|  |  |
| --- | --- |
|  | Classification |

|  |
| --- |
|  |

P042-Hi03 - Plan d’urgence

<Nom du projet / Nom de l’objet à protéger>

|  |
| --- |
|  |

|  |  |
| --- | --- |
| Classification | Non classifié / INTERNE, CONFIDENTIEL, SECRET |
| Statut | En cours d’élaboration, en cours de vérification, terminé/approuvé |
| Numéro du projet |  |
| Chef de projet (CP BP) |  |
| Version | Du Template V3.1 |
| Date |  |
| Mandant |  |
| Auteur(s) |  |

Suivi des modifications

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Description, remarque | Nom |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Distribution

|  |  |  |
| --- | --- | --- |
| Fonction | Nom | Département / Office |
| DSIO |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Table des matières

1 Remarques générales 4

1.1 Description 4

1.2 Responsabilités 5

1.2.1 Bénéficiaires de prestations 5

1.2.2 Fournisseurs de prestations 5

1.3 But du document 5

1.4 Marche à suivre 5

1.5 Documentation BCM de l’office 6

1.6 Processus d’affaires pris en charge 6

2 Préparation aux situations d’urgence 7

2.1 Généralités 7

2.2 Mesures préventives 7

2.3 Simulations de situations d’urgence 7

3 Mesures d’urgence 7

3.1 Description de l’objet à protéger 7

3.2 Mesures immédiates 8

4 Annexe A: moyens auxiliaires en matière de gestion de la continuité des affaires (BCM) 9

4.1 Champ d’application 9

4.2 Mesures recommandées en matière de gestion de la continuité des affaires (BCM) 9

4.3 Gestion des crises et des situations d’urgence 10

4.3.1 Orientation stratégique de la gestion des situations d’urgence 10

4.3.2 Terminologie : dérangement, urgence, crise ou catastrophe 10

4.3.3 Scénarios d’urgence et interlocuteurs 10

4.3.4 Analyse de la situation 11

4.4 Communication et relations publiques en cas de crise 11

4.4.1 Bureau de l’état-major de crise et centre de suivi de la situation 11

5 Annexe B: Références 12

5.1 Table des documents 12

5.2 Lexique 12

# Remarques générales

**Remarques sur la façon de remplir le document**

Vous pouvez vous référer aux normes et recommandations suivantes dans le cadre de l’élaboration du plan d’urgence:

* [BSI-Standard 100-4 Notfallmanagement](https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/Standard04/ITGStandard04_node.html) (norme de l’Office fédéral allemand de la sécurité des technologies de l’information [BSI] concernant la protection informatique de base)
* Normes ISO/CEI 27001,27002 e 27031
* [Recommandations en matière de Business Continuity Management (BCM)](http://www.swissbanking.org/library/richtlinien/empfehlungen-fuer-das-business-continuity-management-bcm-2013/recommandations-en-matiere-de-business-continuity-management-bcm/%40%40download/file/999925_f.pdf) de l’Association suisse des banquiers, SwissBanking, reconnues par la FINMA comme standard minimal d’autorégulation
* [Directives en matière de Business Continuity Management (BCM) au sein de l’administration fédérale](https://intranet.ncsc.admin.ch/dam/ncscintra/de/dokumente/empfehlungen/Begriffserklaerungen_KaVor_v01-1.pdf.download.pdf/Begriffserklaerungen_KaVor_v01-1.pdf).

Le texte en bleu sert d’aide pour remplir le document.

## Description

L'exigence O3 de la protection informatique de base (Si001) sur le thème de la "continuité de l’activité" permet de déduire la nécessité d'un concept d’urgence.

Le plan d’urgence repose sur le concept SIPD. Il se rapporte au même objet à protéger. En outre, l’analyse des risques menée dans le cadre du concept SIPD constitue une base essentielle pour l’élaboration du plan d’urgence.

La figure ci-dessous précise la place du plan d’urgence dans le contexte du concept SIPD, en le délimitant par rapport à d’autres domaines.



Figure 1: Place du plan d’urgence

## Responsabilités

### Bénéficiaires de prestations

Les bénéficiaires de prestations (BP) sont responsables du respect des directives informatiques et des décisions du Conseil fédéral, du DFF, de l’UPIC et des départements ou de la Chancellerie fédérale dans leurs domaines de compétences respectifs (art. 21, al. 2, OIAF).

Dans le contexte de la gestion des situations d’urgence, ils ont notamment les tâches suivantes :

* Examen des accords de niveau de service (Service Level Agreements, SLA) avec les fournisseurs de prestations
* Sauvegardes et solutions de récupération des données
* Gestion des autorisations et contrôle des accès aux données

### Fournisseurs de prestations

Les fournisseurs de prestations (FP) internes sont responsables du respect des directives informatiques et des décisions du Conseil fédéral, du DFF, de l’UPIC et des départements ou de la Chancellerie fédérale dans leurs domaines de compétences respectifs (art. 23, al. 2, OIAF).

D’où notamment les activités suivantes, qui relèvent de la gestion des situations d’urgence :

* Gestion des situations d’urgence et protection du centre de calcul contre les sinistres
* Remplacement de l’infrastructure.

## But du document

Le plan d’urgence décrit la planification des cas d’urgence et la poursuite des activités liées à l’objet à protéger afin de garantir le maintien et le rétablissement des activités dans les situations extraordinaires.

Le plan d’urgence doit également comporter un contrôle des accords de niveau de service (SLA) conclus avec le fournisseur de prestations et assurer leur mise à jour si des modifications s’avèrent nécessaires.

## Marche à suivre

La figure ci-dessous indique la marche à suivre pour créer un plan d’urgence. Cette marche à suivre s’applique uniquement aux offices qui disposent d’une BCM, vérifient régulièrement son degré d’actualité (notamment si les responsabilités ou les coordonnées ont changé) et la complètent en conséquence.



Figure 2: Marche à suivre pour créer un plan d’urgence

## Documentation BCM de l’office

Les documents suivants relevant de la BCM sont établis par l’office:

|  |
| --- |
| BCM |
| Analyse d’impact sur les activités (*Business lmpact Analyse*, BIA) |  |
| Stratégie de gestion de la continuité des affaires |  |
| Plan de continuité des opérations (*Business Continuity Plan*, BCP) |  |
| … |  |

## Processus d’affaires pris en charge

L’objet à protéger prend en charge les processus d’affaires suivants:

|  |  |  |
| --- | --- | --- |
| Critique (c) | Processus d’affaires | Responsable du processus d’affaires |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Préparation aux situations d’urgence

## Généralités

La préparation aux situations d’urgence est la base pour la mise en œuvre des stratégies de continuité. Elle décrit les conditions en place et donne les informations utiles pour agir. Tous les aspects organisationnels et conceptuels, avec les mesures et activités de gestion des situations d’urgence, devraient être exposés dans ce cadre.

## Mesures préventives

Cette phase consiste à identifier les mesures qui sont appropriées à l’objet à protéger et économiquement adéquates, et/ou à les coordonner avec les mesures déjà en place des fournisseurs de prestations.

**Questions de contrôle :**

* Les mesures définies dans le concept SIPD ou celles déjà appliquées par les fournisseurs de prestations sont-elles été coordonnées avec les mesures prévues, et en a-t-on dûment tenu compte ?
* Une préparation équivalente aux situations d’urgence existe-t-elle par exemple chez le fournisseur de prestations ?
* A-t-on pris en compte les exigences de l’analyse des besoins de protection ?
* Ces exigences sont-elle prises en compte dans les accord de niveau de service (SLA)?
* …

## Simulations de situations d’urgence

Le bon fonctionnement des mesures adoptées et de la gestion des situations d’urgence devrait être testé, lors de simulations de cas d’urgence. Après un tel exercice, il convient d’évaluer le processus correspondant avec les services impliqués.

# Mesures d’urgence

Ce chapitre est conçu de manière à ce qu’un spécialiste externe soit à même de mettre en œuvre les mesures d’urgence.

## Description de l’objet à protéger

La description sera analogue à celle du concept SIPD.

**Questions de contrôle :**

* Y a-t-il dans le même contexte d’autres objets à protéger ?
* …

## Mesures immédiates

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

**Questions de contrôle :**

* Des mesures immédiates sont-elles définies ? Lesquelles doivent être appliquées selon la situation d’urgence ?
* Les tâches concrètes incombant à des personnes ou rôles spécifiques en cas d’urgence sont-elles définies ?
* Existe-t-il des instructions concrètes pour des urgences particulières ?
* …

# Annexe A: moyens auxiliaires en matière de gestion de la continuité des affaires (BCM)

Si l’office n’a pas encore défini sa gestion de la continuité des affaires (BCM), les points suivants peuvent servir de support aux réflexions sur le sujet.

## Champ d’application

Il s’agit ici de compléter les limites fonctionnelles du concept SIPD, dans la perspective du plan d’urgence.

**Questions de contrôle :**

* Quelles sont les interfaces avec un processus plus général de BCM ?
* …

## Mesures recommandées en matière de gestion de la continuité des affaires (BCM)

Il convient de formuler des recommandations concrètes. Exemples :

* Définition des cas d’urgence, responsable des situations d’urgence
* Analyse des solutions internes ou externes de rechange
* Responsabilités en cas d’urgence
* Plan d’alarme
* Plans d’urgence pour certains événements dommageables
* Plan de sauvegarde des données
* Plan pour des acquisitions de remplacement
* Coordination des accords conclus avec les fournisseurs
* Simulations de cas d’urgence
* Liaisons redondantes
* …

## Gestion des crises et des situations d’urgence

La gestion des situations d’urgence vise à garantir que l’unité administrative puisse s’acquitter à temps de ses tâches principales dans les situations extraordinaires et nécessite donc une approche globale. Il faut prendre en compte tous les éléments nécessaires à la continuation des processus d’affaires critiques en cas de sinistre.

### Orientation stratégique de la gestion des situations d’urgence

Les objectifs stratégiques suivants en matière de gestion des situations d’urgence seront fixés d’avance :

**Questions de contrôle :**

* Quels objectifs concernant les affaires de l’unité administrative doivent être préservés ?
* Quels sont les scénarios susceptibles de provoquer des dommages déterminants ?
* Quels types d’interruption d’activité sont-ils assimilés à une menace existentielle (par ex. à cause d’un dégât d’image) ?
* Degré de tolérance au risque ?
* Nature et intensité des mesures à prendre ?
* But premier des interventions d’urgence ?
* …

### Terminologie : dérangement, urgence, crise ou catastrophe

Il convient de décrire clairement les notions de dérangement, d’urgence, de crise ou de catastrophe. Ces notions doivent être dûment harmonisées avec les responsables du mandant, ainsi qu’avec les fournisseurs de prestations.

### Scénarios d’urgence et interlocuteurs

En cas d’urgence, la répartition des rôles peut être différente de celle prévue pour l’exploitation courante ou définie dans le concept SIPD.

Précisez les utilisateurs ou les interlocuteurs par niveau de gravité (escalade).

|  |  |  |
| --- | --- | --- |
| Type d’incident de sécurité | Interlocuteur | Coordonnées |
| Définition de scénarios d’urgence |  |  |
| * Dérangements mineurs affectant brièvement l’exploitation (voir SLA)
* …
 | Service Deskassistance de 1er niveau (Gestion des incidents) | … |
| * Dérangements interrompant l’exploitation pendant n heures …
* …
 | Service Desk assistance de 2e niveau (intervention) | … |
| * …
 | … | … |
| * …
 | … | … |

**Questions de contrôle :**

* Les scénarios d’urgence ont-ils été définis, avec les éléments déclencheurs ?
* A-t-on déterminé l’interlocuteur compétent pour chaque scénario d’urgence ?
* Les rôles, attributions et compétences correspondants ont-ils été définis ?
* La documentation des voies de transmission de l’information par niveau d’escalade a-t-elle été établie ?
* Qui sont les suppléants ?
* Les interlocuteurs ont-ils été désignés ?
* L’élément déclencheur d’un processus d’escalade est-il défini ?
* La marche à suivre (description du processus) est-elle disponible et connue ?
* Des aides à la décision en matière d’escalade sont-elles disponibles ?
* La manière de procéder en cas d’escalade a-t-elle été définie ?
* Les scénarios d’urgence définis, avec leurs facteurs déclencheurs, ont-ils été coordonnés avec les fournisseurs de prestations ?
* Les accords de niveau de service ont-ils été formulés en conséquence ?
* …

### Analyse de la situation

Il s’agit d’indiquer ici la manière d’évaluer et de classer les situations d’urgence.

**Questions de contrôle :**

* Des aides à la décision pour une évaluation de la situation sont-elles été élaborées ?
* Comment la gestion des situations d’urgence est-elle ensuite analysée et évaluée ?
* La manière d’établir une telle documentation a-t-elle été précisée ?
* Les étapes d’une désescalade sont-elles définies ?
* …

## Communication et relations publiques en cas de crise

Il s’agit de décrire ici les modalités de la communication interne et avec l’extérieur en cas de crise.

**Questions de contrôle :**

* Qui est autorisé à communiquer avec l’extérieur ?
* L’information à communiquer le moment venu est-elle déjà prête ?
* …

### Bureau de l’état-major de crise et centre de suivi de la situation

En cas d’urgence, des locaux seront mis à disposition pour que l’état-major de crise puisse y travailler. Ils satisferont aux exigences spécifiques à l’emplacement et à l’équipement.

**Questions de contrôle :**

* Les sites sont-ils documentés et connus des personnes et des services concernés ?
* Leur accessibilité est-elle garantie ?
* Les processus et activités requis dans ce contexte sont-ils définis ?
* …

# Annexe B: Références

## Table des documents

Inventaire des lois, ordonnances, directives, règlements, spécifications techniques, etc. pertinents pour la gestion des situations d’urgence. La liste ci-dessous sera complétée par les documents propres au département et/ou à l’office.

|  |  |
| --- | --- |
| Type de document | Titre |
| Lois | Base légale du processus métier et/ou de l’application (à compléter par l’auteur) |
|  | [Loi fédérale sur la protection des données (LPD; RS *235.1*)](https://www.admin.ch/opc/fr/classified-compilation/19920153/index.html) |
| Ordonnances | [Ordonnance sur l’informatique dans l’administration fédérale (OIAF; RS *172.010.58*)](https://www.admin.ch/opc/fr/classified-compilation/20081009/index.html) |
|  | [Ordonnance relative à la loi fédérale sur la protection des données (OLPD; RS 235.11)](https://www.admin.ch/opc/fr/classified-compilation/19930159/index.html) |
| Directives | [Directives du Conseil fédéral concernant la sécurité informatique dans l’administration fédérale](https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/grundlagen/w002-weisungen_bundesrat_ikt-sicherheit_bundesverwaltung_wisb.html)  |
| Méthodes | [HERMES – La méthode suisse de gestion de projet](https://www.isb.admin.ch/isb/fr/home/themen/projektmanagement/hermes.html) |
| Documents internes |  |

## Lexique

Pour consulter la définition d’un concept, veuillez vous référer aux recommandations «Explication des termes du domaine BCM / ITSCM au niveau fédéral».