[Logo de l'organisation]

[Nom de l'organisation]

Commented [AES1]: Remplissez tous les champs entre crochets [ ] dans ce document.

PROCEDURE DE GESTION DES INCIDENTS

Commented [AES2]: Pour en savoir plus sur ce sujet, consultez cet article :

How to handle incidents according to ISO 27001
https://advisera.com/27001academy/blog/2015/10/26/how-to-handle-incidents-according-to-iso-27001-a-16/

Code :	
Version :	
Date de la version :	
Créé par :	
Approuvée par :	
Niveau de confidentialité :	

Commented [AES3]: Le système de codage des documents doit être aligné avec le système existant de l'organisation pour la codification des documents ; au cas où un tel système n'est pas en place, cette ligne peut être supprimée.

Historique des modifications

Date	Version	Créé par	Description des modifications
	0.1	Advisera	Structure documentaire de base

Table des matières

1. But, domaine d'application et utilisateurs

Ce document a pour but d'assurer la détection rapide des évènements et des failles de sécurité, ainsi qu'une réaction et une réponse rapide aux incidents de sécurité.

Ce document s'applique à l'ensemble du domaine d'application du Système de management de la sécurité de l'information (SMSI), c'est-à-dire à tous les employés et à d'autres actifs utilisés dans le domaine d'application du SMSI, ainsi qu'aux fournisseurs et à d'autres personnes extérieures à l'organisation qui sont en contact avec les systèmes et les informations au sein du domaine d'application du SMSI.

Les utilisateurs de ce document sont l'ensemble des employés de [nom de l'organisation], ainsi que toutes les personnes mentionnées ci-dessus.

Commented [AES4]: Indiquez le nom de votre organisation.

2. Documents référencés

- Norme ISO/IEC 27001, clauses 7.4, A.5.7, A.5.24, A.5.25, A.5.26, A.5.27, A.5.28, A.6.4 et A.6.8
- Politique de sécurité de l'information
- [Liste des exigences légales, réglementaires, contractuelles et autres]

Commented [AES5]: Vous pouvez consulter un modèle pour ce document dans le dossier "05_Politiques_generales" de la Boîte à outils ISO 27001 et ISO 22301 Premium.

Commented [AES6]: Si vous ne disposez pas de cette Liste, alors énumérez ici les lois et contrats qui définissent les exigences relatives à la gestion des incidents.

3. Gestion des incidents

Un incident de sécurité de l'information désigne "un ou plusieurs évènements indésirables ou inattendus en matière de sécurité de l'information présentant une forte probabilité de compromettre les opérations commerciales et de menacer la sécurité de l'information" (ISO/IEC 27000 :2018).

3.1. Réception et classification des incidents, failles et évènements

Chaque employé, fournisseur ou autre tiers, qui est en contact avec les informations, les systèmes ou les secteurs sensibles de [nom de l'organisation], doivent signaler toute menace, faille du système, tout incident ou évènement, qui pourrait conduire à un incident, de la façon suivante :

Commented [AES7]: Indiquez le nom de votre organisation.

1. tous les évènements relatifs aux technologies de l'information et de la communication doivent être signalés à [titre du poste]
2. [illegible]

Commented [AES8]: Indiquez le titre du poste de la personne

Commented [AES9]: Indiquez le titre du poste de la personne

[illegible]

Commented [AES10]: D'autres systèmes de signalement [illegible]

La personne qui reçoit les informations doit les classifier de la façon suivante :

a) menace, faille ou évènement de sécurité – aucun incident n'a eu lieu, mais l'évènement relatif à un système, à un processus ou à l'organisation peut déclencher la survenance d'un incident dans un avenir proche ou lointain

b) incident mineur – un incident qui ne peut pas impacter significativement la confidentialité ou l'intégrité des informations ni causer une indisponibilité à long terme
c) incident majeur – un incident qui peut produire des dommages significatifs suite à la perte de confidentialité ou d'intégrité des informations, ou peut causer une interruption de la disponibilité des informations et / ou des processus pendant une durée inacceptable

3.2. Processus de traitement des failles ou des évènements de sécurité

La personne qui reçoit les informations concernant une menace, une faille ou un évènement de sécurité analyse les informations, établit la cause et, si nécessaire, suggère des actions préventives et correctives.

3.3. Traitement des incidents mineurs

Si un incident mineur est signalé, la personne qui reçoit les informations doit suivre les étapes suivantes :

1. prendre des mesures pour contenir l'incident
2. analyser les causes de l'incident
3. prendre des mesures correctives pour éliminer les causes de l'incident
4. informer les personnes qui ont été impliquées dans l'incident, ainsi que [titre du poste], concernant le processus de traitement de l'incident

La personne qui a reçu des informations relatives à un incident mineur doit enregistrer l'incident [décrire la méthode d'enregistrement].

Commented [AES11]: Par ex. manuel, électronique ou

3.4. Traitement des incidents majeurs

En cas d'incidents majeurs, qui pourraient perturber les activités pendant une durée inacceptable, le [Plan de reprise en cas de désastre] est appliqué.

3.5. Leçons tirées des incidents

Commented [AES12]: Supprimer cette section si la mesure

[Titre du poste] doit examiner, tous les trois mois, l'ensemble des incidents mineurs et inscrire tous les incidents récurrents, ou ceux qui pourraient se transformer en incidents majeurs à la prochaine occasion, dans le Journal des incidents.

[Titre du poste] doit analyser chaque incident enregistré dans le Journal des incidents (identifier le type, la gravité et le coût de l'incident) et, si nécessaire, suggérer des actions préventives ou correctives.

3.6. Sanctions disciplinaires

Commented [AES13]: Supprimer cette section si la mesure

[Titre du poste] doit engager une procédure disciplinaire pour chaque violation des règles de sécurité.

3.7. Collecte de preuves

Commented [AES14]: Supprimer cette section si la mesure

[Titre du poste] définira les règles concernant la manière d'identifier, de collecter et de préserver les éléments qui auront valeur de preuve dans les procédures judiciaires et autres.

4. 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	Fichiers partagés sur Intranet	[illegible]	[illegible]	3 ans

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

5. Validité et gestion documentaire

Ce document est valide à compter du [date].

[illegible]

Commented [AES15]: Il ne s'agit que d'une recommandation ; [illegible]

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

- le nombre de failles ou d'incidents qui n'ont pas été signalés aux personnes autorisées
- le nombre d'incidents qui n'ont pas été traités de la manière la plus appropriée
- [illegible]
- [illegible]
- [illegible]

6. Annexes

- Annexe 1 – Journal des incidents

[titre du poste]
[nom]

[signature]

Commented [AES16]: Nécessaire uniquement si la Procédure pour le contrôle des documents et des enregistrements prescrit que les documents papier doivent être signés.