

Eigenerklärung zur Leistungsfähigkeit hinsichtlich Hard-/Software

- | | | | |
|---|---|-----------------------------|-------------------------------|
| 1 | Anbieter kann je Gerätetyp der Leistungsklasse 1 bis 3 Geräte entsprechend den Forderungen des Leistungsverzeichnisses bereitstellen? | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 2 | Anbieter kann beim Auftraggeber Scan-Server Convert2PDF entsprechend den Forderungen des Leistungsverzeichnisses anbinden? | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 3 | Anbieter kann Softwarelösung für FollowMe-Server entsprechend den Forderungen des Leistungsverzeichnisses bereitstellen? | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 4 | Anbieter kann eine Lösung anbieten, welche physisch voneinander getrennte Netzwerke unterstützt?

In den getrennten Netzwerken müssen die Geräte für sich administriert werden und unabhängige Scan-Server und FollowMe-Server eingerichtet werden. | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 5 | Authentifizierung über MiFare | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 6 | Einhaltung der EU-Datenschutzgrundverordnung | <input type="checkbox"/> ja | <input type="checkbox"/> nein |
| 7 | Einhaltung der, die zu liefernden Systeme betreffenden Inhalte der IT-Sicherheitsrichtlinie Druck- und Scaninfrastruktur der Stadtverwaltung Chemnitz (siehe Anlage) | <input type="checkbox"/> ja | <input type="checkbox"/> nein |

Ort, Datum

Unterschrift (bevorzugt digital)



CHEMNITZ
KULTURHAUPTSTADT
EUROPAS 2025

IT- Sicherheitsrichtlinie

Druck und Scaninfrastruktur

Stand: Aug. 2024

Status: freigegeben

Version: 2.1

Amtsleiter 10

Amtsleiter 18

Herausgeber: Stadt Chemnitz, Amt für Organisation und Informationsverarbeitung

Autor: Lars Seit, Danny Sobeck

Sicherheitsrichtlinie Druck- und Scaninfrastruktur

Historie:

Version	Stand	Änderung
1.0	Nov.2011	Revision infolge neuen Druckkonzepts
1.1	Dez. 2016	Revision infolge modernisierten IT Grundschutzes
2.0.	Okt. 2018	Revision, Aufnahme der Arbeitsanweisung Amt 10 „Datenschutz und Informationssicherheit bei Abgabe bzw. Verschrottung von Kopierern oder Druckern“, Verantwortlichkeiten deutlicher

Inhaltsverzeichnis

Inhaltsverzeichnis.....	3
1 Einleitung.....	4
1.1 Zweck.....	4
1.2 Ziel	4
1.3 Geltungsbereich	4
1.4 Referenzdokumente	4
2 Regelungen	5
2.1 Verantwortlichkeiten	5
2.2 Konzeption	5
2.3 Managed Print Services	6
2.4 Sicherer Betrieb	6
2.5 Geregelte Außerbetriebnahme	8

1 Einleitung

1.1 Zweck

Diese Regelung dient dazu, die sichere Konfiguration und den sicheren Betrieb der Druckinfrastruktur der Stadt Chemnitz, zu gewährleisten.

Wie jedes IT-System sind auch Drucker, digitale Kopierer, netzfähige Scanner und Multifunktionsgeräte vielfältigen Gefahren ausgesetzt. Ohne entsprechende Schutzmaßnahmen wäre es leicht möglich, sich unberechtigt Zugriff auf sensible Informationen zu beschaffen.

Die Umsetzung der Regelungen dieser Richtlinie soll ein angemessenes Sicherheitsniveau der Druckinfrastruktur gewährleisten.

1.2 Ziel

Mit dieser Sicherheitsrichtlinie sind die zentralen Vorgaben der Leitung der Stadt Chemnitz, welche in der IT-Sicherheitsleitlinie verankert sind, für das Drucksystem umzusetzen. Darin wird ein normales Sicherheitsniveau gefordert mit Ausnahme der Anforderung an die Vertraulichkeit sensibler, personenbezogener Daten, welche als hoch eingestuft wurde.

Neben den allgemeinen Gefährdungen, die für die meisten IT-Systeme gelten, gibt es drucksystemtypische Gefährdungen wie Vertraulichkeitsverlust der gedruckten Daten oder Auswertung von Restinformationen in Multifunktionsgeräten. Diesen ist mit geeigneten Maßnahmen zu begegnen.

1.3 Geltungsbereich

Die Sicherheitsrichtlinie Druckinfrastruktur gilt für alle im Kernnetz der Stadt Chemnitz eingerichteten Drucker und Multifunktionsgeräte. Sie richtet sich an die Administratoren und Techniker des Amts für Informationsverarbeitung, die zuständigen Sachbearbeiter vom Hauptamt sowie an die Partnerfirma des Managed Print Service (MPS).

Die Maßnahmen decken die Lebenszyklen Planung, Beschaffung, Konfiguration, Betrieb und Aussonderung ab.

1.4 Referenzdokumente

- Einrichtung von lokalen Druckern in Kindertageseinrichtungen
- Sicherheitsrichtlinie für Server
- Qualifizierungsmatrix
- Dienstanweisung DA 1051
- Glossar IT-Sicherheitsrichtlinien (*kursiv* dargestellte Begriffe sind enthalten)

2 Regelungen

2.1 Verantwortlichkeiten

Die Stadt Chemnitz betreibt ein Managed-Print-Service Konzept (MPS). Dabei ist die beauftragte Partnerfirma für die Einhaltung der Regelungen dieser Richtlinie an den Druckern und Multifunktionsgeräten, die konforme Konfiguration der Serverkomponenten und Protokolle ebenso verantwortlich wie für die ordnungsgemäße Außerbetriebnahme.

Technische Vorgaben für den Betrieb trifft dabei das Amt für Informationsverarbeitung, organisatorische Vorgaben das Hauptamt ebenso wie Vorgaben zur Außerbetriebnahme und Verschrottung.

Sollten Arbeiten von Technikern der Stadt Chemnitz erfolgen, sind diese verantwortlich. Dabei ist die Installation und Administration der Serverkomponenten der Druckinfrastruktur ausschließlich durch einen Server-Administrator mit ausreichender Qualifikation vorzunehmen.

Anhand der Qualifizierungsmatrix sind vom IT-Abteilungsleiter fehlende Qualifikationen zu ermitteln und ggf. Schulungen zu veranlassen.

Der IT-Sicherheitsbeauftragte prüft die Umsetzung der Vorgaben aus dieser Richtlinie im Rahmen von Audits.

Änderungen an der Richtlinie sind vom IT-Sicherheitsbeauftragten in Zusammenarbeit mit den Server-Administratoren vorzunehmen. Sollten Teile in Zuständigkeit des Amtes 10 geändert werden ist dieses zu beteiligen.

2.2 Konzeption

Bei der Planung der Druckinfrastruktur müssen mindestens folgende Aspekte berücksichtigt werden:

- Kauf oder Miete der Endgeräte; Servicekonzept
- Analyse Druckvolumen
- Geräteklassen
- Standorte der Drucker und Multifunktionsprinter (MFP)
- Berechtigungskonzept (Drucker und Verwaltung, Abrechnung)
- Architektur der Druckserverinfrastruktur, Verfügbarkeit
- Nutzungsrichtlinien (Direktdruck, FollowMe Prinzip, Einschränkungen)
- Havariekonzept, Ausfall-Server oder kritischer Drucker
- Benutzerrichtlinien für sicheres Drucken
- Verschlüsselung der in den Geräten eingebauten Speichermedien
- Unterstützung sicherer Protokolle zur Datenübertragung und Administration
- Beschaffungsanforderungen müssen die Kriterien der IT- Sicherheit enthalten

2.3 Managed Print Services

Die Partnerfirma zu MPS muss sorgfältig ausgewählt werden.

Eignungskriterien dafür sind u. a.

- wirtschaftliche Situation und Größe des Unternehmens
- vergleichbare Referenzprojekte
- Einsatz von Mitarbeitern mit ausreichender Qualifikation
- kompetente, deutschsprachige Hotline / UHD
- die zum Einsatz kommenden Geräte und die Software müssen in vollem Umfang die IT-Sicherheitskriterien unter 2.4. und 2.5 sowie die spezifischen funktionellen Anforderungen erfüllen

Die MPS Partnerfirma muss ein detailliertes Informationssicherheits- und Datenschutzkonzept vorlegen.

Unter Zuarbeit der Stadt Chemnitz erstellt die MPS Partnerfirma einen Notfallplan für die zentralen Infrastrukturkomponenten sowie ein Informationssicherheits- und Datenschutzkonzept.

Vor der Auswahl sind die zum Einsatz kommenden Geräte und Softwarekomponenten in einer Teststellung ausführlich zu testen.

Folgende Aspekte müssen geregelt und dokumentiert werden:

- Kommunikationswege, Ansprechpartner
- Festlegung von Arbeitsabläufen und Zuständigkeiten
- Zugriff des Dienstleisters auf IT-Ressourcen, Definition von Schnittstellen
- Definition von Servicelevels, Reaktionszeiten, Eskalationsstufen

Die Dienstleistungsqualität und der Projektstand sind halbjährlich zu prüfen.

2.4 Sicherer Betrieb

MFP Geräte werden nach Möglichkeit in Kopierräumen oder Büroräumen aufgestellt. Sie dürfen nur in Ausnahmefällen in öffentlichen Bereichen aufgestellt werden und dürfen dann nur über „*FollowMe*“ betrieben werden.

Die Authentisierung am MFP erfolgt vorzugsweise mit einer Chipkarte (MiFare Classic) alternativ kann es über Nutzernamen/Passwort erfolgen.

Wenn eine Datenspeicherung auf der Festplatte des MFP erfolgt, muss diese verschlüsselt erfolgen.

Um Angriffe auf Drucker, Kopierer und Multifunktionsgeräte zu erschweren, muss der Zugriff auf diese Geräte beschränkt werden. Den Nutzern dürfen nur die für den Betrieb erforderlichen Funktionen zur Verfügung stehen.

Alle Administrationszugriffe dürfen nur über einen verschlüsselten Kanal (https) nach Authentifizierung stattfinden. Fernzugriffe wie Webinterface (https), FTP (File Transport Programme) oder Telnet müssen für Administratoren einzuschränken und zu deaktivieren sein.

Beim Einsatz von SNMP zum Management der Geräte ist SNMPv3 zu verwenden.

Bei Verwendung des Drucksystems Common Unix Printing System (CUPS) muss es in einer aktuellen Version unter Nutzung des Protokolls IPP erfolgen.

Zuständigkeiten für den Austausch von Verbrauchsmaterialien müssen geregelt und den Nutzern bekannt sein.

Neben den zur zentralen Abrechnung erforderlichen Werten sind Änderungen der Konfigurationseinstellungen und fehlgeschlagene Anmeldevorgänge zu protokollieren. Der Zugriff auf Protokolle muss für berechtigte Personen einzuschränken sein.

Es muss sichergestellt werden, dass die Geräte stets die korrekte Systemzeit haben.

Die Systemressourcen und Messwerte zur Betriebssicherheit sind immer auf kritische Werte hin zu überwachen.

Druck- und Scanaufträge müssen nach der Bearbeitung automatisch entfernt werden (es sei denn Nutzer wählt explizit, dass sie gespeichert werden sollen)

Nicht verarbeitete Druckaufträge müssen automatisch, nach definierten Zeiten, zu löschen sein.

Beim Netzwerkscan muss ausgeschlossen werden, dass Scandateien in einem anderen als dem dafür vorgesehenen Verzeichnis gespeichert werden.

Es dürfen dabei nur aktuelle und sichere Protokolle zum Einsatz kommen. (kein SMB1)

Der Aufbau der Druckinfrastruktur muss dokumentiert werden.

Wenn die Fax-Funktionalität des Multifunktionsgerätes genutzt werden soll, muss sichergestellt sein, dass der hierfür erforderliche Anschluss an das Telefonnetz nicht zu unkontrollierten Datenverbindungen zwischen dem LAN und Fremdnetzen führen kann.

Wenn die Fax-Funktion nicht genutzt wird, ist sie zu deaktivieren.

Sicherheitspatches der Managementsoftware und Firmware der Geräte müssen zeitnah installiert werden. Die Aktualisierung der Firmware der Drucker und Multifunktionsgeräte muss möglichst zentral erfolgen. Eine zentrale Kontrolle des Firmwarestandes aller Geräte sollte möglich sein. Patches und Updates müssen aus vertrauenswürdigen Quellen bezogen werden.

Alle Drucker und MFP Geräte müssen zur Netzwerkauthentifizierung den Standard IEEE 802.1X EAP TLS mit Zertifikat unterstützen.

MFP Geräte müssen perspektivisch in einem eigenen Netzsegment, getrennt von Clients und Servern, betrieben werden.

Die zum Einsatz kommende Verwaltungs- und Abrechnungssoftware muss mandantenfähig sein, um unterschiedliche Berechtigungen und Sichten der verschiedenen mit dem System arbeitenden Sachgebiete abbilden zu können.

Zentrale Komponenten der Druckinfrastruktur bei deren Ausfall eine große Anzahl Drucker nicht mehr funktionieren würde sind redundant auszulegen.

Benutzer müssen für den sicheren Gebrauch der Multifunktionsgeräte eingewiesen werden. Es sind daher von der MPS Partnerfirma die Geräteverantwortlichen zu schulen, welche als Multiplikatoren dienen.

Weiterhin ist bei jedem Multifunktionsgerät ein Merkblatt zur Bedienung der wichtigsten Funktionen zu hinterlegen und aktuell zu halten.

2.5 Geregelte Außerbetriebnahme

Bei Rückholung der vertragsgegenständlichen Systeme muss die MPS Partnerfirma grundsätzlich eine Datenlöschung/-bereinigung durchführen. Es wird dabei zwischen einer Standardlöschung und einem Sonderlöschverfahren, welches durch die SVC zu beauftragen ist unterschieden.

Löschverfahren

Die Standardlöschung wird bei jedem zurückgenommenen System durchgeführt. Es werden alle Kundendaten, die sich auf dem System befinden, sicher gelöscht. Eine eventuell vorhandene Festplatte wird mit der systemeigenen Funktion formatiert.

Darüber hinaus werden folgende Maßnahmen durchgeführt:

- Löschen des Adressbuchs, der E-Mail-Einstellungen, Netzwerk-Einstellungen, Fax-Einstellungen, des Dokumentenservers und der Remote-Einstellungen
- Löschen der Kundendaten auf dem NV RAM
- Gegebenenfalls Löschen von SD-Karten und weiteren angebundenen Geräten
- Entfernen von Bildrückständen auf der Trommel
- Entfernen von auf dem Vorlagenglas zurückgelassenen Dokumenten
- Entfernen möglicher Papierstaus
- Entfernen von Papier aus den Papierkassetten
- Entfernen von auf dem System angebrachten Aufklebern

Der komplette Prozess muss lückenlos durch die MPS Partnerfirma dokumentiert werden.

Zusätzlich gilt:

1. Die Löschung von Geräten darf nur von der MPS Partnerfirma oder von zertifizierten Vertrags-/Vermarktungspartnern der MPS Partnerfirma durchgeführt werden. Dies hat die MPS Partnerfirma im Rahmen der Dokumentation von Punkt 3 zu bestätigen.
2. Die MPS Partnerfirma hat die Löschung der Daten der Stadt Chemnitz in Datenbanken im Zusammenhang mit den Geräterückgaben schriftlich zu bestätigen.

3. Die Dokumentation zur Löschung der Daten nach diesen Richtlinien muss seitens der MPS Partnerfirma bei der Stadtverwaltung Chemnitz vorliegen. Dies kann seitens der MPS Partnerfirma durch Sammelbeleg über die gelöschten Geräte erfolgen.

4. Bei sensiblen Geräten (z.B. Personalabteilung) sind Stichproben über die Löschung durchzuführen. Hierzu wird seitens des Hauptamtes stichprobenartig das gerätespezifische Löschprotokoll abgefordert.

Anlage 1 zur IT- Sicherheitsrichtlinie „Druck und Scaninfrastruktur“

Einrichtung von lokalen Multifunktionsgeräten in Kindertageseinrichtungen

Version 1.0
Juli 2025
Autor: Lars Seit

1. Einleitung

In dieser Anlage zur IT- Sicherheitsrichtlinie „Druck- und Scaninfrastruktur“ werden technische und organisatorische Vorgaben definiert um den Mindestanforderungen an IT-Sicherheit und Datenschutz bei lokalen Multifunktionsgeräten in Kindertageseinrichtungen der Stadt Chemnitz zu genügen.

Das ist erforderlich, da die technische Ausrüstung an den Kitas es nicht ermöglicht, die Multifunktionsgeräte nach den Standardvorgaben zu betreiben, gleichzeitig ist der Einsatz solcher für die Aufgabenerfüllung notwendig.

2. Anforderungen

Aufgrund der Verarbeitung sensibler personenbezogener Daten an Geräten, die nicht in jedem Fall durch den Zugriff unberechtigter Personen räumlich geschützt werden können, ist es erforderlich, durch geeignete technische und organisatorische Maßnahmen, deren sicheren Betrieb zu gewährleisten.

Die Anforderungen an die Verfügbarkeit, Belastbarkeit und Integrität sind untergeordnet.

3. Regelungen

Technische Vorgaben:

In den Kitas können Geräte der Leistungsklasse 2 lokal (ohne Netzanschluss) betrieben werden.

Dabei werden folgende Funktionen zur Verfügung gestellt:

- Kopieren
- Drucken über die USB Schnittstelle (von USB Stick)
- Scannen auf die USB Schnittstelle (auf USB Stick)

Alle anderen Funktionen der Geräte müssen deaktiviert sein.

Der LAN-Anschluss ist zu deaktivieren.

Die Standardkonfiguration ist zu dokumentieren.

Die Konfiguration ist mit einem komplexen Gerätepasswort zu schützen. Dieses darf nur dem Kreis der zugelassenen Techniker bekannt sein.

Wenn erforderlich, z.B. bei Verdacht des Bekanntwerdens oder beim Ausscheiden von Technikern muss das Passwort geändert werden.

Erforderliche Sicherheitspatches sind zu installieren.

Die Geräte dürfen nicht ohne komplettes Neuaufsetzen und Neukonfiguration im zentralen Verwaltungsnetz der SVC eingesetzt werden.

Wenn möglich sind die Multifunktionsgeräte in abschließbaren Räumen aufzustellen. Sollte das nicht möglich sein muss die unbefugte Nutzung mittels PIN verhindert werden.

Daten auf vorhandene Festplatten/ SSDs in den Multifunktionsgeräten sind, wenn möglich, stets verschlüsselt abzulegen.

Dokumente dürfen nicht dauerhaft auf den Multifunktionsgeräten gespeichert werden können.

Es ist zu verhindern, dass über die USB Schnittstelle Daten des Gerätes ausgelesen werden können.

Bei Außerbetriebnahme ist die Festplatte/ SSD sicher, unwiederbringlich zu löschen.

Organisatorische Maßnahmen:

Die Einhaltung der Vorgaben ist stichprobenartig zu prüfen.

Es sind die betreffenden Maßnahmen der Dienstanweisung 1051 zu beachten und die Nutzer der Multifunktionsgeräte sind zu sensibilisieren.

Insbesondere

- sind keine Ausdrücke an den Multifunktionsgeräten liegen zu lassen,
- dürfen keine Ausdrücke sensibler Daten in öffentlich zugänglichen Papierkörben entsorgt werden,
- sind die Regelungen zu mobilen Datenträgern (USB Sticks) zu beachten.