Vorlage

Technische Richtlinie für den Betrieb von Informationssystemen [Gemeinde/Stadt]

Erläuterung zur Vorlage

Die Vorlage Technische Richtlinie für den Betrieb von Informationssystemen ist Teil einer Vorlagenreihe, die sämtliche relevanten Informationssicherheitsdokumente umfasst. Die empfohlene Vorgehensweise, die Hilfestellungen und die Erläuterungen zu den Vorlagen sind dem Leitfaden Informati­onssicherheit in Gemeinden – Bevölkerungszahl < 6000 beziehungsweise > 6000 zu entnehmen.

Die Vorlage ist den jeweiligen Gegebenheiten anzupassen. Die anzupassenden Punkte befinden sich in ecki­gen Klammern [ ].

Der Leitfaden Informationssicherheit in Gemeinden – Bevölkerungszahl < 6000 beziehungsweise > 6000, die Vorlagen und weitere Dokumente sind auf [www.datenschutz.ch](https://datenschutz.ch/datenschutz-in-oeffentlichen-organen/informationssicherheit) publiziert.

Änderungskontrolle

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Beschreibung, Bemerkung | Name |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Inhalt

[1 Allgemeine Bestimmungen 4](#_Toc151709740)

[1.1 Gegenstand und Zweck 4](#_Toc151709741)

[1.2 Geltungsbereich 4](#_Toc151709742)

[1.3 Grundlagen 4](#_Toc151709743)

[2 Betriebsleistungsgrad 5](#_Toc151709744)

[3 Dokumentation 5](#_Toc151709745)

[4 Passwörter 6](#_Toc151709746)

[5 Sicherheit von Informationsübertragungen 7](#_Toc151709747)

[6 Sicherheit von Informationssystemen 7](#_Toc151709748)

[6.1 Inbetriebnahme (bei Betrieb vor Ort) [Löschen, wenn der Betrieb ausgelagert wurde] 8](#_Toc151709749)

[6.2 Inbetriebnahme (bei ausgelagertem Betrieb) [Löschen, wenn der Betrieb vor Ort erfolgt] 8](#_Toc151709750)

[6.3 Betrieb 9](#_Toc151709751)

[6.4 Ausserbetriebnahme (bei Betrieb vor Ort) [Löschen, wenn der Betrieb ausgelagert wurde] 9](#_Toc151709752)

[6.5 Ausserbetriebnahme (bei ausgelagertem Betrieb) [Löschen, wenn der Betrieb vor Ort erfolgt] 10](#_Toc151709753)

[7 Verwaltung der Netzwerksicherheit 10](#_Toc151709754)

[7.1 Anforderungen / Dokumentation 10](#_Toc151709755)

[7.2 Netztrennung 10](#_Toc151709756)

[7.3 Sicherheitsanforderungen Netzwerk der [Gemeinde/Stadt] 11](#_Toc151709757)

[7.4 Routers und Switches 12](#_Toc151709758)

[7.5 WLAN 12](#_Toc151709759)

[7.6 Firewall 13](#_Toc151709760)

[7.7 VPN 14](#_Toc151709761)

[8 Mobiles Arbeiten und mobile Geräte 14](#_Toc151709762)

[9 Telefonie (VoIP) 15](#_Toc151709763)

[10 Drucker / Kopierer / Multifunktionsgeräte 16](#_Toc151709764)

[11 Verwaltung von Bedrohungen und Schwachstellen 17](#_Toc151709765)

[12 Verschlüsselungsmassnahmen 17](#_Toc151709766)

[12.1 Kryptografische Verfahren 17](#_Toc151709767)

[12.2 Digitale Zertifikate 18](#_Toc151709768)

[13 Datensicherung und -wiederherstellung 18](#_Toc151709769)

[14 Sicherheit von Testdaten 19](#_Toc151709770)

[15 Protokollierung und Kontrolle 19](#_Toc151709771)

[15.1 Allgemeine Anforderungen 19](#_Toc151709772)

[15.2 Sicherheitsprotokollierung 19](#_Toc151709773)

[15.3 Applikationsprotokollierung 20](#_Toc151709774)

[16 Physische Sicherheit 20](#_Toc151709775)

[16.1 Zutritt 20](#_Toc151709776)

[16.2 Sicherheitsmassnahmen 20](#_Toc151709777)

[17 Fernwartung 21](#_Toc151709778)

[18 Umgang mit Informationssicherheitsvorfällen 22](#_Toc151709779)

[19 Genehmigung und Inkrafttreten 22](#_Toc151709780)

# Allgemeine Bestimmungen

## Gegenstand und Zweck

Diese Richtlinie regelt die Anforderungen, die bei Installation, Konfiguration und Betrieb der IKT-Umgebung eingehalten werden müssen.

Sie bezweckt den Schutz der Informationen vor einem Verlust der Vertraulichkeit, Verfügbarkeit und Integrität.

[Auswahl aus den zwei folgenden Absätzen: Ersten Absatz verwenden, wenn der Betrieb der IKT-Umgebung durch die Gemeinde/Stadt selbst erfolgt. Zweiten Absatz verwenden, wenn der Betrieb der IKT-Umgebung ausgelagert wurde]

[Erster Absatz, bei eigenem Betrieb:] Ausnahmen zu den in dieser Richtlinie definierten Vorgaben sind durch die Informationssicherheitsverantwortlichen/den Informationssicherheitsverantwortlichen (ISV) mit einer Begründung durch [die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber] bewilligen zu lassen.

[Zweiter Absatz, bei Auslagerung:] Ausnahmen zu den in dieser Richtlinie definierten Vorgaben sind durch [IKT-Betreiber] mit einer Begründung durch die/den ISV bewilligen zu lassen.

Die Richtlinie lehnt sich an die Vorgaben der Allgemeinen und Besonderen Informationssicherheitsrichtlinien des Kantons Zürich an.

## Geltungsbereich

Die Richtlinie gilt für den/die internen oder externen Betreiber der IKT-Umgebung der [Gemeinde/Stadt].

## Grundlagen

Die Grundlagen für die [Gemeinde/Stadt] sind:

* Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4))
* Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.41))
* Verordnung über die Informationsverwaltung und -sicherheit (IVSV, [LS 170.8](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.8))
* Allgemeine Richtlinie für Informationssicherheit und Datenschutz [Gemeinde/Stadt]
* Weisung zur Informationssicherheit und zum Datenschutz [Gemeinde/Stadt]
* Rollen- und Berechtigungskonzept [Gemeinde/Stadt]
* Notfallkonzept [Gemeinde/Stadt]
* Bedrohungsanalyse [Gemeinde/Stadt]
* [Schutzbedarfsanalyse](http://www.datenschutz.ch) [Gemeinde/Stadt]
* [IT-Grundschutzkompendium](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/IT_Grundschutz_Kompendium_Edition2022.pdf?__blob=publicationFile&v=5) des Bundesamts für Sicherheit in der Informationstechnik (BSI, Deutschland)

Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen zu beachten.

# Betriebsleistungsgrad

Bei der Auswahl und Konfiguration der IKT-Umgebung der [Gemeinde/Stadt] sind die Anforderungen an die Verfügbarkeit, Ausfallsicherheit und Wiederherstellung zu berücksichtigen. Die Anforderungen ergeben sich aus der für das Notfallkonzept der [Gemeinde/Stadt] durchgeführten Bedrohungsanalyse und sind entsprechend an den externen IKT-Dienstleister oder die interne IKT-Organisation zu überbinden.

Zu berücksichtigen und definieren sind insbesondere:

* Mengengerüste und entsprechend Kapazität und Anzahl Transaktionen
* Betriebszeiten, ohne Wartungsfenster (z.B. 7–18 Uhr)
* Angestrebte Verfügbarkeit (z.B. 99,5% über das Jahr)
* Monitoring der Systeme (permanent oder in gewissen Zeitintervallen)
* Maximale Ausfalldauer pro Vorfall (Recovery Time Objective, RTO) (z.B. 8 h)
* Maximale Ausfalldauer pro Jahr (errechnet sich aus der Verfügbarkeit pro Jahr)
* Maximaler Datenverlust bei einem Ausfall (Recovery Point Objective, RPO) (z.B. 1 Tag)

Entsprechend den Anforderungen sind Infrastrukturen oder einzelne Komponenten allenfalls redundant auszulegen und die Massnahmen zur Wiederherstellung nach einem Ausfall zu definieren.

Zusätzlich sind die folgenden Punkte insbesondere bei einer Auslagerung des IKT-Betriebs an einen externen Dienstleister vertraglich zu regeln und zu kontrollieren.

* Supportzeiten (z.B. 8–17 Uhr)
* Reaktionszeit (Zeit, bis Dienstleister auf Anfrage reagiert, z.B. 2 h)
* Interventionszeit (Zeit, bis Dienstleister Arbeit an Störung aufnimmt, z.B. 6 h)
* Behebungszeit (Zeit, bis Problem behoben ist, z.B. 72 h)
* Kontrollmittel zur Überwachung der Leistungen
* Eskalationspfad und -massnahmen
* Kosten der Dienstleistungen (in Vertrag inbegriffen/nicht inbegriffen)

# Dokumentation

Die Betriebsumgebung der [Gemeinde/Stadt] ist zu dokumentieren. Alle im Besitz und/oder in den Räumlichkeiten der [Gemeinde/Stadt] befindlichen technischen Komponenten sowie Applikationen und Betriebssysteme sind in der Schutzbedarfsanalyse der [Gemeinde/Stadt] zu erfassen und stets aktuell nachzuführen. Allenfalls ist dies durch den IKT-Provider zu erbringen.

Zudem sind folgende Dokumentationen zuhanden der [Gemeinde/Stadt] zu erstellen:

* Netzwerkplan/Diagramm, das alle Komponenten sowie Schnittstellen enthält
* Betriebskonzept oder -dokumentation, das folgende Angaben enthält:
	+ Architektur
	+ Standorte
	+ Mengengerüste
	+ Autorisierungen inkl. Administratoren
	+ Passwörter (in separatem, geschütztem Dokument)
	+ Logging
	+ Backup- und Restore-Massnahmen
	+ Konfiguration (Server, Clients, Netzwerkkomponenten)
	+ Schutzmassnahmen wie Firewalls, Virenschutz, Hardening etc.
	+ Notfallregelung
	+ Incident Management und Change Management
	+ Betreiber, Verantwortliche und Prozesse

# Passwörter

Für Passwörter und alphanumerische PIN-Codes gelten mindestens folgende Anforderungen:

* Authentifizierungsinformationen müssen einer eindeutigen Entität zugeordnet werden können (z.B. Benutzer, Identität, IKT-System oder Service).
* Initialpasswörter müssen einzigartig sein und sind zwingend während der ersten Anmeldung durch die Benutzerin/den Benutzer zu ändern.
* Numerische PIN-Codes müssen mindestens sechs Zeichen lang sein, wo dies die entsprechenden Geräte zulassen.
* Biometrische Merkmale gelten sinngemäss als Authentifizierungsmerkmal (z.B. Fingerprint).
* Nach fünf gescheiterten Anmeldeversuchen muss das Konto permanent gesperrt werden. Der Prozess zum Zurücksetzen des Kontos ist zu definieren.
* Passwörter dürfen nur zurückgesetzt werden, wenn sich Benutzerinnen oder Benutzer eindeutig identifizieren können.
* Wird ein Passwort geändert, darf dieses nicht mit den letzten fünf Passwörtern identisch sein.
* Passwörter und PIN-Codes dürfen bei der Authentifizierung nicht im Klartext auf dem Bildschirm angezeigt werden.
* Passwörter und PIN-Codes sind gemäss den Anforderungen für Verschlüsselungsmassnahmen zu schützen.
* Es dürfen nicht dieselben Passwörter und PIN-Codes für private und dienstliche Zwecke verwendet werden.

Für Konten von Benutzerinnen und Benutzern gelten folgende zusätzlichen Anforderungen:

* Passwörter und alphanumerische PIN-Codes müssen entweder
1. mindestens 25 Zeichen lang sein und
2. die Verwendung von unzulässigen Passwortmerkmalen muss technisch verifiziert werden (siehe Auflistung unten)
* oder mindestens 12 Zeichen lang sein und eine Mischung aus mindestens drei der folgenden Kategorien enthalten:
1. Grossbuchstaben
2. Kleinbuchstaben
3. Zahlen
4. Sonderzeichen

Für administrative Konten gelten folgende zusätzlichen Anforderungen:

* Passwörter und alphanumerische PIN-Codes müssen entweder
1. mindestens 30 Zeichen lang sein und
2. die Verwendung von unzulässigen Passwortmerkmalen muss technisch verifiziert werden (siehe Auflistung unten)
* oder mindestens 16 Zeichen lang sein und eine Mischung aus mindestens drei der folgenden Kategorien enthalten:
1. Grossbuchstaben
2. Kleinbuchstaben
3. Zahlen
4. Sonderzeichen
* Gruppenpasswörter werden nur vergeben, wenn dies zwingend erforderlich ist. Sie sind sofort zu ändern, wenn sich die Zusammensetzung der Gruppe verändert oder wenn sie unautorisierten Personen bekannt geworden sind.

Für technische Konten gelten folgende zusätzlichen Anforderungen:

* Passwörter müssen eine Mischung aus allen der folgenden Kategorien enthalten:
1. Grossbuchstaben
2. Kleinbuchstaben
3. Zahlen
4. Sonderzeichen
* Interaktive Anmeldungen mit technischen Konten sind verboten. Technische Konten dürfen nicht von Benutzerinnen oder Benutzern für Arbeiten auf Informationssystemen verwendet werden.

Die Verwendung von folgenden Passwortmerkmalen ist unzulässig:

1. kompromittierte Passwörter (z.B. Datenlecks)
2. leicht verfügbare Begriffe (z.B. Wörterbücher)
3. simple Muster (z.B. abcdefgh, 123456)
4. kontextspezifische Informationen (z.B. Gemeindename)
5. personenbezogene Informationen (z.B. Geburtsdatum)
6. benutzer- oder servicebezogene Informationen (z.B. Anmeldedaten)

Um die Sicherheit weiter zu erhöhen, können Intervalle zum Wechsel der Passwörter eingerichtet werden, z.B. alle 90 oder 180 Tage.

Passwörter für administrative und technische Konten sind in geeigneter Form zu hinterlegen, so dass im Notfall auf sie zugegriffen werden kann, beispielsweise in einem gesicherten Passwortmanager oder einem verschlossenen Umschlag in einem Tresor.

# Sicherheit von Informationsübertragungen

Informationen zu Verwaltungstätigkeiten sind bei der elektronischen Übertragung und dem physischen Transport in Abhängigkeit ihrer Schutzstufe vor unbefugter Kenntnisnahme und Bearbeitung zu schützen.

Beim Austausch von Informationen mit externen Organisationen und Personen werden in Abhängigkeit von der Klassifizierung der auszutauschenden Informationen die folgenden Anforderungen geprüft und wenn nötig vertraglich geregelt:

1. Verfahren zur Sicherstellung der Nachvollziehbarkeit
2. Einsatz von Verschlüsselungsverfahren bei elektronischem Austausch gemäss Kapitel 12 Verschlüsselungsmassnahmen
3. Aufrechterhaltung einer Informationskette während der elektronischen Übertragung (z.B. Sendungsverfolgung, Empfangsbestätigung)
4. Definierte Verfahren, die Informationen und Datenträger während des physischen Transports schützen

# Sicherheit von Informationssystemen

Um die Sicherheit von Informationssystemen zu gewährleisten, sind folgende Grundsätze bei Inbetriebnahme, Betrieb und Ausserbetriebnahme einzuhalten. Die Anforderungen gelten bei einem Vor-Ort-Betrieb bei der [Gemeinde/Stadt] wie auch bei einem ausgelagerten Betrieb. Bei einem ausgelagerten Betrieb sind die Massnahmen durch den Betreiber zu erfüllen und nachzuweisen.

## Inbetriebnahme (bei Betrieb vor Ort) [Löschen, wenn der Betrieb ausgelagert wurde]

* Neue Informationssysteme müssen im IKT-Inventar und in der Schutzbedarfsanalyse der [Gemeinde/Stadt] nachgeführt werden.
* Auf Systemen der [Gemeinde/Stadt] dürfen nur zugelassene, inventarisierte Anwendungen installiert werden.
* Von eingesetzten Softwareprogrammen sollten Sicherungskopien angefertigt werden, sofern das rechtlich erlaubt und technisch möglich ist. Alle notwendigen Pakete und Informationen sollten vorhanden sein, um die Software im Notfall wieder installieren zu können. Die originalen Installationsquellen sowie die Lizenznummern müssen an einem geeigneten Ort sicher aufbewahrt werden.
* Neue Informationssysteme müssen vor der Inbetriebnahme auf die Kompatibilität mit bestehenden Systemen geprüft, getestet und abgenommen werden. Vor der produktiven Inbetriebnahme muss eine Dokumentation der Systeme vorliegen.
* Eine Installationsanweisung muss erstellt werden, die alle benötigten Anwendungsmodule (Bibliotheken), die Installationsreihenfolge und die Konfiguration der Anwendungsmodule beinhaltet.
* Für Testsysteme sind die gleichen Sicherheitsanforderungen umzusetzen wie für Produktivsysteme. Insbesondere gilt diese Anforderung, wenn auf Testsystemen mit Daten aus produktiven Systemen (Datenkopien) gearbeitet werden muss. Die Anzahl der verwendeten vertraulichen Daten ist auf ein Minimum zu beschränken. Die Daten sind nach Durchführung der Tests zu löschen. Über die Verwendung von Daten aus produktiven Systemen in Tests ist ein Protokoll zu führen.
* Informationssysteme sind mindestens mit folgenden Massnahmen zu härten
	+ Setzen eines BIOS-Passworts, um Änderungen durch Benutzende vorzubeugen
	+ Keine lokalen Administrationsrechte für Benutzende
	+ Einschränkung der Benutzerrechte auf die nötigen Funktionen (z.B. Deaktivierung der PowerShell)
	+ Deaktivierung aller Dienste, die nicht benötigt werden
	+ Deinstallation aller Software, die nicht dienstlich benötigt werden
	+ Sperren von USB-Ports und DVD-Laufwerken, wenn sie nicht zwingend benötigt werden
	+ Einrichten einer automatischen Bildschirmsperre nach max. zehn Minuten mit gesicherter Entsperrung
	+ Deaktivierung der Übermittlung von Telemetriedaten soweit möglich
* Virenschutzprogramme sind auf allen IKT-Systemen einzusetzen. Die Risiken der Internetnutzung sind mit geeigneten Massnahmen möglichst gering zu halten.
* Internetbrowser sollten zentral so vorkonfiguriert werden, dass die wichtigsten Sicherheitseinstellungen gewährleistet sind (keine Speicherung von Formulardaten, kein Auto-Vervollständigen, möglichst keine Cookies, Auswahl Plug-ins und Erweiterungen, privater Modus bzw. Chronik-Einstellungen, keine Übermittlung von Daten an den Hersteller). Der Benutzende sollte diese Einstellungen nicht ändern können.
* Die Protokollierung gemäss Kapitel 15 muss bei der Inbetriebnahme von Informationssystemen sichergestellt ist.
* Zumindest für mobile Geräte (Laptops) ist eine Festplattenverschlüsselung einzurichten.
* Für Server und Clients ist eine Referenzinstallation zu erstellen, mit der neue Systeme aufzusetzen sind.

## Inbetriebnahme (bei ausgelagertem Betrieb) [Löschen, wenn der Betrieb vor Ort erfolgt]

* Neue Informationssysteme, die sich im Besitz und/oder den Räumlichkeiten der [Gemeinde/Stadt] befinden, müssen im IKT-Inventar und der Schutzbedarfsanalyse der [Gemeinde/Stadt] nachgeführt werden.
* Durch den Betreiber ist sicherzustellen, dass auf Systemen der [Gemeinde/Stadt] nur durch die [Gemeinde/Stadt] autorisierte Anwendungen installiert werden.
* Von Softwareprogrammen, die durch die [Gemeinde/Stadt] erworben wurden, sollten Sicherungskopien angefertigt werden, sofern das rechtlich erlaubt und technisch möglich ist. Alle notwendigen Pakete und Informationen sollten vorhanden sein, um die Software im Notfall wieder installieren zu können. Die originalen Installationsquellen sowie die Lizenznummern müssen an einem geeigneten Ort sicher aufbewahrt werden.
* Neue Informationssysteme müssen durch den Betreiber vor der Inbetriebnahme auf die Kompatibilität mit bestehenden Systemen geprüft, getestet und abgenommen werden. Vor der produktiven Inbetriebnahme muss eine Dokumentation der Systeme vorliegen.
* Der Betreiber hat für Testsysteme die gleichen Sicherheitsanforderungen umzusetzen wie für die Produktivsysteme. Insbesondere gilt diese Anforderung, wenn auf Testsystemen mit Testdaten aus produktiven Systemen (Datenkopien) gearbeitet werden muss. Die Anzahl der verwendeten vertraulichen Daten ist auf ein Minimum zu beschränken. Die Daten sind nach Durchführung der Tests zu löschen. Über die Verwendung von Daten aus produktiven Systemen in Tests ist ein Protokoll zuhanden der [Gemeinde/Stadt] zu führen.
* Informationssysteme sind mindestens mit folgenden Massnahmen zu härten
	+ Setzen eines BIOS-Passworts, um Änderungen durch Benutzer vorzubeugen
	+ Keine lokalen Administrationsrechte für Benutzende
	+ Einschränkung der Benutzerrechte auf die nötigen Funktionen (z.B. Deaktivierung der PowerShell)
	+ Deaktivierung aller Dienste, die nicht benötigt werden
	+ Deinstallation aller Software, die nicht dienstlich benötigt werden
	+ Sperren von USB-Ports und DVD-Laufwerken, wenn sie nicht zwingend benötigt werden
	+ Einrichten einer automatischen Bildschirmsperre nach max. zehn Minuten mit gesicherter Entsperrung
	+ Deaktivierung der Übermittlung von Telemetriedaten soweit möglich
* Virenschutzprogramme sind auf allen IKT-Systemen einzusetzen. Die Risiken der Internetnutzung sind mit geeigneten Massnahmen möglichst gering zu halten.
* Internetbrowser sollten zentral so vorkonfiguriert werden, dass die wichtigsten Sicherheitseinstellungen gewährleistet sind (keine Speicherung von Formulardaten, kein Auto-Vervollständigen, möglichst keine Cookies, Auswahl Plug-ins und Erweiterungen, privater Modus bzw. Chronik-Einstellungen, keine Übermittlung von Daten an den Hersteller). Der Benutzende sollte diese Einstellungen nicht ändern können.
* Die Protokollierung gemäss Kapitel 15 ist vor der Inbetriebnahme von Informationssystemen sicherzustellen.
* Zumindest für mobile Geräte (Laptops) ist eine Festplattenverschlüsselung einzurichten.
* Für Server und Clients ist eine Referenzinstallation zu erstellen, mit der neue Systeme aufzusetzen sind.

## Betrieb

* Alle IKT-Systeme wie Server, Clients und Netzwerkkomponenten sind regelmässig mit den aktuellsten Updates und Patches zu versorgen.
* Schwachstellen für IKT-Systeme und Anwendungen sind laufend zu überprüfen und gemäss ihrer Kritikalität zu behandeln (z.B. mit Updates oder Austausch).
* Produkte, die nicht mehr vom Hersteller unterstützt werden, sind abzulösen.
* Die Verfügbarkeit und Qualität der Anwendungsdienste sind laufend zu überprüfen. Sicherheitsrelevante Ereignisse sind aufzuzeichnen und periodisch oder bei Verdacht auszuwerten.
* Jegliche Änderungen an IKT-Systemen und Anwendungen müssen über einen dokumentierten Change-Prozess erfolgen. Im Fall eines ausgelagerten Betriebs ist die Kundschaft vorgängig über Änderungen zu informieren.

## Ausserbetriebnahme (bei Betrieb vor Ort) [Löschen, wenn der Betrieb ausgelagert wurde]

Die Ausserbetriebnahme und fachgerechte Entsorgung von Informationssystemen erfolgen nach einem dokumentierten Prozess. Bei der Ausserbetriebnahme oder einer Reparatur von Informationssystemen, insbesondere wenn sie Speichermedien enthalten, müssen Informationen unwiederbringlich gelöscht werden, bevor die Informationssysteme ausgetauscht, entsorgt oder wiederverwendet werden (z.B. mobile Endgeräte, Drucker, Kameras).

Geräte, die ausser Betrieb genommen werden, sind aus dem IKT-Inventar und der Schutzbedarfsanalyse zu entfernen.

## Ausserbetriebnahme (bei ausgelagertem Betrieb) [Löschen, wenn der Betrieb vor Ort erfolgt]

Der Betreiber verfügt über einen dokumentierten Prozess für die Ausserbetriebnahme und die fachgerechte Entsorgung von Informationssystemen. Bei der Ausserbetriebnahme oder einer Reparatur von Informationssystemen, insbesondere bei IKT-Systemen, die Speichermedien enthalten (z.B. mobile Endgeräte, Drucker, Kameras), werden Informationen durch den Betreiber irreversibel gelöscht, bevor die Informationssysteme ausgetauscht, entsorgt oder wiederverwendet werden. Die [Gemeinde/Stadt] wird über das Vorgehen informiert, Protokolle sind bei Bedarf einsehbar.

Geräte, die ausser Betrieb genommen werden, sind aus dem IKT-Inventar und der Schutzbedarfsanalyse zu entfernen (nur Geräte in den Räumlichkeiten der [Gemeinde/Stadt]).

# Verwaltung der Netzwerksicherheit

## Anforderungen / Dokumentation

Für das Netzwerkdesign bei der [Gemeinde/Stadt] ist eine Dokumentation inkl. Netzplan zu erstellen, worin Anforderungen und Vorgaben beschrieben werden, wie Netze sicher konzipiert und aufgebaut werden. Es ist unter anderem festzulegen,

* in welchen Fällen die Sicherheitszonen zu segmentieren sind und in welchen Fällen Benutzergruppen bzw. Mandanten logisch oder sogar physisch zu trennen sind,
* welche Kommunikationsbeziehungen und welche Netz- und Anwendungsprotokolle jeweils zugelassen werden,
* wie der Datenverkehr für Administration und Überwachung netztechnisch zu trennen ist,
* welche verwaltungsinterne und standortübergreifende Kommunikation (WAN, Funknetze) erlaubt ist und welche Verschlüsselung im WAN, LAN oder auf Funkstrecken erforderlich ist.

## Netztrennung

Zur Beachtung: auf die Umsetzung der nachfolgenden Regelungen zur Netztrennung kann verzichtet werden, wenn die [Gemeinde/Stadt] ausschliesslich über einen Leunet-Anschluss verfügt und zudem keinen eigenen Server vor Ort betreibt.

Das Gesamtnetz muss in mindestens folgende drei Sicherheitszonen physisch separiert sein:

* interne Zone (trusted),
* demilitarisierte Zone (DMZ),
* externe Zone (inklusive Internetanbindung sowie Anbindung an andere nicht vertrauenswürdige Netze)

Interne Zone (trusted)

Systeme in diesen Zonen werden vollumfänglich durch die [Gemeinde/Stadt] oder einen beauftragten Partner betrieben. Der Zugang eines Endsystems in eine entsprechende Zone im Access-Bereich ist nur nach vorgängiger Authentifizierung der Hardware möglich. Es bestehen aus dieser Zone keine direkten Übergänge zu Fremdnetzen.

Beispiel: Gemeindezone intern/trusted

Demilitarisierte Zone (DMZ)

DMZ-Zonen verfügen grundsätzlich über erhöhte Sicherheitsanforderungen. Übergänge zu Fremdnetzen erfolgen immer über DMZ-Zonen, in denen Proxyservices bereitgestellt werden. DMZ-Zonen verfügen über einen Anschluss an den Perimeter Extern und an den Perimeter Intern. Die DMZ-Zonen werden nach System- und Sicherheitskriterien voneinander getrennt. Der Zugang von und zu DMZ-Zonen wird mit Firewalls Outside mit Stateful Inspection geschützt. Die DMZ Inside wird zusätzlich, wenn möglich mit UTM-Funktionalitäten (dynamische Paketfilterung), ausgestattet.

Die Firewall-Struktur muss für alle Dienste bzw. Anwendungen, die aus dem Internet erreichbar sind, um eine sogenannte externe DMZ ergänzt werden. Es sollte ein Konzept zur DMZ-Segmentierung erstellt werden, das die Sicherheitsrichtlinie und die Anforderungsspezifikation nachvollziehbar umsetzt. Abhängig vom Sicherheitsniveau der IKT-Systeme müssen die DMZ-Segmente weitergehend unterteilt werden. Eine externe DMZ muss am äusseren Paketfilter angeschlossen werden.

Externe Zone (untrusted)

Systeme in diesen Zonen werden durch Dritte betreut und/oder die Erfüllung der Sicherheitsanforderungen für Endsysteme kann nicht kontrolliert werden. Ein Zugang in diese Zone ist ohne Authentifizierung des Endsystems möglich.

Beispiele: Gemeinde extern/untrusted, Gebäudeleitsysteme extern/untrusted, BYOD, Access-Zone Gäste

## Sicherheitsanforderungen Netzwerk der [Gemeinde/Stadt]

* Grundsätzlich dürfen nur gehärtete Endsysteme mit einem definierten Software-Zustand (Virenschutz, Security-Patches usw.) Zugang zum Netzwerk der [Gemeinde/Stadt] erhalten.
* IKT-Systeme mit unterschiedlichem Schutzbedarf z.B. Clients und Server sollten in verschiedenen Sicherheitssegmenten platziert werden. Die Kommunikation zwischen diesen Segmenten muss mindestens durch eine Firewall kontrolliert werden. Ist dies nicht möglich, richtet sich der Schutzbedarf nach dem höchsten vorkommenden Schutzbedarf im Sicherheitssegment. Es muss sichergestellt werden, dass keine Überbrückung von Segmenten oder gar Zonen möglich ist. Öffentlich zugängliche Räume z.B. Präsentations-, Veranstaltungs- und Schulungsräume sollten in einem abgetrennten Segment angeschlossen sein.
* Alle Endgeräte, die für das Management der IKT-Infrastruktur benötigt werden, sollten in dedizierten Segmenten positioniert werden. Die Kommunikation mit diesen Endgeräten sollte durch eine Firewall kontrolliert werden.
* Wenn innerhalb von internem Netz, Extranet oder DMZ über Verbindungsstrecken kommuniziert wird, die für einen erhöhten Schutzbedarf nicht ausreichend sicher sind, sollte die Kommunikation angemessen auf Netzebene verschlüsselt werden.
* Der Internetverkehr muss über die Firewall-Struktur geführt werden, ausser wenn die [Gemeinde/Stadt] ausschliesslich über Leunet mit dem Internet verbunden ist. Die Datenflüsse müssen durch die Firewall-Struktur auf die benötigten Protokolle und Kommunikationsbeziehungen eingeschränkt werden.
* Für den Managementzugriff auf Netzkomponenten und auf Managementinformationen muss eine geeignete Authentisierung verwendet werden. Dafür müssen die entsprechenden Vorgaben umgesetzt werden. Die Default-Passwörter auf den Netzkomponenten müssen geändert werden. Die neuen Passwörter müssen ausreichend stark sein und regelmässig geändert werden.
* Die Netzmanagement-Lösung muss in das Protokollierungskonzept der [Gemeinde/Stadt] eingebunden werden (siehe auch Kapitel 15). Weiter müssen mindestens folgende Ereignisse protokolliert werden:
	+ Unautorisierte Zugriffe bzw. Zugriffsversuche
	+ Leistungs- oder Verfügbarkeitsschwankungen des Netzes
	+ Fehler in automatischen Prozessen z.B. bei der Konfigurationsverteilung sowie
	+ eingeschränkte Erreichbarkeit von Netzkomponenten
* Software bzw. Firmware und Konfigurationsdaten für Netzkomponenten sollten automatisch über das Netz verteilt und ohne Betriebsunterbrechung installiert und aktiviert werden können. Die benötigten Informationen sollten an zentraler Stelle sicher verfügbar sein sowie in die Versionsverwaltung und die Datensicherung eingebunden werden.

## Routers und Switches

* Ein Router oder Switch muss sicher konfiguriert werden, bevor er bei der [Gemeinde/Stadt] eingesetzt wird.
* Nur dafür autorisierte Personen dürfen die Geräte installieren und konfigurieren.
* Alle Konfigurationsänderungen müssen nachvollziehbar dokumentiert sein.
* Die Integrität der Konfigurationsdateien muss in geeigneter Weise geschützt werden.
* Die Standard-Benutzerkonten sind zu ändern, bevor Router und Switches in Betrieb genommen werden.
* Passwörter dieser Konten müssen geändert werden. Nicht benutzte Benutzerkonten müssen deaktiviert werden.
* Zugangspasswörter müssen verschlüsselt gespeichert werden.
* Router und Switches müssen so konfiguriert sein, dass nur zwingend erforderliche Dienste, Protokolle und funktionale Erweiterungen genutzt werden. Nicht benötigte Dienste, Protokolle und funktionale Erweiterungen müssen deaktiviert oder ganz deinstalliert werden. Ebenfalls müssen nicht benutzte Schnittstellen auf Routern und Switches deaktiviert werden.
* Unbenutzte Netzwerkports müssen nach Möglichkeit deaktiviert oder zumindest einem dafür eingerichteten Unassigned VLAN zugeordnet werden.
* Informationen über den internen Konfigurations- und Betriebszustand müssen nach aussen verborgen werden.
* Unnötige Auskunftsdienste müssen deaktiviert werden.
* Die/der ISV muss sich über bekannt gewordene Schwachstellen informieren.
* Updates und Patches müssen so schnell wie möglich eingespielt werden. Vorab sollte auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches für bekannte Schwachstellen verfügbar sind, müssen andere geeignete Massnahmen getroffen werden, um Router und Switches zu schützen.
* Ein Router oder Switch muss so konfiguriert werden, dass er unter anderem folgende Ereignisse protokolliert:
	+ Konfigurationsänderungen (möglichst automatisch)
	+ Reboot
	+ Systemfehler
	+ Statusänderungen pro Interface, System und Netzsegment
	+ Login-Fehler (zumindest dann, wenn sie wiederholt auftreten)
* Die Verantwortlichen müssen darauf achten, dass bei der Protokollierung alle rechtlichen Rahmenbedingungen eingehalten werden. Änderungen an der Konfiguration sollten zudem automatisch protokolliert werden.
* Die Konfigurationsdateien von Routern und Switches müssen regelmässig gesichert werden. Die Sicherungskopien müssen so abgelegt werden, dass im Notfall darauf zugegriffen werden kann.

## WLAN

* Die [Gemeinde/Stadt] muss eine generelle Strategie zur WLAN-Nutzung festlegen, bevor WLANs eingesetzt werden. Die Strategie muss beinhalten, in welchen Organisationseinheiten, für welche Anwendungen und zu welchem Zweck WLANs eingesetzt und welche Informationen darüber übertragen werden dürfen. Ebenso muss festgelegt werden, in welchen räumlichen Bereichen WLANs aufgebaut werden sollen.
* Access Points müssen zugriffssicher montiert werden. Ausseninstallationen müssen vor Witterungseinflüssen und elektrischen Entladungen wie Blitzschlag in geeigneter Weise geschützt werden.
* Die Kommunikation über das WLAN muss komplett kryptografisch abgesichert werden. Die eingesetzten kryptografischen Verfahren müssen den Standard WPA2 oder stärker erfüllen.
* Wird WPA2 mit Pre-Shared Keys (WPA2-PSK) verwendet, muss ein komplexer Schlüssel mit mindestens zwanzig Zeichen verwendet werden. Der Schlüssel sollte regelmässig gewechselt werden.
* Access Points dürfen nicht in der Konfiguration des Auslieferungszustandes verwendet werden. Voreingestellte SSIDs (Service Set Identifiers), Zugangskennwörter oder kryptografische Schlüssel der Access Points müssen direkt nach Inbetriebnahme geändert werden.
* Unsichere Administrationszugänge müssen abgeschaltet werden (z.B. Telnet oder http).
* Access Points müssen verschlüsselt administriert werden.
* Werden WLANs an ein LAN angebunden, sollte der Übergang zwischen WLANs und LAN abgesichert werden, beispielsweise durch einen Paketfilter.
* Bei Gästezugängen ins Internet genügt eine einfache User-Authentifizierung (z.B. als Self-Service-Portal mit einem SMS). Dadurch wird die gesetzeskonforme Registrierung und Überwachung von Benutzeraktivitäten eingehalten. Bei einem Sicherheitsvorfall können die Mobile-Nummern abgefragt werden.
* Bei allen Komponenten der WLAN-Infrastruktur (Access Points, Distribution System, WLAN-Management-Lösung etc.) sollte regelmässig überprüft werden, ob alle festgelegten Sicherheitsmassnahmen umgesetzt und diese korrekt konfiguriert sind.
* Öffentlich aufgestellte Access Points sollten regelmässig stichprobenartig darauf geprüft werden, ob es gewaltsame Öffnungs- oder Manipulationsversuche gab. Die Auditergebnisse sollten nachvollziehbar dokumentiert und mit dem Soll-Zustand abgeglichen werden. Abweichungen sollte nachgegangen werden.

## Firewall

* Eine Firewall muss sicher konfiguriert werden, bevor sie bei der [Gemeinde/Stadt] eingesetzt wird.
* Nur autorisierte Personen dürfen eine Firewall installieren und konfigurieren (z.B. die/der ISV Betrieb oder vertraglich gebundene Dienstleister).
* Die Integrität der Konfigurationsdateien sollte geeignet geschützt werden.
* Zugangspasswörter müssen verschlüsselt gespeichert werden.
* Die gesamte Kommunikation zwischen den beteiligten Netzen muss über die Firewall geleitet werden.
* Von aussen dürfen keine unbefugten Verbindungen in das geschützte Netz aufgebaut werden können. Aus dem geschützten Netz dürfen keine unbefugten Verbindungen aufgebaut werden können.
* Es müssen Verantwortliche benannt werden, die Filterregeln entwerfen, umsetzen und testen. Zudem muss geklärt werden, wer Filterregeln verändern darf. Die Entscheidungen, die relevanten Informationen und die Entscheidungsgründe müssen dokumentiert werden.
* Für die Firewall müssen eindeutige Regeln dafür festgelegt werden, welche Kommunikationsverbindungen und Datenströme zugelassen werden. Alle anderen Verbindungen müssen durch die Firewall unterbunden werden (Whitelist-Ansatz, Standardregel ist «deny»).
* Temporäre Regeln müssen zeitlich definiert werden, jedoch maximal drei Monate zugelassen sein, und wenn möglich automatisch deaktiviert werden.
* Die Regeln müssen die Kommunikationsbeziehungen mit angeschlossenen Dienst-Servern berücksichtigen, die über die Firewall geführt werden (z.B. E-Mail- oder Web-Servern).
* Die Firewall-Regeln müssen regelmässig überprüft werden. Nicht mehr benötigte Regeln sind umgehend zu löschen.
* IKT-Systeme dürfen von aussen nur über eine Firewall auf das interne Netz zugreifen.
* Informationen über den internen Konfigurations- und Betriebszustand müssen nach aussen bestmöglich verborgen werden.
* Die/der ISV muss sich über bekannt gewordene Schwachstellen informieren. Updates und Patches müssen so schnell wie möglich eingespielt werden. Vorab sollte auf einem Testsystem überprüft werden, ob die Sicherheitsupdates kompatibel sind und keine Fehler verursachen. Solange keine Patches bei bekannten Schwachstellen verfügbar sind, müssen andere geeignete Massnahmen getroffen werden, um die Firewall zu schützen.
* In regelmässigen Abständen müssen Systemsicherungen der Firewall erstellt werden. Das System muss ebenfalls gesichert werden, bevor eine Firewall neu installiert oder anders konfiguriert wird.
* Wenn gesicherte Datenbestände wieder eingespielt werden, müssen sich die sicherheitsrelevanten Dateien wie Access-Listen, Passwortdateien und Filterregeln auf dem sicherheitstechnisch erforderlichen Konfigurationsstand befinden.
* Alle Konfigurationsänderungen sowie sicherheitsrelevante Aufgaben einer Firewall müssen dokumentiert werden, insbesondere Änderungen an den Systemdiensten und dem Regelwerk der Firewall. Die Dokumentation muss vor unbefugten Zugriffen geschützt werden. Änderungen an der Konfiguration müssen möglichst automatisch protokolliert werden.
* Die Firewall muss so konfiguriert werden, dass sie mindestens folgende Ereignisse protokolliert:
	+ Konfigurations- und Regeländerungen
	+ abgewiesene Netzverbindungen (Quell- und Ziel-IP-Adressen, Quell- und Zielport oder ICMP/ICMPv6-Typ, Datum, Uhrzeit)
	+ fehlgeschlagene Zugriffe auf System-Ressourcen aufgrund fehlerhafter Authentisierungen, mangelnder Berechtigung oder nicht vorhandener Ressourcen
	+ allgemeine Systemfehlermeldungen

## VPN

* Für VPN-Clients, VPN-Server und VPN-Verbindungen muss eine sichere Konfiguration festgelegt werden. Sie sollte geeignet dokumentiert werden. Die zuständige Administratorin/der zuständige Administrator muss regelmässig kontrollieren, ob die Konfiguration noch sicher ist, und sie eventuell für alle IKT-Systeme anpassen.
* Wird ein externes Netz über ein VPN angebunden, sollten nach dem derzeitigen Stand der Technik sichere Authentifizierungs- und Verschlüsselungsverfahren mit ausreichender Schlüssellänge verwendet werden.
* Das Verfahren zum Schlüsselaustausch sollte dem Stand der Technik entsprechen. Es sollte sichergestellt werden, dass VPN-Verbindungen nur zwischen den dafür vorgesehenen IKT-Systemen und Diensten aufgebaut werden. Die eingesetzten Tunnelprotokolle sollten für den Einsatz geeignet sein.
* Es muss regelmässig geprüft werden, ob ausschliesslich berechtigte IKT-Systeme und Benutzende auf das VPN zugreifen können. Nicht mehr benötigte VPN-Zugänge müssen zeitnah deaktiviert werden. Der VPN-Zugriff sollte auf die benötigten Benutzungszeiten beschränkt werden.

# Mobiles Arbeiten und mobile Geräte

Wenn mobile Geräte für dienstliche Zwecke verwendet und diese auf dienstliche Informationen zugreifen, sind folgende Punkte sicherzustellen:

* Mobile Geräte müssen mit einem Boot-Passwort bzw. einem PIN-Code, Fingerabdruck o.ä. geschützt werden.
* Für den Zugriff von ausserhalb der Räumlichkeiten der Verwaltung ist eine Zwei-Faktor-Authentifizierung zu verwenden.
* Mobile Geräte sind stets mit den neuesten Softwareupdates zu versehen.
* Daten auf mobilen Geräten wie Notebooks oder Smartphones sind zu verschlüsseln.
* Falls auf Smartphones oder Tablets Applikationen mit Personendaten aufgerufen werden können, sind diese mit einem zusätzlichen Passwort zu schützen.
* Es ist sicherzustellen, dass nur zugelassene mobile Endgeräte Zugang zum internen Netzwerk haben. Der Anschluss privater mobiler Endgeräte an die internen Netzwerke ist zu unterbinden.
* Bei Verwendung von privaten Mobilgeräten für die Bearbeitung von Personendaten ist die Speicherung von Daten in Cloud-Speichern zu vermeiden oder zu unterbinden.
* Auf privaten Mobilgeräten sind zusätzliche Schutzprogramme wie Virenschutzprogramme zu verwenden.
* Die Informationen zu Verwaltungstätigkeiten sind ausserhalb der Räumlichkeiten und Anlagen der Verwaltung vor Einsicht von Dritten zu schützen, z.B. durch einen Sichtschutz (Polarisierungsfilter, Sichtschutzfolie).
* Wechselmedien wie USB-Speicher müssen mit einem Passwortschutz und einer Verschlüsselungssoftware ausgestattet sein.
* Es ist eine anerkannte Software zur Verfügung zu stellen, mit der Wechselmedien vor dem ersten Gebrauch sowie bei Bedarf sicher gelöscht werden können.

# Telefonie (VoIP)

Bei der Installation und Verwendung von Telefonie-Systemen über Voice-over-IP (VoIP) sind folgende Grundsätze zu beachten:

* Die Qualität der Sprachübertragung ist durch eine ausreichend grosse Bandbreite sicherzustellen (Quality of Service, QOS). Für den Netzwerkverkehr besteht wenn möglich eine dedizierte Netzwerkverbindung oder Prioritätsregeln (Quality of Service, QOS).
* Die Vor- und Nachteile von Soft- oder IP-Telefonen werden abgewogen. Falls IP-Telefone eingesetzt werden, sind diese wenn möglich über eigene Netzwerkanschlüsse angeschlossen. Mini-Switches werden nicht verwendet.
* Das Telefonie-Netz ist wo möglich vom PC-Netzwerk getrennt.
* Die Berechtigungen für den Telefonie-Server sowie die Endgeräte sind definiert und entsprechend den Vorgaben des Rollen- und Berechtigungskonzepts umgesetzt.
* Es sind nur wirklich benötigte Benutzeraccounts aktiv und deren Berechtigungen sind möglichst restriktiv gesetzt.
* Voreingestellte Initialpasswörter auf Geräten sind zu ändern.
* In einem Verzeichnis sind alle Nummern aufgeführt und den Teilnehmenden zugeordnet.
* Die einzelnen Komponenten sind im IKT-Inventar aufgeführt und mit einer Detailbeschreibung versehen.
* Nicht benötigte Ports sind deaktiviert.
* Nur wirklich benötigte Softwarekomponenten sind installiert.
* Sprach-, Signalisierungs- und Verbindungsdaten sind verschlüsselt. Das Schlüsselmanagement ist geregelt.
* Mit Vorteil wird ein System zur Erkennung von Angriffen auf die Telefonie-Infrastruktur (IDS/IPS) eingesetzt.
* Mit Vorteil wird ein System zur Erkennung des Anschlusses von nicht zulässigen Geräten eingesetzt.
* Die Telefoniekomponenten werden regelmässig aktualisiert und gepatcht.
* Falls eine Remote-Administration der Telefoniekomponenten eingesetzt wird, erfolgt diese abgesichert, z.B. verschlüsselt und mit Zertifikaten.
* Der Zutritt zur Telefonie-Infrastruktur (VoIP- Server-System) ist nur autorisierten Personen möglich.
* Benutzeraccounts von ausgetretenen Mitarbeiterinnen und Mitarbeitern werden zeitnah gelöscht.
* Dokumentationen und Verträge mit dem Betreiber der Telefonie-Umgebung sind vorhanden. Die Verträge enthalten im Minimum die wichtigsten Betriebsparameter wie:
	+ Garantierte Verfügbarkeit
	+ In- und Ausserbetriebnahme
	+ Verfahren bei Ausfällen von Hard- und Software
	+ Sicherheitsmassnahmen
	+ Wartung/Änderungen
	+ Zugriffsrechte/Administration
	+ Abrechnungsmodus
	+ Regelung Verantwortlichkeiten

# Drucker / Kopierer / Multifunktionsgeräte

Für den Einsatz von Druckern, Kopierern und Multifunktionsgeräten gelten folgende Grundsätze:

Beschaffung/Wartung

* Bei einer Wartung und einem Austausch müssen vor Abtransport eines Geräts alle darauf gespeicherten Daten unwiederbringlich gelöscht oder der Gerätespeicher ausgebaut werden. Für den letzteren Fall ist zu regeln, was mit dem Speicher geschieht.
* Für die Liefer-/Wartungsfirma ist eine Ansprechperson zu definieren, welche die ordnungsgemässe Abwicklung von Lieferung, Inbetriebnahme, Instruktion, Wartung und Austausch sicherstellt.
* Bei Lieferung ist ein Geräteabnahmeprotokoll zu verlangen und durchzuarbeiten, um sicherzustellen, dass sicherheitsrelevante Einstellungen nach Vorgabe konfiguriert sind.

Platzierung

* Drucker sind so aufzustellen, dass nur Berechtigte Zugang haben. Standorte, an denen sich Externe unbegleitet aufhalten können, sind zu vermeiden.
* Falls Geräte in öffentlich zugänglichen Räumen aufgestellt werden müssen, beispielsweise in Schulen oder Schalterräumen, ist darauf zu achten, dass die Geräte als Ganzes gegen Diebstahl gesichert sind. Die Datenspeicher der Geräte sind beispielsweise mit Schlössern an den Wartungsöffnungen zu schützen. Zusätzlich sind entsprechende Geräteeinstellungen vorzunehmen (keine permanente Speicherung von Daten, Ausdruck nur nach Login).
* Anstelle eines offenen Papierkorbs ist in der Nähe von gemeinsam genutzten Multifunktionsgeräten ein Schredder oder eine Reisswolf-Box zu platzieren, so dass Fehldrucke oder liegen gelassene Dokumente ordnungsgemäss vernichtet werden können.

Technische Massnahmen

* Der Einsatz von Netzwerkgeräten ist analog der Anbindung von Clients zu planen. Die Konfiguration, Berechtigungen usw. müssen festgelegt werden.
* Der Einsatz eines Druckservers ermöglicht die zentrale Protokollierung und Verwaltung sowie einen besseren Schutz vor Angriffen.
* Passwörtern für Bedienfeld (Konsole) sowie für ein allfälliges Web-GUI für die Wartung müssen eingerichtet werden. Vordefinierte Initialpasswörter sind zu ändern.
* Verschlüsselung der Kommunikation von und zu den Geräten mit IPSec- oder IPP-Protokoll sowie TLS/SSL ist sicherzustellen.
* Nicht benötigte Ports und Protokolle auf den Geräten sind zu sperren, um unerwünschte Verbindungen zu verhindern.
* E-Mail-Funktion sind zu sperren, falls nicht benötigt.
* Vordefinierte Zieleingaben sind zu verwenden, beispielsweise aus internem Adressbuch, statt manueller Zieleingabe (Mail-to, Scan-to).
* Daten aus dem Speicher nach Ausdruck/Kopie sind zu löschen, wenn möglich automatisch. Funktionen zum unwiederbringlichen Löschen von Daten sind zu verwenden.
* Festplatten beziehungsweise Gerätespeicher sind zu verschlüsseln.
* Authentifizierung der Benutzerinnen und Benutzer an den Geräten mit Passwort/PIN, Chipkarte oder ähnlichem ist zu aktivieren, damit ein Ausdruck erst nach Login erfolgt, insbesondere bei öffentlich zugänglichen Druckern.
* Automatischer Log-off des Benutzenden nach einer definierten Inaktivitätszeit ist konfigurieren.
* Benutzende sind nach einer bestimmten Anzahl fehlerhafter Anmeldeversuche automatisch zu sperren.
* Zugriffe und Zugriffszeiten für die Fernadministration der Geräte sind zu definieren und einzuschränken.
* Beim Einsatz von netzfähigen Komponenten sind Mechanismen zum Schutz vor Angriffen aus dem Netzwerk einzurichten, damit Geräte nicht unberechtigt an das Netzwerk angeschlossen werden können (z.B. IEEE 802.1X oder ähnliches Verfahren zur netztechnischen Zugangskontrolle verwenden).
* Interne Firewall zur Steuerung von Zugriffen ist zu verwenden. Wo vorhanden sind beispielsweise nur Zugriffe aus festgelegten IP-Bereichen zu ermöglichen.
* Separate Netzwerkzonen für Drucker, Kopierer und Multifunktionsgeräte sind zu verwenden.
* Netzwerkverbindungen vom Druckserver zu anderen IKT-Systemen ausser zu den voreingestellten Druckern sind zu verhindern.
* Drucker, Kopierer und Multifunktionsgeräte sind bei Sicherheitsprüfungen zu berücksichtigen.
* Gerätesoftware ist regelmässig zu aktualisieren.

Verfügbarkeit

Falls die Geräte eine hohe Verfügbarkeit aufweisen müssen, sind Massnahmen für die Überbrückung von Ausfällen vorzusehen:

* Konfigurationen sind zu dokumentieren und/oder zu speichern, damit Ersatzgeräte schnell eingerichtet werden können.
* Allenfalls sind Reservegeräten für Drucker, Kopierer, Multifunktionsgeräte und Druckserver vorzuhalten (Cold Standby).
* Für Verbrauchsmaterialien sind angemessene Reserven sicherzustellen und die Bestände sind zu überwachen.
* Damit Geräte, Gerätekomponenten und Verbrauchsmaterialien untereinander ausgetauscht werden können, sind einheitliche Geräte zu beschaffen.

Vertragliche Anforderungen

* Wartungs- oder Lieferverträgen mit festgelegten Reaktionszeiten sind abzuschliessen, die an die Anforderungen der [Gemeinde/Stadt] angepasst sind.
* Die datenschutzrechtlichen Aspekte und Geheimhaltungspflichten sind in Verträgen mit Lieferanten und Wartungsfirmen zu regeln.
* Die sicherheitsrelevanten Einstellungen und Massnahmen für Lieferung, Wartung und Austausch von Druckern, Kopierern und Multifunktionsgeräten sind zu regeln, beispielsweise Löschung von Daten oder Ausbau von Speichermedien.

# Verwaltung von Bedrohungen und Schwachstellen

Sämtliche IKT-Systeme und Anwendungen sind regelmässig auf Schwachstellen zu überprüfen. Schwachstellen sind innerhalb einer angemessenen Frist, gemäss ihrer Kritikalität, mit wirksamen Massnahmen zu begegnen (z.B. mit Updates). Die identifizierten Schwachstellen sind regelmässig zu rapportieren.

Die im IKT-Inventar erfassten Angaben wie Produkt, Modell, Hersteller und Version können dabei zur Prüfung auf allfällige Schwachstellen dienen.

Bei Auslagerung des IKT-Betriebs ist durch den Betreiber darzulegen, wie diese Massnahmen erfüllt werden.

# Verschlüsselungsmassnahmen

## Kryptografische Verfahren

Die verwendeten kryptografischen Verfahren entsprechen jeweils dem aktuellen Stand der Technik (AES
oder SHA-3). Sie sind im Anhang A – Kryptografische Verfahren geregelt [Anhang A einfügen]. Kryptografische Schlüssel sind während ihrer gesamten Lebensdauer ausreichend zu schützen (Generierung, Verwendung, Erneuerung, Sicherung, Zerstörung). Kompromittierte oder gebrochene kryptografische Schlüssel sind umgehend zu erneuern und die Informationen sind neu zu verschlüsseln.

Falls ein kryptografischer Schlüssel verloren geht oder nicht abgerufen werden kann, muss eine befugte Person den Zugriff auf die Informationen wiederherstellen können. Wenn kryptografische Schlüsselkopien zum Beispiel für Backup-Zwecke erstellt werden, müssen diese auf dieselbe Weise wie die kryptografischen Schlüssel selbst geschützt werden. Wird der originale kryptografische Schlüssel vernichtet, so sind Sicherungskopien ebenfalls zu vernichten.

## Digitale Zertifikate

Bei der Verwendung von digitalen Zertifikaten gelten folgende Anforderungen:

* Beim Einsatz von asymmetrischen kryptographischen Verfahren müssen die Zertifikate von einer akzeptierten CA (Certificate Authority) ausgestellt, respektive von einer akzeptierten RA (Registration Authority) überprüft sein.
* Zertifikate, die ausschliesslich für den internen Gebrauch verwendet werden, sind von internen CAs auszustellen, um selbst signierte Zertifikate zu vermeiden. Der erhöhte Schutzbedarf der internen CA ist sicherzustellen.
* Die CA-Hierarchie einer internen PKI (Public Key Infrastructure) besteht mindestens aus einer Stammzertifizierungsinstanz (Root CA) und einer ausstellenden Zertifizierungsstelle (Issuing CA). Root CAs sind offline und werden nur zur Ausstellung von neuen CAs oder Root CA CRLs in Betrieb genommen.
* Die Gültigkeitsdauer für Schlüssel von internen CAs (Root CA oder Issuing CA) darf maximal zehn Jahre betragen, für alle anderen Schlüssel maximal drei Jahre.
* Schlüssel von internen CAs sind durch ein Hardware-Security-Modul oder Verfahren mit äquivalenter Sicherheit zu schützen.
* Issuing CAs müssen regelmässig neue Zertifikatsperrlisten (CRL) ausstellen.
* Die verantwortlichen Stellen, beziehungsweise Personen werden vor Ablauf der Gültigkeit von Schlüsseln frühzeitig informiert.
* Details für den Einsatz von Zertifikaten sind in einer Certificate Policy (CP) und in einem Certificate Practice Statement (CPS) zu regeln.

# Datensicherung und -wiederherstellung

Für die Datensicherung und -wiederherstellung gelten die folgenden Anforderungen:

* Alle dienstlichen Daten müssen regelmässig gesichert werden.
* Die folgenden Parameter sind für die Datensicherungen einzuhalten und in der Betriebsdokumentation zu beschreiben:
	+ Sicherungszeitplan mit maximalem Zeitabstand zwischen zwei Sicherungen (RPO)
	+ Tägliche, wöchentliche, monatliche und jährliche Sicherung der Daten
	+ Art der Datensicherung (inkrementell oder voll)
	+ Aufbewahrungs- und Löschfristen von Backup-Daten: Aufbewahrung der monatlichen Sicherungen während eines Jahres und jährliche Sicherungen bis zur Archivierung der Daten
	+ Maximale Dauer bis zur Wiederherstellung von Daten sowie Prozess zur Wiederherstellung
* Für den Zugriff auf die Backup-Daten und ihre Übermittlung gilt mindestens das gleiche Schutzniveau wie für das zu sichernde Informationssystem.
* Die Ausführung von Backups ist zu überwachen. Fehlerhafte oder nicht ausgeführte Backups sind über das Incident Management zu verfolgen.
* Backup-Daten müssen in unterschiedlichen Gefahrenzonen und mit genügend örtlichem Abstand voneinander gespeichert und aufbewahrt werden. Backup-Daten sind zudem vor unbefugtem Zugriff zu schützen, entweder durch physische Massnahmen oder Verschlüsselung.
* Die Lesbarkeit von Datensicherungen ist für jedes eingesetzte Backup-Verfahren mindestens jährlich zu prüfen.
* Die Wiederherstellbarkeit von Daten und die Funktionalität von wiederhergestellten Informationssystemen sind gemäss Sicherungskonzept regelmässig zu prüfen.

Wenn für die Datensicherung ein Online-Speicher genutzt werden soll, müssen mindestens folgende Punkte im Vertrag mit dem Dienstleister geregelt werden:

* Ort der Datenspeicherung
* Vereinbarungen zur Dienstgüte (SLA)
* geeignete Authentisierungsmethoden
* Verschlüsselung der Daten
* Verschlüsselung auf dem Transportweg
* Schlüsselmanagement durch Auftragnehmende

Zu beachten sind in diesem Zusammenhang auch die folgenden Merkblätter:

* [Leitfaden Bearbeiten im Auftrag](https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_bearbeiten_im_auftrag.pdf)
* [Merkblatt Online-Speicherdienste](https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_online_speicherdienste.pdf)
* [Merkblatt Cloud Computing](https://docs.datenschutz.ch/u/d/publikationen/formulare-merkblaetter/merkblatt_cloud_computing.pdf)
* [Leitfaden Auslagerung: Berücksichtigung des CLOUD Act](https://docs.datenschutz.ch/u/d/publikationen/leitfaeden/leitfaden_auslagerung_beruecksichtigung_des_cloud_act.pdf)

# Sicherheit von Testdaten

Daten, insbesondere Personendaten und besondere Personendaten, auf nicht produktiven Umgebungen müssen entsprechend ihrer Klassifikation gemäss der Allgemeinen Richtlinie für Informationssicherheit und Datenschutz geschützt werden.

Die Weitergabe von produktiven Daten, insbesondere Personendaten und besonderen Personendaten, an Dritte zu Test- und Entwicklungszwecken sind zu regeln.

Tests sind, wenn immer möglich, mit anonymisierten oder pseudonymisierten Daten durchzuführen.

# Protokollierung und Kontrolle

Die Anforderungen an die Protokollierung gelten für alle IKT-Systeme und Fachapplikationen, die entsprechende Funktionen unterstützen. Falls dies auf bestehenden Systemen und Applikationen nicht gewährleistet ist, sind die Anforderungen bei ihrem Ersatz als Kriterium zu berücksichtigen.

## Allgemeine Anforderungen

* IKT-Systeme müssen über eine einheitliche Zeitangabe zur Protokollierung des Zeitpunkts eines Ereignisses verfügen (z.B. NTP).
* Protokolldaten müssen jederzeit zur Verfügung stehen und für eine zeitnahe Analyse zugänglich sein.
* Protokolldaten müssen nach Ablauf der erforderlichen Aufbewahrungsfrist gelöscht werden.
* Beim Zugriff auf Protokolldaten gelten die folgenden Anforderungen:
	+ Veränderungen an Protokolldaten müssen technisch unterbunden oder protokolliert werden.
	+ Zugriffsrechte auf Protokolldaten müssen gemäss dem Rollen- und Berechtigungskonzept der [Gemeinde/Stadt] umgesetzt werden.
	+ Die Protokollierungsfunktion der IKT-Systeme ist zu überwachen und bei Ausfall der Protokollierung über den Incident-Prozess zu behandeln.

## Sicherheitsprotokollierung

* Zur Erkennung von Angriffen auf die IKT-Sicherheit sind Protokolldaten von Benutzer- und Systemaktivitäten, Ausnahmen, Fehlern und informationssicherheitsrelevanten Ereignissen zu erstellen, aufzubewahren und regelmässig durch autorisiertes Personal zu überprüfen.
* Jedes IKT-System muss die folgenden Ereignisse aufzeichnen können:
	+ Systemereignisse, Systemfehler, Warnungen
	+ Benutzerereignisse, z.B. Starten von Applikationen, Zugriff auf Dateien, Hinzufügen eines neuen Accounts, Änderungen von Berechtigungen, Login eines Nutzenden, (De-)Aktivierung von Sicherheitsmechanismen (Logging, Anti-Virus usw.)
* Für jedes IKT-System sind die zu protokollierenden Ereignisse zu definieren.
* Protokollformate haben sich an gängigen Standards zu orientieren (z.B. Syslog Message Format)
* Protokolldaten müssen mindestens Folgendes enthalten:
	+ Identität der Entität, auf der das Ereignis auftrat (Domäne, IP-Adresse, DNS-Hostname) und Verursacher einer Aktivität
	+ Aktivität und Details von Ereignissen (z.B. An- und Abmeldung, Request Headers)
	+ Zeitstempel der Aktivität
	+ Ergebnis der Aktivität (Erfolg bzw. Misserfolg) einer Aktivität (z.B. HTTP-Statuscode 200 OK, erfolgreicher Zugriff)
* Ausgewählte Protokolldaten müssen wenn möglich in Echtzeit, aber mindestens täglich auf einer zentralen Protokollinfrastruktur gespeichert werden.
* Die Aufbewahrung von Protokolldaten in der zentralen Protokollinfrastruktur ist fallabhängig unter Berücksichtigung der datenschutzrechtlichen Vorgaben zu regeln.

## Applikationsprotokollierung

* In Fachapplikationen sind, wo dies technisch möglich ist, Logs zu führen, die es erlauben, die Pflicht zum Nachvollzug von Mutationen an Datensätzen zu erfüllen.
* Die Logs müssen folgende Angaben enthalten:
	+ Benutzererkennung
	+ Datum und Zeitpunkt der Mutation
	+ Geänderte Inhalte/Felder und vorheriger Wert
* Es müssen mindestens die letzte Mutation, falls möglich, auch mehrere, aufgezeichnet werden.

# Physische Sicherheit

Die Gebäude der [Gemeinde/Stadt], insbesondere die Räume, in denen Server- und Netzwerksysteme untergebracht sind, sind durch angemessene Massnahmen vor unbefugtem Zutritt sowie Umwelteinflüssen zu schützen.

## Zutritt

* Gebäude und Räume sind durch ein Schliesssystem geschützt.
* Zutrittsrechte und -mittel werden zentral verwaltet und dokumentiert.
* Zutrittsberechtigungen zu Gebäuden und Räumen werden gemäss einem definierten, dokumentierten und genehmigten Prozess erteilt.
* Zutrittsberechtigungen sind personengebunden zu erteilen.
* Zutritte bzw. Zugriffe auf Server- und Netzwerkkomponenten werden besonders restriktiv erteilt.
* Der Zutrittsprozess ist dokumentiert und die Einhaltung des Prozesses wird regelmässig überprüft.
* Zutritte werden, wenn möglich automatisiert, in einem Log festgehalten.

## Sicherheitsmassnahmen

Gebäude

* Die Verwaltungsgebäude sind gegen Blitzeinschläge geschützt.
* Die Verwaltungsgebäude und insbesondere Räume, in denen schützenswerte Daten untergebracht sind, sind mit angemessenen Massnahmen gegen Einbruch geschützt.
* Empfehlenswert ist die Installation von Sensoren für die Erkennung von Rauch und Hitze, die an ein Alarmierungssystem gekoppelt sind, das Warnmeldungen an einen definierten Personenkreis verschickt.

Server- und Netzwerkräume

Räume, in denen Server und Netzwerkkomponenten untergebracht sind, werden wie folgt geschützt.

Feuer

* Räume oder Schränke werden möglichst feuersicher ausgewählt (z.B. keine Räume mit Holzverkleidungen oder -balken, keine Holzschränke).
* Die Räume für die Unterbringung von Servern und Netzwerkkomponenten sind, wenn möglich, abgetrennt.
* In den Räumen dürfen keine brennbaren oder brandbeschleunigenden Materialien gelagert werden (Papier, Karton, Holz, Chemikalien etc.). Wo möglich werden Brandschutztüren eingesetzt. Staub und andere Verschmutzung werden verhindert.
* Essen, Trinken und Rauchen sind verboten.
* Falls Räume mit grosser Hitzeentwicklung verwendet werden, ist für eine ausreichende Kühlung gesorgt.
* Sensoren für die Erkennung von Rauch und Hitze sind installiert, die an ein Alarmierungssystem gekoppelt sind, das Warnmeldungen an einen definierten Personenkreis verschickt. Nach Möglichkeit ist eine IKT-konforme Feuerlöschanlage installiert.
* Türen und Fenster werden geschlossen gehalten.

Wasser

* Räume oder Schränke werden so gewählt, dass sie einem möglichst kleinen Wasserrisiko ausgesetzt sind (z.B. nicht im Keller, Räume ohne Wasserleitungen, Räume ohne Fenster, Räume nicht direkt unter dem Dach).
* Sensoren für die Erkennung von Wasser bzw. hoher Feuchtigkeit sind installiert, die an ein Alarmierungssystem gekoppelt sind, das entsprechende Warnmeldungen an einen definierten Personenkreis verschickt.
* Türen und Fenster werden geschlossen gehalten.

Beleuchtung

* Die Räume sind mit einer Notbeleuchtung ausgestattet, um den Zugang ohne externe Stromversorgung sicherzustellen.

Notstrom

* Im Minimum ist eine unterbrechungsfreie Stromversorgung (USV) vorhanden, die kurzfristige Stromausfälle kompensiert, respektive das kontrollierte Herunterfahren eines Servers gewährleistet. Optional werden damit auch Netzwerkkomponenten abgedeckt.
* Die Verkabelung (IKT und Notstrom) ist gekennzeichnet und dokumentiert.

# Fernwartung

Fernwartungszugänge erlauben die Übernahme der Kontrolle eines Rechners innerhalb einer Zone durch einen Nutzenden ausserhalb des Netzwerks der [Gemeinde/Stadt] (z.B. durch Supportpartner).

Benötigt eine externe Stelle oder der interne IKT-Betrieb den Einsatz von Fernwartungszugängen, muss der Anwendungszweck und die technische Umsetzung geklärt werden. Für jede Mitarbeiterin und jeden Mitarbeiter (intern und extern), die bzw. der einen Fernwartungszugriff benötigt, ist ein Antrag einzureichen. Als Voraussetzung für die Bewilligung sind folgende Anforderungen zu erfüllen:

* Der Einsatz und der Zweck des benötigten Zugangs müssen schriftlich definiert und klar begrenzt werden.
* Der Fernwartungszugang darf nur für die Bedürfnisse des Einsatzes und Zwecks genutzt werden. Eine weitergehende Nutzung ist nicht zulässig.
* Die Liste der aktuell Berechtigten muss laufend geführt werden.
* Die Authentifizierung aller Zugriffe hat über eine zentrale Instanz zu erfolgen.
* Eine starke Authentisierungsmethode ist zu verwenden.
* Die Menge der Rechner, die von aussen erreicht werden können, ist auf die minimal notwendige Anzahl zu begrenzen.
* Der Zugang muss indirekt mit einem VPN über einen kontrollierbaren Rechner (Jump-Host) in einer DMZ erfolgen. Alle Zugriffe und Interaktionen sind zu protokollieren. Die Protokolle müssen zentral, revisionssicher aufbewahrt werden.
* Die Freischaltung von temporären Zugriffen externer Partner (unregelmässiger Zugriff) erfolgt auf vorgängige Anfrage zentral und ist zeitlich auf ein Minimum beschränkt (z.B. zwei Stunden).
* Es ist technisch sicherzustellen, dass Zugriffe von externen Partnern nur innerhalb des bewilligten Zeitfensters stattfinden können.
* Der Zugriff auf Ressourcen, die nicht für die Zweckerfüllung benötigt werden, ist zu unterbinden.

Es werden keine Firmenzugänge bereitgestellt, sondern nur persönliche Zugänge für berechtigte Mitarbeitende des Partners.

* Strategische Partner können einen 7×24-Std.-Zugang beantragen.
* Situativ benötigte Zugänge von Partnern werden zeitlich befristet freigeschaltet.
* Mit externen Mitarbeitenden bzw. deren Arbeitgeber sind die Rahmenbedingungen in einem Vertrag zu regeln. Dabei sind mindestens folgende Punkte vorzusehen:
	+ Vor Erteilung einer Berechtigung erfolgt eine angemessene Sicherheitsüberprüfung.
	+ Jede und jeder berechtigte externe Mitarbeitende muss die Beachtung der Vorschriften und Rahmenbedingungen für den Fernwartungszugang schriftlich bestätigen.
	+ Eine Geheimhaltungsverpflichtung muss unterzeichnet werden.

# Umgang mit Informationssicherheitsvorfällen

[Diesen Absatz löschen, wenn der Betrieb vor Ort erfolgt:] Bei Kenntnisnahme von Informationssicherheitsvorfällen erfolgt eine sofortige Rapportierung durch den IKT-Betreiber [Firma] an die ISV oder den ISV der [Gemeinde/Stadt] respektive deren/dessen Stellvertretung. Diese/dieser rapportiert bei Bedarf an [die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber].

[Diesen Absatz löschen, wenn der Betrieb ausgelagert wurde:] Bei Kenntnisnahme von Informationssicherheitsvorfällen erfolgt eine sofortige Rapportierung durch die ISV oder den ISV an [die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber].

Mögliche Informationssicherheitsvorfälle sind (nicht abschliessend):

* Verlust, Löschung oder Vernichtung von Daten, Kopien von Daten oder von Datenträgern
* Veränderung oder Manipulation von Informationen
* Unberechtigter Zugriff oder Bekanntgabe an Unbefugte
* Funktionalität eines oder mehrerer Informationssysteme gestört oder nicht mehr vorhanden

Beweismittel zum Nachvollzug des Informationssicherheitsvorfalls sind zu sichern.

# Genehmigung und Inkrafttreten

Beschlossen durch [die Gemeindeschreiberin/den Gemeindeschreiber / die Stadtschreiberin/den Stadtschreiber] mit Beschluss [NR.] am [DATUM].

[Ort und Datum] [Name]

[Gemeinde/Stadt] [Gemeindeschreiberin/Gemeindeschreiber / Stadtschreiberin/Stadtschreiber]

V 1.2 / Oktober 2023

[Anhang A – Kryptografische Verfahren ergänzen]