Vorlage

Betriebsdokumentation [Gemeinde/Stadt]

Erläuterung zur Vorlage

Die Vorlage Betriebsdokumentation 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, 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 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Betriebsdokumentation [Gemeinde/Stadt]

Die Betriebsdokumentation in der vorliegenden Form stellt eine Maximalvariante dar. Falls einzelne Technologien nicht eingesetzt werden, kann auf die jeweiligen Kapitel verzichtet werden, ebenso bei Auslagerung von bestimmten Diensten oder Komponenten.

Allgemeines

Der Gliederungspunkt «Allgemeines» soll nicht als Kapitel gestaltet werden. Er fasst allgemeine Informationselemente zusammen, die das Dokument ergänzen.

* Verteilerliste
* Inhaltsverzeichnis
* Abkürzungen
* Definitionen
* Verzeichnis der Abbildungen und Tabellen
* Referenzierte Dokumente

# Zweck des Dokuments

Erläuterung, zu welchem Zweck das Dokument erstellt wurde

# Einführung

Erläuterung, an wen das Dokument gerichtet ist und Verweis auf zugrundeliegende oder ergänzende Dokumente/Richtlinien

## Zielgruppen

## Verweise auf Richtlinien

# Organigramm

Erläuterung, wer für die IKT-Umgebung und deren Betrieb verantwortlich und zuständig ist

## Organigramm

## Verantwortlichkeiten

### Beschaffung

### Betrieb

## Kontaktpersonen

# Lokalitäten

Erläuterung der verschiedenen Gebäude und Räumlichkeiten, in denen IKT-Komponenten zum Einsatz kommen sowie Zutrittsregelungen und Schutzmassnahmen

## Standort und Räumlichkeiten

## Zutrittsregelung und -prozesse

## Zutrittsrechte

## Schutzmassnahmen

### Stromausfall

### Feuer

### Feuchtigkeit / Wasser

### Hitze

### Einbruch

### Blitzschlag

## Alarmierung

### Überwachungssystem

### Alarmierungsart und -empfänger

# Systemübersicht

Gesamtüberblick über die IKT-Umgebung

## Überblick/Diagramm IKT-Architektur

## Mengengerüste

## Standortpläne

## Hard- und Softwareverzeichnis

### Hardware (Verweis auf IKT-Inventar)

### Software (Verweis auf IKT-Inventar)

### Lizenzen (Verweis auf IKT-Inventar)

# Netzwerk

Beschreibung der eingesetzten Netzwerke

## Überblick Netzwerke (Kabel, kabellos)

## Technische Beschreibung Kabelnetzwerk

### Netzpläne / -diagramme

### Zonen / Zonentrennung

### Protokolle

### Verschlüsselung

### Netzwerkauthentisierung

## Technische Beschreibung kabellose Netzwerke

### Netzpläne / -diagramme

### Zonen / Zonentrennung

### Protokolle

### Verschlüsselung

### Netzwerk- und Userauthentifizierung

### Access Points / SSID

# Server

Beschreibung der eingesetzten Server (falls lokal vorhanden)

## Überblick Server

## Technische Beschreibung des/r Systems/e

### Technische Beschreibung

### Einsatzzweck

### Betriebssystem

### Konfiguration

### Spezielle Einstellungen

### Speicher / Partitionierung

### Installierte Anwendungen und Hilfsprogramme

### Referenzinstallation / Image

## Externe Schnittstellen

## Directory-Struktur

### Installationsverzeichnisse

### Applikationen

### User-Basisverzeichnisse (Home)

### Daten

### Log-Dateien

## Benutzer und Rechte (Administration und technisch)

## Administrationspasswörter (siehe Notfallkonzept)

## Voraussetzungen zur Aufnahme bzw. Wiederaufnahme des Betriebs

## Massnahmen zur Aufnahme des Betriebs

### Start/Stop Server

### Start/Stop Dienste

### Start/Stop Applikationen

# Speichersysteme

Beschreibung der eingesetzten Speichersysteme (falls lokal vorhanden)

## Überblick eingesetzte Speichersysteme

## Technische Beschreibung des/r Systems/e

### Technische Beschreibung

### Einsatzzweck

### Betriebssystem

### Konfiguration

### Spezielle Einstellungen

### Speicher / Partitionierung

## Wechselmedien

### Technische Beschreibung

### Einsatzzweck

### Passwortschutz / Verschlüsselung

### Sichere Löschung

## Administrationspasswörter (siehe Notfallkonzept)

# Clients

Beschreibung der eingesetzten Clients

## Überblick Clients (fest und mobil)

## Technische Beschreibung der Systeme

### Technische Beschreibung

### Einsatzzweck

### Betriebssystem

### Konfiguration

### Spezielle Einstellungen (z.B. Festplattenverschlüsselung)

### Speicher / Partitionierung

### Installierte Anwendungen und Hilfsprogramme

### Referenzinstallation / Image

## Schnittstellen / Vernetzung

## Benutzer und Rechte (Administration und technisch)

## Administrationspasswörter (siehe Notfallkonzept)

# Drucker, Kopierer, Multifunktionsgeräte

Beschreibung der vorhandenen Clients

## Überblick Drucker, Kopierer und Multifunktionsgeräte

## Technische Beschreibung der Systeme

### Technische Beschreibung

### Einsatzzweck

### Konfiguration

### Spezielle Einstellungen (z.B. Festplattenverschlüsselung)

### Speicher

### Userauthentifizierung, Passwörter

## Schnittstellen / Vernetzung

## Administrationsbenutzer und -rechte

## Administrationspasswörter (siehe Notfallkonzept)

# Router

Beschreibung der eingesetzten Router

## Überblick Router

## Technische Beschreibung des/r Systems/e

### Technische Beschreibung

### Einsatzzweck

### Betriebssystem

### Konfiguration

### Spezielle Einstellungen

## Schnittstellen / Vernetzung

## Administrationsbenutzer und -rechte

## Administrationspasswörter (siehe Notfallkonzept)

# Firewall

Beschreibung der eingesetzten Firewall(s) (Ausnahme: [Gemeinde/Stadt] verfügt ausschliesslich über einen Leunet-Anschluss und über keine eigenen Server vor Ort)

## Überblick Firewall(s)

## Technische Beschreibung des/r Systems/e

### Technische Beschreibung

### Einsatzzweck

### Betriebssystem

### Konfiguration

### Spezielle Einstellungen

### Schnittstellen / Vernetzung

### Administrationsbenutzer und -rechte

### Firewall-Regeln

### Prozesse für Firewall-Regeln (siehe auch Change-Management)

### Administrationspasswörter (siehe Notfallkonzept)

# Datenverbindungen

Beschreibung der vorhandenen externen Datenverbindungen (nicht notwendig, wenn [Gemeinde/Stadt] nur über Leunet mit dem Internet verbunden ist)

## Überblick Datenverbindungen

## Technische Beschreibung des/r Systems/e

### Technische Beschreibung

### Einsatzzweck / Verbindungspartner

### Konfiguration

### Verschlüsselung / Schlüsselmanagement

### Zertifikate

### Spezielle Einstellungen

# Zugriffsrechte

Erläuterung der Zugriffsstrukturen, mit Verweis auf Rollen- und Berechtigungskonzept

## Rechte- und Benutzerstrukturen

## Vergabe von Zugriffsberechtigungen (Administratoren, technische User)

# Protokollierung

Beschreibung der Protokollierungsvorkehrungen, wo technisch möglich

## Umfang

### Systeme unter Protokollierung

### Zeitsynchronisation

### Sicherheitsprotokollierung

### Benutzerprotokollierung

### Speicherort der der Protokolle

### Schutz der Protokolle vor Veränderung

### Aufbewahrungsdauer Protokolle

## Auswertung

### Auswertungsmöglichkeiten

### Berechtigungen für Auswertungen

# Remote-Zugriffe

Beschreibung von Remote-Zugriffen sowohl für Benutzende als auch Betreiber oder Lieferanten

## Zugriffsmethoden (z.B. VPN)

### Konfiguration

### Verschlüsselung

## Zugriffsberechtigte

### Prozess/Kompetenzen zur Zugriffsgewährung

### Geheimhaltungsverpflichtung

# Betriebsprozesse

Beschreibung der Prozesse für die Aufrechterhaltung des Betriebs und der Sicherheit

## Patch Management

### Überwachung auf Schwachstellen

### Überwachung auf Updates und Patches

### Regelungen zur Systemaktualisierung

## Wartung

### Betriebszeiten

### Wartungsfenster

### Regelung zur Benutzerinformation

## Incident Management

### Prozesse

### Verantwortlichkeiten / Kontakte

### Tool / Hilfsmittel

## Change Management

### Prozesse

### Verantwortlichkeiten / Kontakte

### Tool / Hilfsmittel

### Test- und Abnahmeverfahren

## Monitoring

### Überwachung Verfügbarkeit, Performance und Speicher

### Berichterstattung

## Security Management

### Vorgehen/Meldeweg bei Detektion von Sicherheitsvorfällen

### Protokollierung / Dokumentation

# Ausserbetriebnahme

Erläuterung, wie Daten gelöscht und Systeme entsorgt werden

## Löschprozesse

## Entsorgung

# Betriebssicherheit

Erläuterung der Massnahmen zur Sicherstellung der Informationssicherheit

## Technische Sicherheitsmassnahmen

### Benutzerauthentifizierung

### Passwörter

### Einschränken von Systemfunktionen

### Einschränken von Dateizugriffen

### Sperrung von Geräten

### Schutz vor Schadsoftware

### Sperren des BIOS

## Malware- und Virenschutz

### Eingesetzte Produkte

### Verteilung

### Aktualisierung

## Internetbrowser

### Eingesetzte Produkte

### Sicherheitskonfiguration

# Datensicherung

Beschreibung der eingesetzten Datensicherungstechnologie, des Umfangs, der Periodizität und der Aufbewahrung sowie der Wiederherstellungsprozesse

## Art der Datensicherung

### Inkrementelle Backups

### Vollbackups

### Generationen (Tag, Monat, Jahr)

## Lokales Datensicherungssystem

### Backup-System

### Beschriftung der Speichermedien

### Schutzmassnahmen (z.B.Verschlüsselung)

### Aufbewahrung (Ort, Auslagerung)

### Aufbewahrungsdauer, Löschung

## Remote Datensicherungssystem

### Art der Datensicherung

### Ort der Datenspeicherung

### Vertragliche Grundlagen

### Dienstgüte (SLA)

### Verschlüsselung / Schlüsselmanagement

### Aufbewahrungsdauer, Löschung

## Zu sichernde Daten

### Konfigurationsdaten

### Benutzerdaten

## Sicherungszeitplan

### Sicherungsintervalle

### Max. Abstand zwischen Sicherungen (RPO)

### Max. Dauer Wiederherstellung (RTO)

## Wiederherstellung von Daten

### Prozesse und Kompetenzen zur Wiederherstellung

### Reaktionszeiten

### Wiederherstellungstests

# Telefonie

Beschreibung der VoIP-Telefonie-Infrastruktur

## Telefonserver

### Typ

### Konfiguration

### Berechtigungen

### Passwörter (siehe Notfallkonzept)

## Eingesetzte Telefone

### Gerät/Typ (Soft- oder IP-Telefon)

### Anschluss Telefone

### Konfiguration Telefone

### Berechtigungen

### Passwörter

## Generelles

### Nummernverzeichnis

### Verschlüsselung / Schlüsselmanagement

### Remote-Administration

### Protokollierung

### Vertragliche Grundlagen

### Dienstgüte (SLA)

# Notfallvorsorge

Die Risiken und Notfallmassnahmen sind grundsätzlich im Notfallkonzept der [Gemeinde/Stadt] beschrieben. In diesem Kapitel können Massnahmen auf Seiten des Betreibers aufgeführt werden.

## Notfallregelungen Betreiber

## Notfallkontakte Betreiber

## Notfalltests und Koordination mit Betreiber

V 1.2 / Oktober 2023