Annexe 1 – Plan de réponse aux incidents

Commented [AES1]: Pour apprendre à remplir ce document et pour consulter des exemples concrets de ce que vous devez rédiger, regardez ce tutoriel vidéo : "How to Write a Business Continuity Plan According to ISO 22301".

Pour accéder au tutoriel : dans votre boîte de réception, consultez l'e-mail que vous avez reçu au moment de l'achat. Vous y trouverez un lien et un mot de passe qui vous permettront d'accéder au tutoriel vidéo.

Historique des modifications

Date	Version	Créé par	Description de la modification
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce Plan a pour but d'assurer la santé et la sécurité des personnes en cas de désastre ou autres incidents, et de contenir l'incident. L'objectif est de réduire les dommages causés à l'organisation à un niveau le plus faible possible.

Ce Plan est appliqué à tous les incidents majeurs qui menacent de perturber toute activité critique au sein du domaine d'application du SMCA pour une période plus longue que l'objectif de point de reprise pour chaque activité individuelle (plus loin dans le texte : incidents perturbateurs).

Les utilisateurs de ce document sont l'ensemble des employés de [nom de l'organisation].

Commented [AES2]: Indiquez le nom de votre organisation.

2. Autorisations et responsabilités dans la réponse aux incidents

Fonction dans la reprise / titre du poste	*Autorisations et responsabilités*
Tout employé	Aviser l'unité organisationnelle responsable de l'incident
[Titre du poste] ou équipe dans [nom de l'unité organisationnelle]	Toutes les mesures nécessaires pour activer les solutions pour résoudre les incidents liés aux technologies informatiques et de communication
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]
[illegible]	[illegible]

Commented [AES3]: Par ex. chef de service des technologies de l'information

Commented [AES4]: Par ex. agent des opérations

Commented [AES5]: Doit être la personne nommée dans le [illegible]

Commented [AES6]: Voir aussi : [illegible]

Commented [AES7]: Doit être la personne nommée dans le [illegible]

Commented [AES8]: Doit être nommé(e) par le DRH

3. Communication

Commented [AES9]: Cette section devrait être étendue avec [illegible]

Le tableau suivant indique les responsabilités pour la communication (envoyer aussi bien que recevoir des informations et répondre aux demandes d'informations) avec divers types de parties intéressées :

	[Téléphone]	*[Réunions]*	[illegible]	[illegible]	[illegible]		
[Employés]							
[Propriétaires / actionnaires]							
[illegible]							
[illegible]							
[illegible]							

Commented [AES10]: Copiez les responsabilités de la Stratégie + ajoutez quand cette communication a besoin d'être initiée (immédiatement après qu'un incident ne survienne / après qu'il ait été contenu / après qu'il ait été résolu, etc.)

[illegible]

[illegible]							
[illegible]							
[Services d'urgence]							
[diverses autorités d'Etat]							

La procédure de communication est la suivante :

1. Tout employé qui reçoit une demande de communication ou veut initier une communication vers les parties intéressées, doit transférer une telle demande à une personne responsable comme indiqué dans le tableau ci-dessus.
2. Une personne responsable doit être d'accord avec [titre du poste] sur le contenu de la communication. Quand c'est possible, des modèles de contenu de communication doivent être utilisés de manière à équilibrer le besoin d'informations des parties intéressées et la prévention des rumeurs et de la désinformation.
3. [illegible]
4. [illegible]

La personne responsable du tableau ci-dessus est responsable de documenter chaque communication avec les parties intéressées.

Commented [AES11]: Doit être la personne nommée dans le [illegible]

4. Procédures pour les incidents perturbateurs

Commented [AES12]: Inclure ici tous les incidents identifiés [illegible]

4.1. Gestion d'un incident perturbateur

4.1.1. Obligation de tous les employés de rapporter les incidents

Chaque employé est obligé de rapporter tout incident perturbateur de la manière suivante :

- tous les incidents liés aux technologies informatiques et de communication sont rapportés par téléphone à [titre du poste ou équipe de l'unité organisationnelle]
- [illegible]

Commented [AES13]: Si la nature de l'incident ne nécessite pas [illegible]

Commented [AES14]: Par ex. chef de service des technologies de l'information

Commented [AES15]: Par ex. agent des opérations

Tout autre évènement ou vulnérabilité du système qui n'a pas encore évolué en incident perturbateur, doit être rapporté de la même façon.

Commented [AES16]: Si cette question est déjà réglée par la [illegible]

Si un incident nécessite l'intervention de la Police, d'Ambulances ou de Services du feu, la première personne disponible doit appeler [numéro de téléphone] et en informer la personne responsable dans son unité organisationnelle ou le Gestionnaire de crise.

En cas d'incident, les employés peuvent communiquer librement seulement avec leurs famille et la Police, Ambulances ou Services du feu, tandis que toute autre communication est laissée à la charge de l'Equipe de gestion de crise.

4.1.2. Traitement des incidents perturbateurs

La personne qui reçoit des informations à propos d'un incident, doit évaluer si l'incident / l'incident potentiel est réel ou faux, et s'il est déterminé comme réel, immédiatement activer ce plan en prenant les mesures suivantes :

- commencer à contenir et éradiquer l'incident comme décrit dans les sections suivantes de ce document
- aviser toutes les personnes responsables de la survenue d'un incident au sein de leur zone de responsabilité
- [illegible]
- [illegible]

Commented [AES17]: Par ex. Responsable continuité d'activité, [illegible]

Dans le cas où une personne est incapable de contenir et / ou éradiquer l'incident, il / elle doit informer le Gestionnaire de crise. L'information qui est transmise au Gestionnaire de crise doit comprendre la nature et l'ampleur d'un incident perturbateur et son impact potentiel.

[illegible]

4.1.3. Gestionnaire de crise

Le Gestionnaire de crise doit surveiller l'avancement de la gestion de l'incident et la période de perturbation des activités individuelles, et évaluer le temps nécessaire pour résoudre l'incident.

[illegible]

4.2. Contenir et éradiquer un incident

Commented [AES18]: Ce chapitre ne fournit seulement que des [illegible]

4.2.1. Evacuation du bâtiment (quel que soit le type d'incident)

Le bâtiment est évacué vers les points de rassemblement spécifiés dans la Liste des sites de continuité des activités, annexée au Plan de continuité des activités.

Gestionnaire de crise	• Dans le cas où la vie ou la santé des personnes sont menacées, émettre un ordre d'évacuation • [illegible] • [illegible]

	[illegible]
Équipe responsable d'exécuter l'évacuation	• Evacuation directe vers le point de rassemblement • [illegible] • [illegible]
Tous les employés	• Evacuer conformément aux plans d'évacuation de votre bâtiment • Suivre les instructions fournies par les personnes responsables de diriger l'évacuation • [illegible] • [illegible] • [illegible]
Equipe support de gestion de crise	• Lorsque les personnes se sont rassemblées au point de rassemblement, tenir un registre des personnes présentes et absentes

4.2.2. Incendie

Le bâtiment est évacué selon le plan d'évacuation du bâtiment.

Gestionnaire de crise	• Dans le cas où la vie ou la santé des personnes sont menacées, le Gestionnaire de crise émet un ordre d'évacuation • [illegible]

4.2.3. Interruption de l'alimentation électrique

Equipe support de gestion de crise	• Etablir la cause de l'interruption - est-elle causée par le câblage ou par le distributeur d'électricité
[Titre du poste] ou équipe désignée	• Résoudre le problème avec le distributeur d'électricité
Tous les employés	• En ligne avec les plans de reprise, procéder à d'autres moyens d'exécution des activités, sans l'utilisation d'électricité
Employés dans le [nom du service des technologies de	• Surveiller les dispositifs UPS et exécuter l'arrêt du système d'information si nécessaire

Commented [AES19]: Par ex. analyste des installations, [illegible]

l'information]	

4.2.4. Tremblement de terre

Le bâtiment est évacué selon le plan d'évacuation du bâtiment.

Tous les employés	• Trouver un abri sous un cadre de porte, à proximité d'un mur porteur, ou sous un bureau • Ne pas utiliser les ascenseurs • [illegible] • [illegible] • [illegible]
Gestionnaire de crise	• Dans le cas où la vie ou la santé des gens sont menacées, ordonner l'évacuation du bâtiment lorsque le tremblement de terre est terminé
Equipe support de gestion de crise	• Arrêter tous les services publics - gaz, électricité, chauffage, ventilation, alimentation d'eau • [illegible]

4.2.5. Lettre de menace

Tous les employés	• Si vous recevez une lettre suspecte, ne l'ouvrez pas, tenez-la uniquement par les bords extérieurs • Mettez-la dans une enveloppe vide • [illegible] • [illegible]
[Titre du poste] ou équipe désignée	• Avertir la Police sur le [numéro de téléphone] • [illegible] • [illegible]

Commented [AES20]: Par ex. agent de sécurité

Commented [AES21]: Par ex. agent de sécurité

Commented [AES22]: Par ex. agent de sécurité

4.2.6. Appel de menace / menace de bombe

Tous les employés	• Si vous recevez un appel de menace, notez l'heure exacte et le numéro de l'appelant • [illegible] • Permettez à l'appelant de dire autant que possible, sans interruption : - essayer de le / la faire parler - répéter vos questions, dire que vous ne comprenez pas ce qu'il voulait dire - [illegible] - [illegible]

	• Dans le cas d'une menace de bombe, demandez à l'appelant les questions suivantes : - Est-ce que la bombe va exploser ? Quand ? - Peut-elle être désactivée ? Comment ? - Ou est-elle située ? - [illegible] - [illegible] - [illegible] • Les portes des bureaux ouvertes, si vous être sûrs qu'elles ne sont pas raccordées à la bombe • Ne pas rechercher la bombe dans le bâtiment ! Cela est le travail de la Police • [illegible] • [illegible]
Gestionnaire de crise	• Avertir la personne responsable dans l'unité organisationnelle ciblée par la menace • Ne pas utiliser les points de rassemblement standards - choisir un nouveau point de rassemblement • [illegible] • [illegible] • [illegible]

4.2.7. Défaillance des télécommunications

Employé dans le [nom du service]	• Tout employé qui reçoit des informations à propos de la défaillance • [illegible]
Employés - utilisateurs de services de communication	• Utiliser d'autres moyens de communication

Commented [AES23]: Ces responsabilités relèvent du service [illegible]

4.2.8. Défaillance du système d'information

Employé dans le [nom du service]	• Tout employé qui reçoit des informations à propos de l'incident • [illegible] • [illegible]
Gestionnaire de crise	• Consultation avec tous les services concernés, évaluation de la sévérité de l'incident

Commented [AES24]: Ces responsabilités relèvent du service [illegible]

Tous les employés	• Si possible, procéder à d'autres façons de mener des activités

4.2.9. Attaque malveillante du code

Employés dans le [nom du service]	• Tout employé qui reçoit des informations à propos de l'incident • Si vous traitez avec un type inconnu de code malveillant, [nom du responsable dans l'organisation de la sécurité de l'information] doit être averti • Avertir le producteur de logiciels antivirus • [illegible]
Tous les employés	• Déconnecter physiquement tout ordinateur infecter du réseau ; désactiver les réseaux sans fil, Bluetooth, etc. • [illegible]
Employé dans le [nom du service]	• Si l'ordinateur n'est toujours pas déconnecté du réseau, évaluer si le fait de le déconnecter peut prévenir de nouvelles infections • Désactiver toutes les connexions sans fil sur l'ordinateur • [illegible]

Commented [AES25]: Ces responsabilités relèvent du service [illegible]

Commented [AES26]: Ces responsabilités relèvent du service [illegible]

Commented [AES27]: Ces responsabilités relèvent du service [illegible]

4.2.10. Violation des règles internes et externes

[Titre du poste]	• La procédure est réalisée telle que requise par les lois sur le travail régissant les procédures disciplinaires et les propres procédures disciplinaires de l'organisation

5. Gestion des enregistrements conservés sur la base de ce document

Nom de l'enregistrement	*Lieu de conservation*	[illegible]	[illegible]	*Temps de rétention*
Journal des incidents	Dossiers partagés sur intranet	[illegible]	[illegible]	3 ans

Commented [AES28]: Dans cette colonne, indiquez les données [illegible]

Commented [AES29]: Par ex. Responsable des incidents, [illegible]

Commented [AES30]: Par ex. Responsable des incidents, agent de sécurité, etc.

Seul [titre du poste] peut accorder l'accès aux enregistrements à d'autres employés.

6. Validité et gestion documentaire

Ce document est valide à compter du [date].

Ce document, ainsi que tous les matériaux supplémentaires, sont conservés de la manière suivante :

- la forme papier du document est conservée dans les endroits suivants : Centre de commandement, et tous les autres sites pour les activités
- [illegible]

[illegible]

Lors de l'évaluation de l'efficacité et de la pertinence de ce document, les critères suivants doivent être considérés :

- le nombre d'incidents non-couverts par ce document
- [illegible]

[titre du poste]
[nom]

[signature]

Commented [AES31]: Conservez les documents de façon à [illegible]

Commented [AES32]: Il ne s'agit que d'une recommandation ; [illegible]

Commented [AES33]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.