|  |  |
| --- | --- |
|  | Klassifizierung |

|  |
| --- |
|  |

P042-Hi03 - Notfallkonzept

<Projektname / Schutzobjektname>

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Klassifizierung | Nicht klassifiziert / INTERN / VERTRAULICH / GEHEIM |
| Status | in Arbeit / in Prüfung / genehmigt zur Nutzung |
| Projektnummer |  |
| Projektleiter (PL LB) |  |
| Version | Aus Template V3.1 |
| Datum |  |
| Auftraggeber |  |
| Autor/Autoren |  |

Änderungskontrolle

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

Verteiler

|  |  |  |
| --- | --- | --- |
| Funktion | Name  | Departement / Amt |
| ISBO |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Inhaltsverzeichnis

1 Generelle Anmerkungen 4

1.1 Beschreibung 4

1.2 Verantwortlichkeiten 5

1.2.1 Leistungsbezüger 5

1.2.2 Leistungserbringer 5

1.3 Zweck des Dokuments 5

1.4 Vorgehen 5

1.5 Übergeordnete BCM Dokumentation 6

1.6 Unterstützte Geschäftsprozesse 6

2 Notfallvorsorge 7

2.1 Allgemeines 7

2.2 Präventive Massnahmen 7

2.3 Durchführung von Notfallübungen 7

3 Notfallmassnahmen 7

3.1 Beschreibung des Schutzobjektes 7

3.2 Sofortmassnahmen 7

4 Anhang A: Hilfsmittel BCM 9

4.1 Geltungsbereich 9

4.2 Massnahmenempfehlungen zum BCM 9

4.3 Krisen-/Notfallmanagement 9

4.3.1 Strategische Ausrichtung des Notfallmanagements 9

4.3.2 Erläuterungen von Störungen, Notfällen, Krisen und Katastrophen 10

4.3.3 Notfallszenarien und Ansprechpartner 10

4.3.4 Lagebeurteilung 10

4.4 Kommunikation und Öffentlichkeitsarbeit im Krisenfall 11

4.4.1 Krisenstabsraum / Lagezentrum 11

5 Anhang B: Referenzen 12

5.1 Dokumentenverzeichnis 12

5.2 Begriffe 12

# Generelle Anmerkungen

**Hinweise zum Ausfüllen dieses Dokuments**

Als Hilfsmittel für die Ausgestaltung des Notfallkonzeptes können folgende Standards und Empfehlungen dienen:

* [BSI-Standard 100-4 Notfallmanagement](https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/BSI-Standard-100-4-Notfallmanagement/Umsetzungsrahmenwerk-zum-Notfallmanagement-nach-BSI-Standard-100-4/umsetzungsrahmenwerk-zum-notfallmanagement-nach-bsi-standard-100-4_node.html) (IT-Grundschutz-Standards)
* ISO/IEC-Standards 27001, 27002 und 27031
* [Empfehlungen für das Business Continuity Management (BCM)](https://www.swissbanking.ch/_Resources/Persistent/b/2/1/5/b215cf91b0f9b27c050de8ca12a3f61f1ecd3e1e/SBVg_Richtlinien_Empfehlungen_fu%CC%88r_das_Business_Continuity_Management_2013_DE.pdf) der Schweizerischen Bankiervereinigung, SwissBanking, von der FINMA als Mindeststandard anerkannte Selbstregulierung
* [Empfehlung Begriffserklärungen im Umfeld BCM / ITSCM auf Stufe Bund](https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/empfehlungen/Begriffserklaerungen_KaVor_v01-1.pdf.download.pdf/Begriffserklaerungen_KaVor_v01-1.pdf)

Der blaue Text dient als Hilfe zum Ausfüllen des Dokumentes.

## Beschreibung

Aus Anforderung O3 des IT-Grundschutzes (Si001) zum Thema «Geschäftskontinuität» lässt sich die Notwendigkeit eines Notfallkonzeptes ableiten.

Ausgangslage des Notfallkonzeptes ist das ISDS-Konzept. Das Notfallkonzept bezieht sich auf dasselbe Schutzobjekt wie im ISDS-Konzept beschrieben. Essentielle Grundlage für die Erstellung des Notfallkonzepts ist die im Rahmen des ISDS-Konzeptes erfolgte Risikoanalyse.

Die nachstehende Grafik verdeutlicht die Einordnung des Notfallkonzeptes in den Kontext des ISDS-Konzeptes sowie die Abgrenzung des Notfallkonzepts zu anderen Bereichen.



Abbildung : Einordnung des Notfallkonzepts

## Verantwortlichkeiten

### Leistungsbezüger

Der Leistungsbezüger (LB) ist für die Einhaltung der IKT-Vorgaben und der Beschlüsse des Bundesrates und der Departemente beziehungsweise der Bundeskanzlei in seinem Zuständigkeitsbereich verantwortlich.

Bezüglich des Notfallmanagements bedeutet dies insbesondere:

* Prüfung der SLAs mit den Leistungserbringern,
* Datenbackup, Datenwiederherstellbarkeit,
* Berechtigungs- und Zugriffsmanagement auf Daten.

### Leistungserbringer

Die internen Leistungserbringer (LE) sind für die Einhaltung der IKT-Vorgaben und der Beschlüsse des Bundesrates und der Departemente beziehungsweise der Bundeskanzlei in ihrem Zuständigkeitsbereich verantwortlich.

Bezüglich des Notfallmanagements bedeutet dies insbesondere:

* Notfallmanagement und Notfallsicherheit Rechenzentrum,
* Ersatz-Infrastruktur.

## Zweck des Dokuments

Das Notfallkonzept beschreibt die Notfallplanung und die Fortführung des Geschäftsbetriebes für das Schutzobjekt, um die Aufrechterhaltung und Wiederherstellung der Geschäftsfähigkeit in ausserordentlichen Situationen zu gewährleisten.

Das Notfallkonzept hat auch zum Ziel die Überprüfung der schon mit dem Leistungserbringer bestehenden SLAs und allenfalls die Nachführung notwendiger Ergänzungen.

## Vorgehen

Die nachstehende Grafik vermittelt die Vorgehensweise beim Erstellen des Notfallkonzeptes.

Dieses Vorgehen geht von der Voraussetzung aus, dass ein BCM auf Stufe Amt existiert und es regelmässig auf seine Aktualität hin überprüft (insb. bezüglich veränderten Verantwortlichkeiten/Kontaktdaten) und entsprechend ergänzt wird.



Abbildung : Vorgehen Erstellung Notfallkonzept

## Übergeordnete BCM Dokumentation

Die folgenden Dokumente wurden im Bereich BCM auf Stufe Amt erstellt:

|  |
| --- |
| BCM |
| Business lmpact Analyse (BIA) |  |
| BCM-Strategie |  |
| Business Continuity Plan (BCP) |  |
| … |  |

## Unterstützte Geschäftsprozesse

Folgende Geschäftsprozesse werden durch das Schutzobjekt unterstützt:

|  |  |  |
| --- | --- | --- |
| Kritisch (k) | Geschäftsprozess | Geschäftsprozessverantwortlicher (GPV) |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Notfallvorsorge

## Allgemeines

Die Notfallvorsorge bildet die Grundlage zur Umsetzung der Kontinuitätsstrategien. Sie beschreibt die vorliegenden Bedingungen und beinhaltet alle bei der Konzeption anfallenden

Informationen. Zu beschreiben sind alle präventiven organisatorischen und konzeptuellen Aspekte sowie alle Massnahmen und Tätigkeiten des Notfallmanagements.

## Präventive Massnahmen

In dieser Phase werden die individuell für das Schutzobjekt geeigneten und wirtschaftlich angemessenen Massnahmen identifiziert und/oder mit den existierenden Massnahmen der Leistungserbringer abgestimmt.

**Kontrollfragen:**

* Wurden die definierten Massnahmen im ISDS-Konzept oder Massnahmen, die bereits durch den Leistungserbringer erbracht werden, mit den geplanten Massnahmen abgestimmt/berücksichtigt?
* Existiert beim Leistungserbringer eine entsprechende Notfallvorsorge?
* Wurden die Anforderungen aus der Schuban berücksichtigt?
* Berücksichtigen sie diese in Ihren SLA?
* …

## Durchführung von Notfallübungen

Die Funktionsweise von Massnahmen und Notfallmanagement sollte entsprechend in Form von Notfallübungen geprüft werden. Nach einer Notfallübung ist der entsprechende Notfallprozess mit den involvierten Stellen zu beurteilen.

# Notfallmassnahmen

Dieses Kapitel ist so zu gestalten, dass ein sachverständiger Dritter in der Lage ist, die hier spezifizierten Notfallmassnahmen durchzuführen.

## Beschreibung des Schutzobjektes

Die Beschreibung erfolgt analog dem ISDS-Konzept.

**Kontrollfragen:**

* Existieren im vorliegenden Kontext weitere Schutzobjekte?
* …

## Sofortmassnahmen

Diese Massnahmen haben zum Ziel, ein schnelles und sinnvolles Reagieren auf einen Vorfall zu ermöglichen. Sie sind insbesondere mit jenen des ISDS-Konzepts abzustimmen.

**Kontrollfragen:**

* Sind Sofortmassnahmen definiert? Welche sind je Notfall anzuwenden?
* Sind konkrete Aufgaben für einzelne Personen/Rollen im Notfall definiert?
* Existieren Handlungsanweisungen für spezielle Notfälle?
* …

#  Anhang A: Hilfsmittel BCM

Wenn das BCM im Amt noch nicht geregelt ist, dienen folgenden Punkte als Hilfsmittel zu den BCM-Überlegungen.

## Geltungsbereich

Hier sind die Systemgrenzen aus dem ISDS-Konzept aus der Perspektive Notfallkonzept zu ergänzen.

**Kontrollfragen:**

* Welche Schnittstellen gibt es zu einem übergeordneten BCM?
* …

## Massnahmenempfehlungen zum BCM

Es sind entsprechende Massnahmenempfehlungen zu erarbeiten. Beispiele sind:

* Notfall-Definition, Notfall-Verantwortlicher
* Untersuchung interner und externer Ausweichmöglichkeiten
* Regelung der Verantwortung im Notfall
* Alarmierungsplan
* Notfall-Pläne für ausgewählte Schadensereignisse
* Erstellung eines Datensicherungsplans
* Ersatzbeschaffungsplan
* Abstimmung der Lieferantenvereinbarungen
* Durchführung von Notfallübungen
* Redundante Kommunikationsverbindungen
* …

## Krisen-/Notfallmanagement

Ziel des Notfallmanagements ist es, sicherzustellen, dass die Verwaltungseinheit ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen kann. Eine ganzheitliche Betrachtung ist daher unabdingbar. Es sind alle Aspekte zu betrachten, die zur Fortführung der kritischen Geschäftsprozesse bei Eintritt eines Schadensereignisses erforderlich sind.

### Strategische Ausrichtung des Notfallmanagements

Folgende strategische Ziele des Notfallmanagements sind vorgängig festzulegen:

**Kontrollfragen:**

* Welche Geschäftsziele sollen geschützt werden?
* Welche Schadensszenarien sind ausschlaggebend?
* Welche Arten von Geschäftsunterbrechungen werden als existenzbedrohend angesehen (bzw. Image-Schaden)?
* Höhe der Risikoakzeptanz?
* Art und Höhe der Massnahmen?
* Primäres Ziel der Notfallbehandlung?
* …

### Erläuterungen von Störungen, Notfällen, Krisen und Katastrophen

Klare Beschreibung der Begriffe Störung, Notfälle, Krisen oder Katastrophen. Diese sind sowohl mit den Verantwortlichen des Auftraggebers als auch den Leistungserbringern entsprechend abzustimmen.

### Notfallszenarien und Ansprechpartner

Für den Notfall kann eine andere Rollen-Verteilung gelten als im laufenden Betrieb vorgesehen bzw. im ISDS-Konzept festgehalten ist.

Bestimmen Sie entsprechende Benutzer/ Ansprechpartner je Eskalationsstufe.

|  |  |  |
| --- | --- | --- |
| Art des Sicherheitsvorfalls | Ansprechpartner | Kontaktdaten |
| Definition von Notfallszenarien |  |  |
| * Kleinere Störungen, die den Betrieb kurzzeitig betreffen (s. SLA)
* …
 | Service Desk 1st Level Support (Incident Management) | … |
| * Störungen, die den Betrieb für n-Stunden …
* …
 | Service Desk 2nd Level Support (Intervention) | … |
| * …
 | … | … |
| * …
 | … | … |

**Kontrollfragen:**

* Wurden entsprechende Notfallszenarien und Auslöser definiert?
* Ist definiert, welcher Ansprechpartner für welches Notfallszenario zuständig ist?
* Sind die entsprechenden Rollen, Zuständigkeiten und Kompetenzen definiert?
* Dokumentation der Meldewege und Eskalationsstufen?
* Stellvertretung geregelt?
* Bestimmung von Ansprechpartner?
* Ist der Eskalationsauslöser definiert?
* Ablauf (Prozess) und Prozessbeschreibung vorhanden und bekannt?
* Entscheidungshilfen bei der Eskalation vorhanden?
* Art und Weise, wie bei einer Eskalation vorzugehen ist, definiert?
* Sind die definierten Notfallszenarien und Auslösefaktoren mit dem/den Leistungserbringer/n abgestimmt?
* Sind die Service Level Agreements (SLAs) entsprechend darauf ausgelegt?
* …

### Lagebeurteilung

Hier soll geschildert werden wie eine entsprechende Ausnahmesituation/Lage beurteilt und eingestuft werden kann.

**Kontrollfragen:**

* Wurden entsprechende Entscheidungshilfen zur Lagebeurteilung erstellt?
* Wie erfolgt eine Analyse und Bewertung der Notfallbewältigung?
* Ist definiert, wie und in welcher Art und Weise eine entsprechende Dokumentation erfolgt?
* Sind entsprechende Deeskalationsschritte definiert?
* …

## Kommunikation und Öffentlichkeitsarbeit im Krisenfall

Hier soll beschrieben werden, wie im Krisenfall gegen Innen und Aussen kommuniziert wird.

**Kontrollfragen:**

* Wer darf gegen aussen kommunizieren?
* Sind Kommunikationskonserven vorhanden?
* …

### Krisenstabsraum / Lagezentrum

Im Notfall müssen Räumlichkeiten zur Verfügung stehen, die dem Krisenstab als Arbeitsumgebung dienen und für die besonderen Anforderungen bezüglich des Standortes und der Ausstattung gelten.

**Kontrollfragen:**

* Sind die Standorte dokumentiert und allen beteiligten Personen/Stellen bekannt?
* Ist deren Erreichbarkeit gegeben?
* Sind entsprechende Abläufe und Arbeiten definiert?
* …