längerfristig benötigt werden, sind auf Normalpapier zu kopieren oder einzuscannen. Die Kopien oder eingescannte Fax-Sendungen sind vor unberechtigten Zugriff zu schützen und zu archivieren.

### Ankündigung und Rückversicherung im Umgang mit Fax-Sendungen (NET.4.3.A15 - C)

Wichtige Fax-Sendungen mit vertraulichen Inhalten oder termingebundene Faxsendungen sollten vor Absendung beim Empfänger per Telefon oder E-Mail angemeldet werden. Hierdurch soll sichergestellt werden, dass der Empfänger die Möglichkeit erhält, zum entsprechenden Faxgerät zu gehen und dort das für ihn eingehende Fax direkt entgegenzunehmen, so dass kein anderer das Fax entnehmen kann. Ebenso wird empfohlen beim Empfänger nachzufragen, ob die Fax-Sendung vollständig empfangen, ausgedruckt und ihm übergeben wurde.

Die Mitarbeitenden sind vom Vorgesetzten über die einzuhaltenden Prozesse bei Versendung von vertraulichen oder wichtigen Faxen zu informieren.

### Umgang mit Faxgeräten, die gleichzeitig einen Netzwerkanschluss haben (NET.4.3.b.d.A1 - CIA)

Faxgeräte die neben einem Telefonanschluss auch über einen LAN-Anschluss verfügen (z.B. Multifunktionsgeräte) sind aus Sicherheitsgründen in einem speziell dafür eingerichteten LAN zu betreiben.

Bei IT-Systemen, die über einen LAN-Anschluss und eine Fax-Schnittstelle verfügen, ist die Fax-Schnittstelle zu deaktivieren oder besser zu entfernen sofern diese nicht benötigt wird.