DOCUMENT 05

Fiche réflexe — incident cyber

À imprimer et afficher. Les 60 premières minutes décident de la gravité de l'incident.

Entreprise _____ **Date** _____ **Version** _____

Les 8 réflexes

#	Réflexe	Pourquoi
1	**Garder son calme et alerter** le référent et la direction immédiatement.	Un incident signalé tôt reste souvent un incident mineur.
2	**Isoler** la machine suspecte : débrancher le câble réseau, couper le Wi-Fi. Éviter d'éteindre ou de redémarrer sauf consigne contraire.	Stoppe la propagation et préserve les traces utiles à l'enquête.
3	**Ne rien supprimer**, ne pas « nettoyer » soi-même ; noter l'heure et ce qui s'est passé.	Les éléments de preuve servent au diagnostic, à la plainte et à l'assurance.
4	**Changer les mots de passe** concernés depuis un appareil sain, révoquer les sessions ouvertes, activer la MFA.	Coupe l'accès de l'attaquant aux comptes compromis.
5	**Prévenir** le prestataire informatique, la banque (en cas de fraude au virement) et l'assureur cyber.	L'assurance impose un délai de déclaration, souvent court : consultez votre contrat.
6	**Ne pas payer la rançon** ni négocier seul. Vérifier d'abord l'état des sauvegardes.	Payer ne garantit pas la restitution et finance les attaquants.
7	**Porter plainte** (police ou gendarmerie) et contacter l'assistance **Cybermalveillance.gouv.fr**.	Indispensable pour l'assurance et pour être orienté vers des prestataires qualifiés.
8	**Notifier la CNIL sous 72 h** si des données personnelles sont concernées (notifications.cnil.fr) ; informer les clients concernés.	Obligation RGPD (art. 33) ; le délai court dès que vous avez connaissance de la violation.

Ce qu'il ne faut surtout pas faire

- Utiliser la messagerie compromise pour communiquer sur l'incident : passez par un téléphone ou une messagerie sûre.
- Répondre aux menaces ou cliquer sur les liens du message de l'attaquant.
- Restaurer les données avant d'avoir identifié et isolé l'origine de l'attaque (risque de réinfection).
- Cacher l'incident à vos clients ou à l'autorité lorsque la loi impose de les informer.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Contacts d'urgence — à remplir dès aujourd'hui

Qui	Nom	Téléphone (24 h/24 si possible)
Direction		
Référent cybersécurité / RGPD		
Suppléant		
Prestataire informatique		
Assureur cyber (n° de contrat)		
Banque (opposition / fraude)		
Avocat / conseil		
Cybermalveillance.gouv.fr (assistance)	—	Plateforme nationale d'assistance aux victimes : cybermalveillance.gouv.fr
CNIL — notification de violation	—	notifications.cnil.fr

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.

Journal d'incident (main courante)

Consignez les faits **au fil de l'eau** : cette chronologie sert à la plainte, à l'assureur, à la CNIL et au retour d'expérience.

Date	Heure	Fait constaté / action menée	Par qui

Qualification de l'incident

Nature (hameçonnage, rançongiciel, fraude au virement, vol de matériel, erreur humaine…)	
Systèmes et données touchés	
Données personnelles concernées ? Nombre de personnes	
Activité interrompue (durée estimée)	
Notifications faites (CNIL, assureur, clients, plainte) — dates	

Après l'incident
Dans les 15 jours : retour d'expérience avec l'équipe (qu'est-ce qui a fonctionné, qu'est-ce qui a manqué ?), mise à jour de la charte, du plan de sauvegarde et du registre des violations, et information des clients concernés. Un incident bien géré est aussi une preuve de maturité auprès de vos donneurs d'ordres.

Modèle fourni à titre informatif, à adapter à votre situation. Il ne constitue pas un avis juridique.