PLAN DE RÉPONSE À INCIDENT

Procédure de gestion des incidents de sécurité informatique — Fiche réflexe opérationnelle

FICHE RÉFLEXE
GARDER ACCESSIBLE

EN CAS D'INCIDENT GRAVE : ISOLER D'ABORD (déconnecter du réseau) — ALERTER ENSUITE — NE PAS ÉTEINDRE LES MACHINES (préservation des preuves numériques)

PROCESSUS DE RÉPONSE À INCIDENT — 6 ÉTAPES

ÉTAPE 01
DÉTECTION
H+0

- Alerte SIEM / antivirus
- Signalement utilisateur
- Comportement anormal
- Surveillance logs

ÉTAPE 02
QUALIFICATION
H+1

- Confirmer l'incident
- Évaluer la sévérité
- Identifier le périmètre
- Activer la cellule crise

ÉTAPE 03
CONFINEMENT
H+2

- Isoler les systèmes
- Bloquer les accès
- Couper réseau si nécessaire
- Préserver les preuves

ÉTAPE 04
ÉRADICATION
H+4 – H+24

- Cause racine identifiée
- Supprimer le vecteur
- Patcher les failles
- Scan complet des systèmes

ÉTAPE 05
RESTAURATION
J+1 – J+3

- Restaurer depuis backup sain
- Réinitialiser les accès
- Tests de validation
- Surveillance renforcée

ÉTAPE 06
RETEX
J+7

- Rapport post-incident
- Leçons apprises
- Mise à jour procédures
- Sensibilisation équipes

CONTACTS D'URGENCE INTERNES

RÔLE	NOM	TÉLÉPHONE / EMAIL
RSSI	*[Nom RSSI]*	*[N° RSSI]*
DPO	*[Nom DPO]*	*[N° DPO]*
Direction générale	*[Nom DG]*	*[N° DG]*
IT / Administrateur	*[Nom IT]*	*[N° IT]*
Prestataire cyber	*[Société]*	*[N° urgence 24/7]*
Assurance cyber	*[Assureur]*	*[N° sinistre]*
Juridique / DRH	*[Nom]*	*[N°]*

CONTACTS D'URGENCE EXTERNES — ORGANISMES OFFICIELS

ORGANISME	QUAND CONTACTER	CONTACT
ANSSI / CERT-FR	Incidents majeurs, attaque étatique	**cert.ssi.gouv.fr**
CNIL	Violation de données personnelles	**notifications.cnil.fr**
Police / Gendarmerie	Escroquerie, menace, extorsion	**17 — cyberplainte.fr**
Cybermalveillance.gouv	Assistance, trouver un prestataire	**cybermalveillance.gouv.fr**
InterCERT France	Échanges entre CSIRT	**intercert.fr**

OBLIGATIONS DE NOTIFICATION LÉGALE

CNIL
Violation de données personnelles (RGPD Art. 33)
72h max

ANSSI
Opérateurs essentiels (NIS2 Art. 23)
24h (alerte précoce)

ASSURANCE
Déclaration sinistre cyber selon contrat
Selon contrat

VICTIMES
Notification des personnes concernées (RGPD Art. 34)
Sans délai injustifié

MATRICE DE SÉVÉRITÉ DES INCIDENTS

NIV.	DESCRIPTION	DÉLAI RÉPONSE	ESCALADE
CRITIQUE 1	Ransomware actif, fuite massive, SI arrêté	**15 min**	Direction + ANSSI + Assurance
ÉLEVÉ 2	Intrusion confirmée, vol de données, DoS	**1h**	RSSI + DPO + Direction
MODÉRÉ 3	Malware isolé, tentative phishing réussie	**4h**	RSSI + IT
FAIBLE 4	Alerte bloquée, tentative échouée	48h	IT uniquement

CHECKLIST — PREMIÈRES 60 MINUTES

- ☐ Documenter l'heure exacte de détection et de prise en charge
- ☐ Identifier les systèmes / données affectés
- ☐ Qualifier la sévérité (matrice ci-dessus)
- ☐ Alerter le RSSI et la direction selon le niveau
- ☐ ISOLER les systèmes compromis du réseau
- ☐ NE PAS éteindre les machines (préserver les preuves)
- ☐ Capturer logs, screenshots, preuves numériques
- ☐ Ouvrir un ticket dans le registre des incidents
- ☐ Évaluer si données personnelles sont concernées (CNIL)
- ☐ Évaluer si obligations NIS2 s'appliquent (ANSSI)
- ☐ Activer le PCA si l'activité est interrompue
- ☐ Contacter le prestataire cyber si nécessaire
- ☐ Informer les équipes selon plan de communication interne

TYPES D'INCIDENTS COURANTS — RÉFLEXES

TYPE	ACTION IMMÉDIATE
Ransomware	Couper le réseau, ne pas payer, ANSSI + assurance
Phishing réussi	Changer MDP, activer MFA, analyser la messagerie
Fuite de données	Identifier les données, notifier CNIL dans 72h
Accès non autorisé	Révoquer les accès, auditer les logs
DDoS	Contacter hébergeur, activer protection anti-DDoS
Perte / vol matériel	Effacement distant, changer mots de passe

Besoin d'un accompagnement pour construire votre plan de réponse à incident ?
ayinedjimi-consultants.fr/contact