PROCÉDURE DE GESTION DES INCIDENTS DE SÉCURITÉ ET VIOLATIONS DES RENSEIGNEMENTS PERSONNELS

I. Aperçu

Un plan d'intervention est essentiel pour gérer des cybers incidents de manière efficace. Dans ces moments de crise, on ne sait pas toujours comment agir et prioriser les actions. Un plan d'intervention vient réduire le stress d'oublier des aspects importants.

II. Objectif

Le but de cette procédure est de s'assurer que l'organisation est prête à intervenir en cas de cyber incident de manière à pouvoir reprendre rapidement ses activités.

III. Portée

La portée de cette procédure inclut tous les réseaux et systèmes, ainsi que les parties prenantes (clients, partenaires, employés, sous-traitants, fournisseurs) qui accèdent à ces systèmes.

IV. Reconnaître un cyber incident

Un incident de cybersécurité peut ne pas être reconnu ou détecté immédiatement. Toutefois, certains indicateurs peuvent être les signes d'une atteinte à la sécurité, qu'un système a été compromis, d'une activité non autorisée, etc. Il faut toujours être à l'affût de tout signe indiquant qu'un incident de sécurité s'est produit ou est en cours.

Certains de ces indicateurs sont décrits ci-dessous :

1. Activité excessive ou inhabituelle de la connexion et du système, notamment à partir de tout identifiant d'utilisateur (compte d'utilisateur) inactif.
2. Accès distant excessif ou inhabituel dans votre organisation. Cela peut concerner le personnel ou des fournisseurs tiers.
3. L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible.
4. Une activité inhabituelle liée à la présence de logiciels malveillants, de fichiers suspects ou de fichiers et programmes exécutables nouveaux ou non approuvés.
5. Ordinateurs ou appareils perdus, volés ou égarés qui contiennent des données de cartes de paiement, renseignements personnels ou d'autres données sensibles.

V. Coordonnées des personnes-ressources

RÔLE	NOM	TÉLÉPHONE	ADRESSE COURRIEL
Responsable du traitement des incidents	Marie-Claude Leblond	581-814-3338	mc.leblond@cliniquepropulsion.com
Direction	Philippe Girard	581-814-3338	administration@cliniquepropulsion.com
Responsable des TI	Micaël Vicaire	418-688-8088	mvicaire@absolu.ca
Responsable des communications	Marie-Claude Leblond	581-814-3338	mc.leblond@cliniquepropulsion.com
Avocat-Conseil			

VI. Atteinte à la protection des renseignements personnels – Intervention spécifique

S'il a été confirmé qu'un incident de sécurité lié à une atteinte à la protection des renseignements personnels s'est produit, il faudra effectuer les étapes suivantes :

☐ *Compléter le registre d'incidents de confidentialité pour documenter l'incident.*

☐ *Examiner l'atteinte à la protection des renseignements personnels pour déterminer si des renseignements personnels ont été perdus en raison d'un accès ou utilisation non autorisés, d'une divulgation non autorisée ou de toute atteinte à la protection de ces renseignements personnels et qu'il existe un risque de préjudice sérieux pour les personnes concernées.*

- *Dans un tel cas, le signaler à la Commission de l'accès à l'information au Québec*
- *Et, le signaler aux personnes dont les renseignements personnels sont visés par l'incident.*

VII. Rançongiciel – Intervention spécifique

S'il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

☐ *Déconnecter immédiatement du réseau les appareils visés par un rançongiciel.*
☐ *Ne RIEN EFFACER sur de vos appareils (ordinateurs, serveurs, etc.).*
☐ *Examiner le rançongiciel et déterminer comment il a infecté l'appareil. Cela vous aidera à comprendre comment l'éliminer.*
☐ *Communiquer avec les autorités locales pour signaler l'incident et coopérer à l'enquête.*
☐ *Une fois le rançongiciel supprimé, une analyse complète du système doit être effectuée à l'aide d'un antivirus, d'un anti-maliciel et de tout autre logiciel de sécurité le plus récent disponible afin de confirmer qu'il a été supprimé de l'appareil.*

- ☐ *Si le rançongiciel ne peut pas être supprimé de l'appareil (souvent le cas avec les programmes malveillants furtifs), l'appareil doit être réinitialisé au moyen des supports ou des images d'installation d'origine.*
    - *Avant de procéder à la réinitialisation à partir de supports/images de sauvegarde, vérifier qu'ils ne sont pas infectés par des maliciels.*
- ☐ *Si les données sont critiques et doivent être restaurées, mais ne peuvent être récupérées à partir de sauvegardes non affectées, rechercher les outils de déchiffrement disponibles sur* ***nomoreransom.org*****.**
- ☐ *La politique est de ne pas payer la rançon, sous réserve des enjeux en cause. Il est également fortement recommandé de faire appel aux services d'un chef de projet expert en cyberattaques (breach coach).*
- ☐ *Protéger les systèmes pour éviter toute nouvelle infection en mettant en œuvre des correctifs ou des rustines pour empêcher toute nouvelle attaque.*
- ☐ *Aviser nos clients et fournisseurs qu'ils pourraient recevoir des courriels frauduleux de notre part, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.*
- ☐ *Vérifier si on a encore accès au compte en ligne.*
    - *Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès.*
- ☐ *Changer le mot de passe utilisé pour se connecter à la plateforme.*
- ☐ *Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.*
- ☐ *Activer le double facteur d'authentification pour la plateforme.*
- ☐ *Supprimer les connexions et les appareils non légitimes de l'historique de connexion.*

VIII. Piratage de compte – Intervention spécifique

S'il a été confirmé qu'un piratage de compte s'est produit, il faudra effectuer les étapes suivantes :

- ☐ *Aviser nos clients et fournisseurs qu'ils pourraient recevoir des courriels frauduleux de notre part, et spécifier de ne pas répondre ou cliquer sur les liens de ces courriels.*
- ☐ *Vérifier si on a encore accès au compte en ligne.*
    - *Sinon, communiquer avec le support de la plateforme pour tenter de récupérer l'accès.*
- ☐ *Changer le mot de passe utilisé pour se connecter à la plateforme.*
- ☐ *Si le mot de passe est réutilisé ailleurs, changer également tous ces mots de passe.*
- ☐ *Activer le double facteur d'authentification pour la plateforme.*
- ☐ *Supprimer les connexions et les appareils non légitimes de l'historique de connexion.*

IX. Perte ou vol d'un appareil – Intervention spécifique

S'il a été confirmé qu'une perte d'équipement s'est produite, il faudra effectuer les étapes suivantes :

- ☐ *Le vol ou la perte d'un bien, tel qu'un ordinateur, un ordinateur portatif ou un appareil mobile, doit être signalé immédiatement aux autorités policières locales. Cela inclut les pertes/vols en dehors des heures d'ouverture normale et pendant les week-ends.*
- ☐ *Si l'appareil perdu ou volé contenait des données sensibles et qu'il n'est pas crypté, effectuer une analyse de sensibilité, du type et du volume des données volées, y compris les numéros de cartes de paiement potentiellement concernés.*
- ☐ *Dans la mesure du possible, verrouiller/désactiver les appareils mobiles perdus ou volés (p. ex. : téléphones intelligents, tablettes, ordinateurs portatifs, etc.) et procéder à un effacement des données à distance.*