Procédure de gestion des incidents

Exemple SAS — 50 salariés — Lyon | April 2026

PROCÉDURE DE GESTION DES INCIDENTS DE CYBERSÉCURITÉ

Exemple SAS
Version 1.0 - Date : [Date]
Responsable : RSSI

1. OBJET DE LA PROCÉDURE

Cette procédure définit les modalités de détection, qualification, confinement et résolution des incidents de cybersécurité au sein d'Exemple SAS. Elle vise à assurer une réponse rapide et coordonnée face aux menaces informatiques afin de minimiser leur impact sur l'activité de l'entreprise. Elle s'applique à l'ensemble des collaborateurs et des systèmes d'information de la société.

2. DÉCLENCHEMENT - QU'EST-CE QU'UN INCIDENT DE SÉCURITÉ ?

Un incident de cybersécurité est un événement qui compromet ou menace la confidentialité, l'intégrité ou la disponibilité des systèmes d'information et des données de l'entreprise.
Il peut résulter d'une action malveillante, d'une défaillance technique ou d'une erreur humaine. Tout événement suspect ou anormal doit être considéré comme un incident potentiel jusqu'à preuve du contraire. La détection précoce est essentielle pour limiter les conséquences.

Exemples d'incidents :
- Intrusion détectée sur le réseau informatique ou compromission de comptes utilisateurs
- Logiciel malveillant (virus, ransomware) identifié sur les postes de travail ou serveurs
- Tentative d'hameçonnage (phishing) ciblant les collaborateurs ou vol de données
- Panne système suspecte ou déni de service affectant les services critiques

3. ÉTAPE 1 - DÉTECTION ET SIGNALEMENT

3.1. Qui peut signaler un incident

Tout collaborateur d'Exemple SAS peut et doit signaler un incident de cybersécurité suspecté. Les équipes techniques (informatique, réseau) ainsi que les utilisateurs finaux sont encouragés à remonter immédiatement toute anomalie constatée.

3.2. Canal de signalement

Email : incidents-securite@exemple-sas.fr
Téléphone : 04 XX XX XX XX (ligne dédiée RSSI)
En cas d'urgence critique (P1), privilégier le contact téléphonique.

3.3. Informations à fournir

- Date et heure de détection de l'incident
- Description détaillée des symptômes observés
- Systèmes ou utilisateurs concernés
- Actions déjà entreprises le cas échéant
- Coordonnées du déclarant pour contact de suivi

4. ÉTAPE 2 - QUALIFICATION ET CLASSIFICATION

4.1. Niveaux de gravité

APERÇU — NON CONTRACTUEL

Contenu réservé aux abonnés

Ce document complet inclut 9 sections supplémentaires :

- Étape 4 — Éradication
- Étape 5 — Récupération
- Étape 6 — Notification ANSSI (NIS2, 72h)
- Étape 7 — Communication de crise
- Étape 8 — Retour d'expérience (post-mortem)
- Formulaire de déclaration d'incident
- Matrice d'escalade et contacts d'urgence
- Fiches réflexes par type d'incident
- Template notification ANSSI (24h/72h)

Débloquer avec le plan Pro — 89€/mois

Accédez à kyrionn.com pour débloquer