Vorlage

Notfallkonzept

Erläuterung zur Vorlage

Das vorliegende Dokument Notfallkonzept 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://www.datenschutz.ch/) publiziert.

Notfallkonzept [ORGAN\_S1\_S2]

Inhalt

[1 Allgemeine Bestimmungen 4](#_Toc74231487)

[1.1 Gegenstand und Zweck 4](#_Toc74231488)

[1.2 Geltungsbereich 4](#_Toc74231489)

[1.3 Gesetzliche Grundlagen und Standards zur Informationssicherheit 4](#_Toc74231490)

[2 Notfallorganisation und -infrastruktur 5](#_Toc74231491)

[2.1 Notfallorganisation 5](#_Toc74231492)

[2.2 Notfallinfrastruktur 6](#_Toc74231493)

[3 Bedrohungen 7](#_Toc74231494)

[3.1 Bedrohungsarten (BA) 7](#_Toc74231495)

[3.2 Bedrohungsanalyse 8](#_Toc74231496)

[4 Massnahmenplan 10](#_Toc74231497)

[5 Prozess bei Notfällen 11](#_Toc74231498)

[6 Kommunikation und Öffentlichkeitsarbeit 12](#_Toc74231499)

[7 Notfallübungen und -tests 13](#_Toc74231500)

[8 Überprüfungsprozess 13](#_Toc74231501)

[9 Genehmigung und Inkrafttreten 13](#_Toc74231502)

[10 Begriffsdefinition 14](#_Toc74231503)

[Anhang A: Notfallorganisation / Ansprechpersonen [ORGAN\_S1\_S2] 16](#_Toc74231504)

[Anhang B: Wichtige Unterlagen, Passwörter u.a. [ORGAN\_S1\_S2] 17](#_Toc74231505)

Dokumentenverantwortung

Verantwortlich für die Erstellung sowie die periodische Überprüfung des Dokuments ist [Name verantwortli­che Person(en)]

Das Dokument wird [jährlich, alle zwei Jahre, alle drei Jahre (maximal)] auf seine Aktualität und Richtigkeit überprüft und gegebenenfalls angepasst (siehe Ziffer 8). Die Überprüfung sowie allfällige Änderungen sind in der Änderungskontrolle nachgetragen.

Änderungskontrolle

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

Verteiler

|  |  |  |
| --- | --- | --- |
| Funktion | Name | Abteilung |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Allgemeine Bestimmungen

## Gegenstand und Zweck

Die [ORGAN\_S1\_S2] ist zur Erfüllung ihrer Aufgaben auf verschiedene Faktoren angewiesen wie Mitarbeite­rinnen und Mitarbeiter, Gebäude, IT-Komponenten, Versorgung mit Strom und Netzwerk. Das Notfallkonzept beschreibt die Notfallplanung für Geschäftsprozesse und/oder Ressourcen (Schutzobjekte), um die Aufrecht­erhaltung und Wiederherstellung der ordnungsmässigen Geschäftsfähigkeit in ausserordentlichen Situatio­nen zu gewährleisten.

Das Notfallkonzept ist mit allfälligen externen Leistungserbringern (SLA) und/oder Verantwortlichen bei der [ORGAN\_S1\_S2] inhaltlich abgestimmt. Es ist so gestaltet, dass Dritte in der Lage sind, die Notfallmassnah­men durchzuführen.

Das Notfallkonzept adressiert folgende Fragen:

* Wer ist im Notfall wofür verantwortlich?
* Wo befinden sich in einem Notfall das Lagezentrum, der Sammelplatz und allfällige Ausweicharbeits­plätze?
* Welche Bedrohungen können die Prozesse der [ORGAN\_S1\_S2] gefährden?
* Welche Massnahmen können ergriffen werden, um diese Bedrohungen zu vermindern oder verhindern?
* Wie und durch wen wird in einer Notfallsituation kommuniziert?

## Geltungsbereich

Dieses Notfallkonzept gilt für alle Mitarbeitenden der [ORGAN\_S1\_S2]. Auftragnehmende Firmen sind ver­traglich zur Einhaltung der entsprechenden Anforderungen zu verpflichten.

## Gesetzliche Grundlagen und Standards zur Informationssicherheit

Die rechtlichen Grundlagen der [ORGAN\_S1\_S2] sind:

* Gesetz über die Information und den Datenschutz (IDG, [LS 170.4](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.4,12.02.2007,01.10.2008,109))
* Verordnung über die Information und den Datenschutz (IDV, [LS 170.41](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.41,28.05.2008,01.10.2008,108))
* Verordnung über die Informationsverwaltung und -sicherheit (IVSV, [LS 170.8](http://www.zhlex.zh.ch/Erlass.html?Open&Ordnr=170.8,03.09.2019,01.01.2020,107))
* [ENTSPRECHENDE WEITERE GESETZLICHE GRUNDLAGEN AUFFÜHREN]

Die IVSV regelt unter §§ 12 und 13 die Pflicht von Amtsstellen, die Risiken und den Schutzbedarf für die von ihr verwalteten Informationen zu beurteilen und angemessene organisatorische und technische Massnah­men zum Schutz der Informationen zu treffen.

Vorgaben und Best Practices finden sich im [Standard 100-4](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/bsi-standard-100-4-notfallmanagement_node.html) des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) sowie dem ISO-Standard 27031. Grundlage des Notfallkonzepts bildet zudem die Leitlinie zur Informationssicherheit.

# Notfallorganisation und -infrastruktur

## Notfallorganisation

Nachfolgend ist aufgezeigt, welche Personen der Notfallorganisation angehören und wie die Verantwortlich­keiten und Unterstellungen geregelt sind. Eine ausreichende Stellvertretung ist berücksichtigt und die invol­vierten Mitarbeitenden oder externen Partner sind für ihre Aufgaben vorbereitet und geschult.

Die Zuweisung der Aufgaben der Notfallorganisation sowie die Kontaktangaben der Personen und Firmen sind unter Anhang A erfasst.

Abbildung 1: Organigramm Notfallorganisation

Die Aufgaben der Notfallorganisation sind:

|  |  |  |
| --- | --- | --- |
| Rolle / Funktion | Aufgaben | Kompetenzen |
| Leitung Notfallorganisation | Leitung und Koordination | Genehmigung von Ressourcen  … |
| Kommunikation | Mitarbeiterinnen, Mitarbeiter, Presse und Öffentlichkeit informie­ren | Ansetzen von Medienkonferenzen  … |
| Stab/Assistenz (optionale Funk­tion) | Unterstützung der Leitung  … | Gemäss Auftrag der Leitung  … |
| IT-Koordinator | Wiederherstellung IT-Betrieb | Kontakt mit IT-Dienstleistern  Zugriff auf Passwörter |
| … | … | … |

Tabelle 1: Aufgaben und Kompetenzen Notfallorganisation

## Notfallinfrastruktur

Nachfolgend ist festgelegt, wo sich in einem Notfall das Lagezentrum befindet sowie der Sammelplatz bei einer Evakuation. Zudem ist definiert, wo Ausweichstandorte bereitgestellt werden können, um den Ge­schäftsbetrieb wiederaufzunehmen.

|  |  |  |
| --- | --- | --- |
| Art des Notfalls | Treffpunkt / Ausweichstandort | Erforderliche Hilfsmittel |
| Evakuation | Sammelplatz gemäss Evakuations­plan (…) | Mobiltelefon  Personalliste |
| Ausfall Gemeindehaus | Sitzungszimmer Schulhaus … | Notfallorder  Laptop  Mobiltelefon |
| Stromausfall Gemeindehaus | Sitzungszimmer Gemeindehaus | Notfallordner  Laptop  Mobiltelefon |
| Ausfall IT / Strom Gemeindehaus | Schulhaus … | Arbeitsanweisungen  Kontaktdaten  Formulare … |

Tabelle 2: Lagezentrum / Ausweichstandorte



Abbildung 2: [Karte Standort Lagezentrum, mit entsprechendem Kartenausschnitt zu ersetzen]

# Bedrohungen

## Bedrohungsarten (BA)

Der vollständige Bedrohungskatalog der [ORGAN\_S1\_S2] ist im Excel-Dokument [Notfallkonzept Bedrohungsanalyse und Massnahmen](https://docs.datenschutz.ch/u/d/informationssicherheit/konzept/identisch/vorlage_notfallkonzept_bedrohungsanalyse.xlsx) aufgeführt.

Die folgende Tabelle listet Beispiele möglicher Bedrohungsarten auf, welche die [ORGAN\_S1\_S2] oder Teile davon beeinträchtigen können. Sie kann aus der produkti­ven Version des Dokuments entfernt werden.

|  |  |
| --- | --- |
| Bedrohungsart | Beschreibung |
| Elementarereignisse | Hochwasser, Grossbrand, Überschwemmung, Sturmwind etc. |
| Organisatorische Mängel | Abwesenheiten von Schlüsselpersonen, nicht definierte Verantwortung, fehlendes Know-How, fehlende Einbindung von Dritten, mangelhafte Verträge |
| Menschliche Fehlhandlung | Versehentliche Beschädigung, Datenvernichtung, Schlüsselverlust etc. |
| Technisches Versagen | Ausfall Stromzufuhr, Kabelbrand, Kurzschluss, Hard- und Softwarefehler etc. |
| Vorsätzliche Handlungen | Hacker-Angriff, Sabotage, Überfall, Diebstahl, Vandalismus etc. |
| … |  |

Tabelle 3: Bedrohungsarten

## Bedrohungsanalyse

Die Bedrohungsanalyse hält fest, welche Bedrohungen auf die [ORGAN\_S1\_S2] wirken können. Die einzelnen Bedrohungen sind auf ihre Auswirkung (AW) und ihre Eintrittswahrscheinlichkeit (EW) bewertet, woraus sich das Risiko (brutto) aus der Multiplikation AW \* EW ergibt.

Zu jeder Bedrohung sind Massnahmen aufgeführt, mit denen das Risiko verhindert oder verringert werden kann. Für einzelne Bedrohungen kann entschieden wer­den, keine Massnahmen einzuleiten. Sodann wird das Risiko (netto) bei Umsetzung der Massnahmen bewertet.

Da sich die Bedrohungslage über die Zeit verändert, werden die Bedrohungen und Massnahmen regelmässig überprüft und bei Bedarf aktualisiert.

Nachfolgend sind Eintrittswahrscheinlichkeit und Auswirkung definiert.

|  |
| --- |
| Eintrittswahrscheinlichkeit (EW) |
| 1 = Unwahrscheinlich: Tritt alle 10 Jahre oder seltener ein |
| 2 = Möglich: Kann etwa einmal pro Jahr eintreten |
| 3 = Wahrscheinlich: Kann etwa einmal pro Monat eintreten |
| 4 = Sehr wahrscheinlich: Kann einmal pro Woche oder öfter eintreten |

|  |
| --- |
| Auswirkung (AW) |
| 1 = Niedrig: Ausfall hat eine geringe, kaum merkliche Auswirkung |
| 2 = Mittel: Ausfall hat merkliche Auswirkungen |
| 3 = Hoch: Ausfall hat erhebliche Auswirkungen |
| 4 = Sehr hoch: Ausfall oder Beeinträchtigung führen zu gravierenden Auswirkun­gen |

Die folgende Tabelle ist zur Erläuterung de Methodik aufgeführt. Die vollständige Bedrohungsanalyse ist im Excel-Dokument [Notfallkonzept Bedrohungsanalyse und Massnahmen](https://docs.datenschutz.ch/u/d/informationssicherheit/konzept/identisch/vorlage_notfallkonzept_bedrohungsanalyse.xlsx) aufgeführt.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bedrohung Nr. | Bedrohung | Ergänzende Beschreibung | EW (1-4) | AW (1-4) | Risikostufe brutto | Massnahme |
| B01 | Grossfeuer | Vernichtung Gemeindehaus  Verlust Papierunterlagen  Ausfall Arbeitsplätze | 1 | 4 | 4 (Mittel) | M1: Feuermelder / Löschanlagen  M2: Elektronische Ablage Daten  M3: Schaffung von Ausweicharbeitsplätzen |
| B02 | Lokales Kleinfeuer | Brand in einzelnen Räumen, Verlust Unterlagen | 2 | 2 | 4 (Mittel) | M1: Feuermelder / Löschanlagen  M2: Elektronische Ablage Daten |
| B03 | Ungünstige klimatische Bedingungen, z.B. Hitze | Überhitzung elektrische Anlagen | 2 | 2 | 4 (Mittel) | M4: Temperaturüberwachung / Klimagerät |
| B04 | Überschwemmung | Interner Schaden oder Überschwem­mung von aussen | 2 | 3 | 6 (Hoch) | M5: Wassermelden |
| B10 | Abwesenheit von Schlüsselperson(en) | Wichtige Aufgaben können nicht aus­geführt werden | 3 | 2 | 6 (Hoch) | M6: Aufbau und Dokumentation Stellvertre­tung |
| B11 | Ausfall oder Störung der Stromversorgung | Betriebsunterbruch | 2 | 3 | 6 (Hoch) | M7: Redundante Stromanbindung oder Notstromaggregat |
| u.a.m. | u.a.m. | … | … | … | … | … |

Tabelle 4: Bedrohungsanalyse

# Massnahmenplan

Abgeleitet aus der Bedrohungsanalyse werden alle Massnahmen in einen entsprechenden Plan übernommen, auf ihre Aufwände/Kosten und Umsetzungszeit in Rela­tion zum Risiko beurteilt und darauf basierend entschieden, ob und wie schnell die Massnahme umgesetzt wird oder nicht. Es gilt zu beachten, dass die Kosten auch interne Aufwände enthalten können.

Bei Umsetzung der Massnahme wird die Risikostufe entsprechend neu bewertet und es wird eingetragen, wann die Massnahme umgesetzt wurde.

Die nachfolgende Tabelle soll zur Veranschaulichung des Vorgangs dienen, der vollständige und konkret ausgefüllte Massnahmenplan ist im Excel-Dokument Vorlage Notfallkonzept Bedrohungsanalyse und Massnahmen aufgeführt. Sie kann aus der produktiven Version dieses Dokuments entfernt werden.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Bedrohung Nr. | Risikostufe brutto | Massnahme | Aufwand / Kosten Massnahme | Massnahme umsetzen J/N | Risikostufe netto | Massnahme umgesetzt |
| B01 / B02 | 4 (Mittel) | M1: Feuermelder / Löschanlagen | CHF 50’000 | Ja | 2 (Niedrig) | Ja (Datum) |
| B02 / B02 | 4 (Mittel) | M2: Elektronische Ablage Daten | CHF 100’000 | Ja | 1 (Niedrig) | Ja (Datum) |
| B01 | 4 (Mittel) | M3: Schaffung von Ausweichar­beitsplätzen | CHF 50’000 | Nein | 4 (Mittel) | … |
| B03 | 4 (Mittel) | M4: Temperaturüberwachung / Klimagerät | CHF 3000 | Ja | 1 (Niedrig) | Ja (Datum) |
| B04 | 4 (Mittel) | M5: Wassermelder | CHF 500 | Ja | 4 (Mittel) | Ja (Datum) |
| B10 | 6 (Hoch) | M6: Aufbau und Dokumentation Stellvertretung | Keine | Ja | 3 (Niedrig) | Ja (Datum) |
| B11 | 6 (Hoch) | M7: Redundante Stromanbindung oder Notstromaggregat | CHF 50’000 | Nein | 6 (Hoch) | … |
| B17 | 2 (Niedrig) | M8: Zeitnahe Datensicherung | CHF 1000 | Ja | 2 (Niedrig) | Ja (Datum) |
| B17 | 2 (Niedrig) | M9: Wiederherstellungstests | CHF 500 | Ja | 2 (Niedrig) | Ja (Datum) |
| u.a.m | u.a.m. | … | … | … | … | … |

# Prozess bei Notfällen

Für den Fall des Auftretens von Notfällen ist der folgende Prozess definiert, siehe auch Ziffer 6.



Abbildung 3: Notfallprozess

# Kommunikation und Öffentlichkeitsarbeit

Ein wichtiger Aspekt des Notfallkonzepts ist, wie bei einem Notfall kommuniziert wird, sowohl intern gegen­über den Mitarbeitenden als auch extern gegenüber Drittfirmen und -organisationen wie auch gegenüber der Öffentlichkeit. Eine falsche, fehlende oder zu spät erfolgte Kommunikation kann im Nachhinein beträcht­liche Reputationsschäden verursachen und offenbart in der Regel, dass die betreffende Organisation nicht entsprechend vorbereitet war.

Die Kommunikation richtet sich nach den verschiedenen Bedrohungsarten. Entsprechende Mitteilungen und der Empfängerkreis sind vorbereitet, so dass diese in einem Krisenfall schnell zur Verfügung stehen.

Analog zur folgenden Beispieltabelle wurde eine Kommunikationsmatrix erstellt, aus der ersichtlich ist, wel­che Stellen bei welchen Ereignissen und in welcher Periodizität informiert werden müssen. Die vollständige und konkret ausgefüllte Kommunikationsmatrix ist im Excel-Dokument [Vorlage Notfallkonzept Bedrohungs­analyse und Massnahmen](https://docs.datenschutz.ch/u/d/informationssicherheit/konzept/identisch/vorlage_notfallkonzept_bedrohungsanalyse.xlsx) aufgeführt. Sie kann aus der produktiven Version des Dokuments entfernt werden.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | Empfänger | | | | | | |
| Ereignisart | Ereignis Beschreibung | Polizei / Sanität / Feuerwehr | Mitarbeitende | Vorgesetzte Behörden | Übrige Behörden | Medien | Betroffene Personen | Weitere |
| Höhere Gewalt | Feuer, Ausfall Verwaltungsgebäude, krank­heitsbedingter Ausfall von vielen Mitarbei­tenden | E |  | T | E | M |  |  |
| Menschliche Fehlhandlung | Versehentliche Datenlöschung |  |  |  |  |  |  | E |
| Technisches Ver­sagen | Ausfall Stromzufuhr |  | E | T |  |  |  | E |
| Vorsätzliche Handlung | Ransomware-Angriff |  |  | T | W |  | E  T | E |
| Vorsätzliche Handlung | Physischer Angriff auf Mitarbeitenden | E | T | W |  | W | T |  |

Tabelle 5: Kommunikation

Legende:

* E = bei Ereignis
* T = innert Tagesfrist / allenfalls tägliches Update
* W = innert Wochenfrist / allenfalls wöchentliches Update
* M = innert Monatsfrist / allenfalls monatliches Update

# Notfallübungen und -tests

Um das Funktionieren des Betriebs bei einem Ausfall oder Notfall sicherzustellen, werden regelmässig ent­sprechende Tests und Übungen durchgeführt und dokumentiert (nachfolgend sind einige Musterbeispiele zur Veranschaulichung aufgeführt).

|  |  |  |  |
| --- | --- | --- | --- |
| Test / Übung | Datum | Resultat | Massnahmen |
| Test:  Ausfall Telefonie / Umschalten auf Mobiltelefone | 01.06.2021 | Gut, vereinzelt nicht ak­tuelle Nummern doku­mentiert | Mobilnummern aktuali­sieren |
| Übung:  Evakuation bei Feuer | 01.06.2021 | Befriedigend, nicht alle Mitarbeiter schnell genug evakuiert | Schulung verbessern |
| Test:  Wiederherstellung IT-Back-up | 01.06.2021 | Gut, alle Daten problem­los wiederhergestellt | Keine |

Tabelle 6: Notfallübungen

# Überprüfungsprozess

Das vorliegende Konzept wird periodisch überprüft und gegebenenfalls angepasst.

Im Zuge der Überprüfung werden die folgenden Faktoren auf ihre Aktualität und Richtigkeit hin beurteilt:

* Geschäftsprozesse
* Ressourcen
* Bedrohungsarten
* Auswirkungen
* Massnahmen
* Verantwortliche Personen und Kontaktdaten

# Genehmigung und Inkrafttreten

Beschlossen von [OBERSTES\_ORGAN\_S1\_S2] mit Beschluss [NR.] am [DATUM].

[ORT UND DATUM] [NAME]

[ORGAN\_S1\_S2] [OBERSTES\_ORGAN\_S1\_S2]

# Begriffsdefinition

|  |  |
| --- | --- |
| Begriff | Bedeutung |
| Auswirkung | Faktor zur Beurteilung, wie gross die Auswirkung bei Eintreten einer Be­drohung ist. |
| Auswirkungsanalyse | Dient dazu, die verschiedenen Auswirkungen bei einem Ausfall eines Ge­schäftsprozesses zu analysieren. |
| Bedrohungsanalyse | (englisch Business Impact Analysis BIA) Beurteilt den Einfluss der verschie­denen Bedrohungsarten auf die Geschäftsprozesse. |
| Bedrohungsart | Verschiedene Faktoren, welche eine Bedrohung für den Geschäftsbetrieb darstellen können. |
| Business Continuity Manage­ment (BCM) | Ganzheitlicher Managementprozess zur Fortführung der kritischen Ge­schäftsprozesse bei Eintritt eines Notfalls. |
| Eintrittswahrscheinlichkeit | Faktor zur Beurteilung, wie wahrscheinlich das Eintreten einer Bedrohung ist |
| Incident / Ereignis | Ereignis einer Störung oder eines Ausfalls. |
| Max. tolerierbare Ausfallzeit (MTA) | Definiert die maximale Dauer, während der ein Geschäftsprozess ausfal­len kann, ohne dass die Institution mittel- bis langfristig ernsthaft bedroht ist. |
| Max. Wiederanlaufzeit (WAZ) | Beschreibt die Zeitspanne von der Unterbrechung eines Prozesses bis zum Beginn des Notbetriebs. |
| Notfall | Ein Notfall ist ein Schadensereignis, bei dem Prozesse oder Ressourcen ei­ner Institution nicht wie vorgesehen funktionieren. Die Verfügbarkeit der entsprechenden Prozesse oder Ressourcen kann innerhalb einer geforder­ten Zeit nicht wiederhergestellt werden. Der Geschäftsbetrieb ist stark be­einträchtigt. Eventuell vorhandene SLAs (Service Level Agreements) kön­nen nicht eingehalten werden. |
| Notfallhandbuch | Das Notfallhandbuch beinhaltet alle Informationen, die während und für die Notfall- und Krisenbewältigung benötigt werden. Es umfasst somit alle Notfallpläne wie den Krisenkommunikationsplan, den Krisenstabsleitfa­den, die Wiederanlauf- und Wiederherstellungspläne. |
| Notfallmanagement | Das Notfallmanagement ist ein Managementprozess mit dem Ziel, gravie­rende Risiken für eine Verwaltungseinheit, die deren Überleben gefähr­den, frühzeitig zu erkennen und Massnahmen dagegen zu etablieren. |
| Notfallverantwortlicher | Der/die Notfallverantwortliche ist die allererste Person, die bei einem Notfall zu informieren ist. Er/sie entscheidet über das weitere Vorgehen und darüber, welche weiteren Personen in welcher Form zu informieren sind. |
| Notfallvorsorge | Die Notfallvorsorge beinhaltet alle bei der Konzeption des Notfallmanage­ment anfallenden Informationen, die nicht direkt für die Notfallbewälti­gung benötigt werden. Sie beinhaltet die Definition von präventiven Mas­snahmen. |
| Risikostufe | Ausmass der Auswirkungen, welche ein Risiko für den Betrieb darstellt. Wird noch in verschiedene Kategorien unterteilt. |
| Störung | Eine Störung ist eine Situation, in der Prozesse oder Ressourcen einer Ver­waltungseinheit nicht wie vorgesehen funktionieren. Die dadurch entste­henden Schäden sind als gering einzustufen. Ein «geringer» Schaden ist ein Schaden, welcher im Verhältnis zum Haushaltsvolumen einer Verwal­tungseinheit zu vernachlässigen ist oder die Aufgabenerfüllung nur unwe­sentlich beeinträchtigt. |

Tabelle 7: Begriffsdefinitionen

Anhang A: Notfallorganisation / Ansprechpersonen [ORGAN\_S1\_S2]

Nachfolgend sind die Kontaktangaben für die im Krisenfall benötigten Personen aufgeführt

|  |  |  |  |
| --- | --- | --- | --- |
| Mitarbeiter/in / Kontaktperson | Organisation | Verantwortlich für | Kontaktdaten |
| Gemeindeschreiber … | [ORGAN\_S1\_S2] | Gesamtleitung Krisenstab | 079 … |
| Leiter … | [ORGAN\_S1\_S2] | Gebäude | 079 … |
| Leiter … | [ORGAN\_S1\_S2] | Kommunikation | 079 … |
| Firma … (Hr. …) | IT-Dienstleister | Betrieb IT / Telefonie | 0800 …  079 … |
| Firma … (Hr. …) | Stromanbieter | Elektrizität | 0800 …  079 … |

Tabelle 8: Notfallorganisation / Ansprechperson

Anhang B: Wichtige Unterlagen, Passwörter u.a. [ORGAN\_S1\_S2]

Bei einem Ausfall oder Krisenfall sollten die wichtigsten Unterlagen (zum Beispiel Verträge, Anleitungen, Zeichnungen, Codes) sowie Passwörter und Zugangscodes (zum Beispiel Admin auf Server, Netzwerkkompo­nenten, Zutrittssysteme oder aber E-Banking) zugreifbar sein.

Nachfolgend sind die Angaben direkt aufgeführt oder ihr Aufbewahrungsort angegeben.

|  |  |  |  |
| --- | --- | --- | --- |
| Unterlagen / Dokument | Beschreibung | Ablageort | Zugriff durch |
| Admin-Passwort Telefonie | In verschlossenem Umschlag | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Admin-Passwort Server | In verschlossenem Umschlag | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Admin-Passwort Router | In verschlossenem Umschlag | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Zugangscodes E-Banking | Passwort (nur 1 Le­segerät vorhanden) | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Wartungsvertrag Fa. X | Kopie des Originals | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Ersatzschlüssel Gebäude … | - | Tresor Verwaltungsgebäude  Tresor Werkhof | Gemeindeschreiber/in /  Stellvertreter/in |
| Ersatzschlüssel Fahrzeug | Zweitschlüssel | Schlüsselkasten Werkhof | Gemeindeschreiber/in /  Leiter/in |

Tabelle 9: Wichtige Unterlagen

V 1.3 / August 2022