Plan de gestion des

Incidents

**Document : Historique**

**Historique des versions du document**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Dates** | **Modifié par** | **Articles modifiés (V +1)** |
| **xxx** | **xxx** | **xxx** | **xxx** |
| **…** |  |  |  |

**Historique des validations**

|  |  |  |
| --- | --- | --- |
| **Nom** | **Fonction** | **Date de la validation par le plus haut niveau de direction** |
| **xxx** | **xxx** | **xxx** |
| **…** |  |  |

Le présent document s’applique à compter du **[date].**

Ce document est conservé comme suit :

1. Sur papier, aux endroits suivants : **[Indiquer les lieux]**.
2. Sous forme numérique aux endroits suivants : **[localisation sur l’intranet, par exemple]**.

Le titulaire de ce document est **[fonction]**. Il vérifie au moins 1 fois par an si des mises à jour sont nécessaires.

Tables des matieres

[Chapitre I. Objectif du document 5](#_Toc57389711)

[Chapitre II. Liens entre les procédures 6](#_Toc57389712)

[Chapitre III. PLAN DE GESTION DES INCIDENTS 8](#_Toc57389713)

[3.1 Etape 1 Préparation 9](#_Toc57389714)

[3.1.1 : Placer un pilote dans l’avion 9](#_Toc57389715)

[3.1.2 : Connaissez vos risques 9](#_Toc57389716)

[3.1.3 : Mesures préventives (avant incident) 9](#_Toc57389717)

[3.2 Etape 2 Notification et Identification 10](#_Toc57389718)

[3.2.1 : Identifiez les activités concernées 10](#_Toc57389719)

[3.2.2 : Identifiez les priorités 13](#_Toc57389720)

[3.3 Etape 3 Activation et Traitement 14](#_Toc57389721)

[3.3.1 : Identifiez vos outils et moyens 14](#_Toc57389722)

[3.4 Etape 4 Eradication 15](#_Toc57389723)

[3.5 Etape 5 Désactivation 15](#_Toc57389724)

[3.6 Etape 6 Leçons acquises (Post Incident Review) 16](#_Toc57389725)

[Chapitre IV. Fiches de gestion des incidents 20](#_Toc57389726)

[Noms des fiches 20](#_Toc57389727)

[Structure des Fiches 20](#_Toc57389728)

[Etape 1 Préparation 20](#_Toc57389729)

[Etape 2 Notification et Identification 20](#_Toc57389730)

[Etape 3 Activation et Traitement 20](#_Toc57389731)

[Etape 4 Eradication 21](#_Toc57389732)

[Etape 5 Désactivation 21](#_Toc57389733)

[Etape 6 Leçons acquises 21](#_Toc57389734)

[Chapitre V. Annexes 22](#_Toc57389735)

[Annexe 1. Liste des contacts (Annuaire) 22](#_Toc57389736)

[A) CONTACTS INTERNES 22](#_Toc57389737)

[B) CONTACTS EXTERNES 22](#_Toc57389738)

Chapitre I.
Objectif du document

*“By failing to prepare, you are preparing to fail.”*

**Benjamin Franklin**

Une bonne préparation est essentielle afin de mieux gérer les incidents. Munissez-vous d’une politique de gestion des incidents !

**L’objectif principal** d’un plan de gestion des incidents est de préparer l’entreprise à gérer les incidents de manière à protéger les processus les plus importants même lors d’évènements soudains et imprévus.

Ce plan est le suivi logique de l’élaboration de votre Risk Assessment et de votre Risk Treatment. Si votre organisation n’a pas encore procédé à ces analyses, il est important de commencer par cette étape car il est difficile de savoir comment gérer un incident quand aucune identification, analyse et évaluation des risques n’a été réalisée et que les mesures de traitement des risques sont inconnues.

La gestion des incidents vous permet de protéger vos activités essentielles en activant le plan de continuité des activités de l’entreprise.

Le présent plan de gestion des incidents identifie certains incidents fréquents et la manière de les gérer pratiquement (voir Fiches). Il convient d’adapter ce plan pour tenir compte du contexte particulier de votre entreprise et de ses choix.

Il est en effet possible que votre entreprise soit soumise à certains risques particuliers (produits chimiques dangereux, inflammables, risques d’explosion, ... Le Code du bien-être au travail doit bien entendu être respecté et les analyses et recommandations fournies par le [SPF Emploi](https://emploi.belgique.be/fr/themes/bien-etre-au-travail) et par [BeSWIC](https://www.beswic.be/fr/politique-du-bien-etre/analyse-des-risques/strategie-danalyse-des-risques-sobane) (analyse de risques SOBANE,...) doivent être suivis.

La gestion des incidents doit être validée par le plus haut niveau de direction de l’entreprise.

Chapitre II.
Liens entre les procédures

Le schéma (voir ci-dessous) indique comment le plan de gestion des incidents s’intègre avec les autres procédures.

1. Pour disposer d’un plan de gestion des incidents efficace, cela suppose que vous avez rempli les templates Risk Assessment et Risk Treatment. Le niveau de risques et la probabilité d’un incident dépendent du Risk Treatment que vous aurez effectué. De même, la gestion d’un incident dépendra beaucoup des mesures préventives et curatives que vous aurez mises en place.
2. En construisant votre plan de gestion des incidents et votre Business Continuity Plan et, il est possible que vous deviez remettre à jour votre Risk Assessment (notamment par ce que vous envisagez de modifier les risques en acquérant de nouveaux outils ou en lançant de nouveaux projets).
3. Votre Risk Assessment et votre plan de continuité des activités présupposent également que vous vous renseigniez auprès de vos fournisseurs, que vous examiniez vos contrats voire que vous imposiez certains niveaux de service (Service Level Agreement SLA) ou certaines clauses auprès de vos fournisseurs.
4. La continuité des activités de l’entreprise a des liens étroits avec la gestion des incidents car vous devez vous assurer que même lors d’un incident vous pourrez continuer les activités (au moins essentielles) de l’entreprise. Le gestionnaire du plan de continuité des activités de l’entreprise transmet les informations nécessaires au gestionnaire du plan de gestion des incidents.
5. Vous pourriez notamment prendre connaissance d’un incident en cours par le biais de vos clients ou de vos fournisseurs.
6. La plupart des incidents n’impliquent pas forcément l’activation du plan de continuité des activités de l’entreprise simplement parce qu’il s’agit de petits incidents “habituels” qui n’ont pas d’impact réel sur les activités. Si un incident ayant un impact sur les activités survient, le gestionnaire des incidents avertit le gestionnaire du plan de continuité des activités qui active le plan de continuité des activités. Pendant l’incident, par le gestionnaire des incidents assure un reporting régulier auprès du gestionnaire du plan de continuité. Après l’incident, le gestionnaire des incidents transmet le “Post incident review” au gestionnaire du plan de continuité.
7. Si l’incident n’a pas d’impact sur la continuité des activités, le gestionnaire du plan de gestion des incidents peut avertir, si besoin, les clients et fournisseurs que l’entreprise rencontre un incident mineur.
8. Si l’incident a un impact sur la continuité des activités, le gestionnaire du plan de continuité des activités s’adresse, si besoin, aux clients et fournisseurs en fonction des éléments d’information qui lui sont transmis par les services fonctionnels ainsi que par le gestionnaire du plan de gestion des incidents.
9. Après un incident, le post incident review vous indiquera peut être qu’il faudrait modifier le risk assessment et le risk treatment
10. Après un incident, le post incident review vous indiquera peut être qu’il faudrait réviser les contrats auprès de vos fournisseurs

Après une gestion des incidents, il est possible que vous deviez revoir votre risk assessment et votre risk treatment ou que votre plan de continuité des activités de l’entreprise doive être amélioré. **Pour plus d’informations concernant les différentes procédures, consultez les templates mis à votre disposition.**

Pour que le plan élaboré fonctionne efficacement en cas d'incident, il est important que les procédures prévues soient **testées** de manière approfondie au préalable **et révisées régulièrement**. Au moins une fois par an, lors du lancement de gros projets et après chaque incident/crise ou catastrophe, pensez à réviser vos plans et à déterminer les "leçons apprises" afin de pouvoir améliorer les plans en fonction des besoins et de l'expérience de l'entreprise.

Toutes les personnes impliquées dans le plan de gestion des incidents doivent **connaître leur rôle** exact et disposer de la version la plus récente de ce plan. (Pensez à en conserver une version papier également).

**1. Risk Assessment & Risk Treatment**

**2. Business Continuity Plan**

**3. Plan de gestion des incidents**

**Fournisseurs
essentiels**

**Clients**

**B**

**A**

**B**

**C**

**D**

**E**

**E**

**F**

**H**

**G**

**G**

**I**

**H**

**J**

**A**

Chapitre III.
PLAN DE GESTION DES INCIDENTS

Le plan de gestion des incidents repose sur six étapes :

## 3.1 Etape 1 Préparation

Voir également Risk Assessment et Risk Treatment.

### 3.1.1 : Placer un pilote dans l’avion

**Qui peut dresser ce plan de gestion des incidents ?**

**Qui peut valider ce plan (direction) ?**

Dans les grandes structures, un groupe (idéalement pluridisciplinaire et inclusif) peut être constitué. Le groupe est chargé d’élaborer les procédures qui tiennent compte des travaux déjà réalisés dans le cadre du Risk Assessment. Celui qui préside ce groupe présente les projets de procédure à la direction pour validation. En cas d’incident, c’est également lui (ou son back up) qui devra organiser le reporting régulier auprès de la direction.

Dans les plus petites structures, il est possible qu’une seule et même personne soit désignée par la direction ou que la direction assume ce rôle elle-même. Dans ce cas, il est néanmoins conseillé de désigner un back up (une personne qui pourra le remplacer en cas d’absence, de maladie ou de départ). Qu'il s'agisse du leader d'une équipe ou d'une personne unique, le gestionnaire en charge du plan de gestion des incidents est l'Incident Manager.

Pensez à inclure votre service interne pour la prévention et la protection au travail (SIPPT) et votre Service Externe pour la Prévention et la Protection au Travail (SEPPT) si vous en disposez.

Assurez-vous de faire valider les procédures/le plan de gestion des incidents et d’organiser le reporting régulier auprès du gestionnaire du plan de continuité des activités et/ou de la direction le cas échéant.

### 3.1.2 : Connaissez vos risques

***Avez-vous réalisé un Risk Assessment ?***

***Avez-vous réalisé un Risk Treatment ?***

Pour que le plan de gestion des incidents puisse être efficace, l’entreprise doit avoir identifié, analysé et évalué ses risques. C’est l’objet du Risk Assessment (voir template). Il faut également que les mesures de traitement des risques soient connues, c’est l’objet du Risk Treatment (voir template).

### 3.1.3 : Mesures préventives (avant incident)

Il s’agit d’ indiquer tout ce que l’entreprise peut mettre en œuvre avant tout incident pour en limiter la fréquence ou l’impact. Il s’agit également d’indiquer si la mesure préventive est effectivement adoptée dans l’entreprise.

## 3.2 Etape 2 Notification et Identification

Il est essentiel de pouvoir détecter, identifier et qualifier/classer rapidement un incident afin d’en limiter l’impact sur la continuité des activités en activant la procédure adéquate. La personne qui reçoit la notification de l’incident qualifie l’incident sur base de critères prédéterminés.

Chaque employé doit signaler tout incident ou événement susceptible d’entraîner un incident, et ce dès que possible. Les clients et fournisseurs peuvent également signaler un incident.

Pensez à indiquer les moyens de signaler les incidents.

La personne qui reçoit les renseignements (p. ex. Helpdesk) doit les classer, par exemple de la manière suivante:

1. **Faible** – aucun incident ne s’est produit, mais l’événement lié à un système, à un processus ou à une organisation peut déclencher la survenance d’un incident dans un avenir proche ou ultérieur;
2. **Mineur** – incident qui n’a pas d’impact significatif sur la continuité des activités;
3. **Majeur** – incident qui peut avoir un impact significatif sur l’organisation, mais qui n’est pas encore considéré comme une crise;
4. **Crise** – incident qui peut avoir un impact significatif sur l’organisation et la continuité des activités.

### 3.2.1 : Identifiez les activités concernées

**Quelles sont les activités à préserver pour assurer la survie économique de l’entreprise?**

**Voir aussi Business Continuity plan (BCP)**

Pour vous aider à établir des priorités dans vos processus et activités, posez-vous les questions suivantes :

1. quelles sont les activités qui pourraient mettre en danger le personnel (ou les clients,...) ?
2. quelles sont les activités qui pourraient avoir un grave impact économique pour l’entreprise après quelques heures ? 24h ? 48h ? Une semaine ?

LISTE DES ACTIVITES ESSENTIELLES

| Activité essentielle 1 |
| --- |
| Liste des éléments nécessaires pour la continuité de l’activité essentielle |
| Personnel clef |
| Information ou données clefs |
| Service informatique (hardware, software) nécessaire |
| Bâtiments |
| Personnes externes de contact (ressources) |
| Interdépendance avec d’autres activités (si oui, lesquelles) |
| ... |

#### 3.3.1 Faible

Lorsque l’information concernant une faiblesse ou un événement est enregistrée, l’employé désigné analyse l’information, détermine si possible la cause et, au besoin, prend des mesures préventives et correctives.

#### 3.3.2 Mineur

Lorsque des incidents mineurs sont identifiés ou signalés, l’employé désigné doit:

1. Prendre des mesures pour endiguer l'incident;
2. Enregistrer l’incident suivant le processus applicable et évaluer la gravité en fonction des niveaux et seuils de service définis;
3. Analyser la cause de l'incident;
4. Prendre des mesures correctives pour éliminer la cause de l'incident (si possible, conformément au délai convenu pour la résolution);
5. Informer les intervenants touchés par l’incident ou impliqués dans l’incident de la résolution.

#### 3.3.3 Majeur

Lorsque des incidents majeurs sont identifiés ou signalés, l’employé désigné doit:

1. Prendre des mesures pour endiguer l'incident;
2. Évaluer la gravité en fonction des niveaux de service et des seuils définis. Un incident mineur peut être étendu à un incident majeur si le temps de résolution dépasse les niveaux de service convenus ou si l'impact continue d'augmenter;
3. Informer toutes les parties prenantes responsables de l’incident survenu dans leur zone de responsabilité et indiquer le délai de résolution prévu (Voir Business Continuity Plan);
4. Constituer l’équipe d’intervention appropriée en cas d’incident;
5. Surveiller l'état d'avancement de l'incident et informer de l'état d'avancement de la gestion de l'incident;
6. Analyser la cause de l'incident;
7. Prendre des mesures correctives pour éliminer la cause de l'incident;
8. Informer les intervenants touchés par l’incident ou impliqués dans l’incident de la résolution.
9. Si l'incident majeur n'est pas réglé dans les délais prévus, l'incident pourrait se transformer en situation de crise. Pensez à prévoir la procédure d'escalade auprès de la direction..

Si l’incident ne peut être résolu dans le délai prévu, le gestionnaire de plan de gestion des incidents avise immédiatement l’équipe de la continuité des activités (Business Continuity Team) afin d’évaluer si le plan de continuité des activités doit être activé.

| **Action** | **Fonction** | **Liens vers d’autres documents****Nom et référence** |
| --- | --- | --- |
| Informer périodiquement le gestionnaire de crise sur la situation et le temps de reprise prévu.  | Incident Manager vers le gestionnaire du Business Continuity Plan | Business Continuity Plan |
| Évaluer périodiquement le temps de retour prévu; Si cela dépasse le Recovery Time Objective fixé (RTO), l’incident doit remonter vers le gestionnaire du Business Continuity Plan. | Incident Manager vers les gestionnaire du Business Continuity Plan | Business Continuity Plan |
| … |  |  |

#### 3.3.4. Crise

En cas de crise, le gestionnaire du Business Continuity Plan organise toutes les réunions en impliquant directement la Direction.

**Enregistrement des incidents**

**Quelle que soit la qualification de l’incident et pendant toute la durée de celui-ci, il s’agit de conserver le journal des incidents.**

**La ou les personnes responsables de la gestion de l’incident doivent consigner toutes les mesures prises dans un registre des incidents.**

**Ce tableau ci-dessous pourrait être utilisé comme modèle pour le journal des incidents:**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Date** | **Type d’incident** | **Brève description de l’incident** | **Équipe en charge** | **Description détaillée (impact, durée, activités impactées, ressources allouées,...)** | **Description des actions prises** |
| **1** |  |  |  |  |  |  |
| **2** |  |  |  |  |  |  |
| **...** |  |  |  |  |  |  |

### 3.2.2 : Identifiez les priorités

En cas d’incident, il est possible que toutes les activités ne fonctionnement pas forcément à 100% et que cela puisse être acceptable.

**En cas d’interruption ou de dégradation de vos activités, quel est l’ordre de priorité des activités ?**

**Quels sont vos objectifs de temps ?**

**Voir également les Risk Assessment, Risk Treatment et plan de continuité des activités**

Vous avez défini vos activités prioritaires (Étape 1) ? Il s’agit maintenant d’identifier l’ordre dans lequel ces activités devraient reprendre (certains services sont interdépendants des autres) et d’identifier les objectifs de temps estimé en les comparant aux objectifs fixés (voir Risk Assessment et Business Continuity Plan) :

* Identifiez votre objectif de temps de recouvrement - Recovery Time Objective (RTO)

Il s’agit du temps maximum qu’il faut pour rétablir le fonctionnement de l’activité à la suite d’une interruption ou d’une (forte) dégradation du service.

* Identifiez votre objectif de point de récupération - Recovery Point Objective (RPO)

Il s’agit de la durée (l’âge) maximum des données qui doivent être récupérées pour que votre entreprise puisse reprendre ses activités essentielles. Vous ne serez peut-être pas capable de faire des recherches historiques sur les 12 derniers mois mais vous pourrez continuer à fonctionner même de manière réduite. Pour certaines entreprises, perdre ne serait-ce que quelques minutes de données peut être catastrophique, tandis que d’autres entreprises peuvent tolérer des périodes (beaucoup) plus longues.

* Identifiez votre objectif de cohérence en matière de résilience - Recovery Consistency Objective (RCO)

Il s’agit de s’assurer que les temps définis (RTO et RPO) en interne sont bien pris en compte dans les contrats avec les externes et particulièrement dans l’accord de niveau de service (SLA). Cela permet notamment de savoir en combien de temps le prestataire externe s’engage à pouvoir intervenir et quelle sanction peuvent s’appliquer à lui si le niveau de service attendu et défini n’est pas délivré.

En fonction des besoins de votre entreprise, r**enseignez-vous auprès :**

* d’un ou de plusieurs **opérateurs télécoms** qui pourront vous offrir une ou plusieurs lignes redondantes
* de votre/vos **fournisseurs de services informatiques** et notamment votre fournisseur de service en nuage (**cloud**) afin de déterminer comment vos données sont sauvegardées et ce à quoi votre fournisseur s’engage vis à vis de votre entreprise.
* de votre **fournisseur de services de paiement en ligne** qui peut offrir des solutions de redondance ou de résilience pour les **paiements**.

En fonction de ce qui précède, identifiez l’ordre dans lequel les actions doivent être entreprises afin d’assurer la continuité des activités essentielles. N’oubliez pas d’envisager l’interdépendance possible de certaines activités et de maintenir un dialogue constant avec le gestionnaire du plan de continuité des activités.

## 3.3 Etape 3 Activation et Traitement

L’objectif principal est de réduire aussi rapidement que possible l’impact de l’incident sur la continuité des activités de l’entreprise.

Les notifications des incidents (p.ex. sous la forme d’un ticket) peuvent être traités par une équipe, p.ex. un helpdesk. Le gestionnaire du plan de gestion des incidents (leader) supervise tous les tickets. Les actions suivantes doivent être exécutées pour faire face à un incident:

| **Action** | **Fonction** | **Liens vers d’autres documents****Nom et référence** |
| --- | --- | --- |
| Effectuer une analyse rapide de la situation sur la base des informations disponibles  | Opérateur Helpdesk |  |
| Déterminer les actions qui doivent être prises pour retrouver un niveau de fonctionnement minimal autorisé | Gestionnaire de l’équipe Helpdesk  |  |
| Faire remonter l’incident en fonction de sa criticité | Gestionnaire de l’équipe Helpdesk vers le gestionnaire du plan de gestion des incidents |  |
| Exécuter les actions à prendre | Gestionnaire du plan de gestion des incidents |  |
| … |  | Voir procédures Business Continuity Plan  |

### 3.3.1 : Identifiez vos outils et moyens

**De quoi et de qui avons-nous besoin pour faire en sorte que ces tâches soient accomplies ?**

**Voir Risk Assessment table (colonnes B et C)**

Pour chaque type d’incident, n’oubliez pas d’identifier :

1. Quelle est la chaîne de commandement ? (voir étape 1)
2. Quel est le scenario (ce qui est craint) et quels sont les types de risques (impact) ? (voir étape 2)
3. Quelles sont les mesures préventives que vous pourriez mettre en place ?
4. Quelles sont les mesures de gestion ?
5. Après un incident, quelles leçons pourriez-vous tirer de cet incident ?

 Tout au long de la gestion d’un incident, pensez également à identifier :

1. Sur qui pourriez-vous vous appuyer : personnes ressources en interne ? personnes ressources en externe ?
2. Quelles sont les procédures à respecter ?

Et concrètement, cela ressemble à quoi ? Pour vous aider, il vous est proposé des “fiches” (voir chapitre IV).

***“Un plan qui dort sur une étagère ne vaut pas le papier sur lequel il est imprimé”***

En effet, si le plan de gestion des incidents prend la poussière, il y a de fortes chances qu’en cas d’incident personne ne sache comment l’appliquer. **Une sensibilisation régulière est nécessaire.**

## 3.4 Etape 4 Eradication

Il n’est pas toujours possible de déterminer pendant l’incident les causes de celui-ci. Dans ce cas, il s‘agira d’abord d’agir sur les conséquences (impact sur la continuité des activités) avant de pouvoir en déterminer la cause. Toutefois, des efforts raisonnables doivent être déployés pour pouvoir identifier la cause et limiter les risques qu’un tel incident se reproduise à nouveau...

## 3.5 Etape 5 Désactivation

Lorsque les services touchés par un incident sont revenus à des opérations normales, l’incident peut être clos par l’équipe de gestion de l’incident (p.ex. helpdesk) en accord avec le gestionnaire du Business Continuity Plan.

Le plan de gestion des incidents est désactivé et un “Post Incident Review” est effectué (voir étape 6).

Les mesures suivantes devraient être prises:

| **Action** | **Fonction** | **Liens vers d’autres documents****Nom et référence** |
| --- | --- | --- |
| Fermer le ticket d’incident | Helpdesk après accord du gestionnaire du plan de gestion des incidents | Ticket dans le cadre de la gestion des incidents |
| Désactiver l’Plan de gestion des incidents | Gestionnaire du plan des incidents |  |
| Effectuer le Post incident Review | Gestionnaire du plan des incidents | Post-Incident Review (document) |
| … |  |  |

## 3.6 Etape 6 Leçons acquises (Post Incident Review)

*“I never lose. I either win or learn.”*

Nelson Mandela

Il s’agit d’apprendre de son expérience en réalisant un “post incident review” afin d’améliorer dans un processus continu la gestion des incidents.

Le Post Incident Review devrait comprendre au moins les éléments suivants ;

| **Élément** | **Information** |
| --- | --- |
| **Administration** |  |
| Numéro de l’incident dans le registre des incidents : |  |
| Date et heure de la détection de l’incident : |  |
| Date et heure de la résolution de l’incident : |  |
| Type d’incident : |  |
| Gravité de l’incident : |  |
| Les clients ont-ils été touchés : |  |
| Gestionnaire de l’incident : |  |
| Description de l’incident : |  |
| ... |  |

|  |  |
| --- | --- |
| **Détection** |  |
| Comment et par qui l’incident a-t-il été détecté : |  |
| L'incident a-t-il été détecté rapidement ou aurait-il pu l'être plus tôt : |  |
| Peut-on utiliser des procédures ou des outils pour détecter les incidents plus tôt : |  |
| Les procédures de notification des incidents ont-elles été suivies : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Evaluation et actions** |  |
| L'incident a-t-il été évalué correctement et correctement : |  |
| L’information appropriée était-elle disponible pour ce faire : |  |
| Le BCP a-t-il été activé : |  |
| Quelles autres mesures ont été prises pour résoudre l’incident : |  |
| Quelles ressources ont été utilisées pour gérer l’incident : |  |
| Le plan est-il suffisamment souple pour faire face à des événements imprévus : |  |
| Les mesures ont-elles été prises en temps opportun : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Communication** |  |
| Une communication interne a-t-elle été envoyée (en temps voulu) :  |  |
| La communication externe a-t-elle été envoyée (en temps voulu) : |  |
| Quels médias ont été utilisés : |  |
| Quand la première communication a-t-elle été envoyée et quelle fréquence de mise à jour a-t-elle été utilisée : |  |
| Les personnes concernées ont-elles été impliquées : |  |
| Quelles sont les communications utiles : |  |
| Quelles communications ont été employées et se sont révélées inefficaces : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Analyse des causes profondes** |  |
| La cause de l’incident a-t-elle été détectée : |  |
| Incidents liés ou de nature similaire : |  |
| Y a-t-il un problème sous-jacent : |  |
| Le problème sous-jacent a-t-il été détecté (voir étape 4 Eradication) : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Prévention**  |  |
| Que peut-on apprendre de ce qui s’est passé : |  |
| Comment éviter la répétition d’incidents, quelles mesures peuvent être prises pour le faire et qui est responsable de leur exécution :  |  |
| **…** |  |

|  |  |
| --- | --- |
| **Adéquation de la réponse** |  |
| Temps réel de récupération (comparez avec le Recovery Time Objective RTO) L’incident a été résolu dans le délai prédéterminé :Pour aucune des activitésSeulement pour quelques activitésPour toutes les activités |  |
| Faut-il réadapter les contrats : |  |
| … |  |

|  |  |
| --- | --- |
| **Pertinence de la réponse du management à l’incident**  |  |
| Le management n'a pas répondu ou n'a pas répondu de manière satisfaisante : |  |
| Le management a répondu, mais n’a pas suivi complètement les plans : |  |
| Le management a répondu pleinement conformément aux plans : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Niveau de préparation du personnel** |  |
| 1. Non préparé |  |
| 2. Partiellement préparé |  |
| 3. Entièrement préparé |  |

|  |  |
| --- | --- |
| **Améliorations souhaitées** |  |
| Quels éléments pourraient être ajustés : |  |
| … |  |

|  |  |
| --- | --- |
| **Dommages et intérêts** |  |
| Y a-t-il des demandes de dommages-intérêts : |  |
| Des demandes de dommages-intérêts ont été déposées auprès de tiers dans le cadre de cet incident : |  |
| **…** |  |

|  |  |
| --- | --- |
| **Divers** |  |
| ... |  |

Chapitre IV.
Fiches de gestion des incidents

## Noms des fiches

Incendie et Inondation

1. Fiche Inondation
2. Fiche Incendie

Informatique

1. Fiche Ransomware
2. Fiche Phishing
3. Fiche CEO Fraude

Energie et Telecom

1. Fiche Energie (Électricité)
2. Fiche Telecom

Communication

Quel que soit le type d’incident, prévoyez de pouvoir communiquer efficacement :

1. Fiche Communication

##  Structure des Fiches

Toutes les fiches proposées suivent une structure identique :

### Etape 1 Préparation

1. Scenario

Il s’agit d’expliquer ce qui est craint

1. Risques

Il s’agit d’indiquer brièvement le type de risques (atteinte à la réputation, destruction de matériel, mise en danger des personnes physiques,...)

1. Mesures préventives (avant incident)

Il s’agit d’ indiquer tout ce que l’entreprise peut mettre en œuvre *avant* tout incident pour en limiter la fréquence ou l’impact. Il s’agit également d’indiquer si la mesure préventive est effectivement adoptée dans l’entreprise.

### Etape 2 Notification et Identification

### Etape 3 Activation et Traitement

1. Mesures de gestion (INCIDENT)

Il s’agit d’indiquer que faire concrètement si le risque est avéré et que l’entreprise fait face à un incident.

### Etape 4 Eradication

### Etape 5 Désactivation

### Etape 6 Leçons acquises

1. Post Incident Review (après incident)

Il s’agit d’ expliquer ce qui a fonctionné et ce qui n’a pas fonctionné durant la gestion de l’incident et d’identifier les points d’action à entreprendre pour réduire la probabilité que le risqué survienne à nouveau ou pour limiter l’impact de l’incident sur l’entreprise (comment faire mieux la prochaine fois?)

Les annexes fournissent une liste des personnes ressources et établissent le lien avec les autres procédures et documents de référence.

Chapitre V.
Annexes

## Annexe 1. Liste des contacts (Annuaire)

### CONTACTS INTERNES

Dressez la liste de toutes les personnes de contact en interne en établissant si besoin la distinction entre les personnes ressources et les services fonctionnels qui pourraient être impactées par un incident.

N’oubliez pas d’indiquer les moyens de contacter la ligne de commandement (gestionnaire du plan de continuité, direction,....) directement et pensez aux vacances, maladies, départs etc. en envisageant plusieurs moyens de communication cumulatifs.

### CONTACTS EXTERNES

| **Fonction** | **Prénom, NOM ou nom de société** | **Référence des contrats** | **Informations** |
| --- | --- | --- | --- |
| **Assureur** |  |  |  |
| **Autorité de protection des données** |  |  | Apprenez à connaître le formulaire de notification de fuite de données et son mode d’emploi AVANT tout incident[Autorité de protection des données](https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles)  |
| **CERT** |  |  | Rue de la Loi 16 1000 BruxellesTel. +32 (0)2 501 05 60E-mail : info@cert.be  |
| **Délégué à la protection des données (DPO) (si externe...)** |  |  |  |
| **Électriciens capables d’intervenir rapidement (en prévoir au moins 2 différents)** |  |  | Numéro de compte1)2)Téléphone fixeBureau1)2) Maison1)2)Mobile1)2)Email 1)2)Liens avec les schémas du tableau électrique. |
| **Gestionnaire de distribution d’électricité** |  |  | Numéro de compteTéléphone fixeBureauMaisonMobileEmail  |
| **Opérateur télécom** |  |  | Numéro d’urgence (24/7)Numéro de compteEmail en cas d’incident : |
| **Prestataire cloud** |  |  | Téléphone fixeBureauMaisonMobileEmail  |
| **Prestataire IT n° xxx** (pensez à identifier tous vos prestataires et leurs rôles : réparation du matériel hardware, cyber sécurité, réseau, serveurs, webmaster....) |  |  | Téléphone fixeBureauMaisonMobileEmail  |
| **Propriétaire du bâtiment** |  |  | Numéro de compteTéléphone fixeBureauMaisonMobileEmail  |
| **SEPPT**Service Externe pour la Prévention et la Protection au travail |  |  |  |
| **...** |  |  |  |