Procédure d'Alerte en Matière de Sécurité de l'Information

Responsable.Sécurité.des.Systèmes.d"Information.(RSSI).Frédéric.Varon¡

La présente procédure a pour objectif de mettre à disposition des parties prenantes un mécanisme clair, confidentiel et accessible leur permettant de signaler tout incident, vulnérabilité ou comportement suspect lié à la sécurité de l'information, afin de prévenir tout dommage, fuite de données ou atteinte à l'intégrité du système d'information.

1 Champ d'application

Cette procédure s'applique à :

- Tous les collaborateurs internes
- Les partenaires, prestataires, clients et tiers ayant un lien contractuel ou opérationnel avec Easypitch-HPL
- Les utilisateurs des systèmes d'information d'Easypitch-HPL

2 Types de problèmes à signaler

Les parties prenantes sont invitées à signaler notamment :

- Tentative de phishing ou réception de courriels suspects
- Perte ou vol d'équipements contenant des données sensibles
- Accès non autorisé à des systèmes ou fichiers
- Comportement inhabituel ou suspect sur le réseau
- Utilisation non conforme des systèmes d'information
- Détection de logiciels malveillants, virus ou ransomwares
- Toute faille ou vulnérabilité technique connue

3 Canaux de signalement disponibles

3.1 En externe

Les signalements peuvent être effectués par l'un des moyens suivants :

- Par courriel confidentiel à : support@tsr-informatique.fr
- Par courrier à l'attention du Responsable Sécurité des Systèmes d'Information : Easypitch, 33 Rue de la Révolution, 93100 Montreuil.

3.2 En interne

- Par communication directe auprès : De Frédéric Varon RSSI.

4 Informations à fournir lors du signalement

Le signalement doit, dans la mesure du possible, inclure les éléments suivants :

- Une description claire et factuelle des faits
- La date et le lieu présumés des faits
- Les noms des personnes impliquées (si connus)

- Tout document ou preuve disponibles

Les signalements peuvent être effectués **de manière anonyme**, mais il est recommandé de laisser un moyen de contact pour un suivi plus efficace.

5 Traitement des signalements

- Tous les signalements sont reçus et traités par le RSSI et/ou la direction.
- Accusé de réception automatique ou personnalisé sous 48 heures ouvrées.
- Évaluation de la criticité de l'incident par le RSSI et son équipe.
- Ouverture d'une enquête technique si nécessaire.
- Mise en œuvre de mesures correctives ou préventives.
- Signalement au CERT pour les logiciels en cas de faille reconnue.
- Signalement à la CNIL dans les 72 heures en cas de fuite avérée de données personnelles.
- Notification aux personnes concernées en cas d'impact avéré.
- L'ensemble du processus est traité de manière confidentielle et dans le respect des droits des personnes concernées.

6 Confidentialité et protection du lanceur d'alerte

- Tous les signalements sont traités dans la plus stricte confidentialité.
- Aucune mesure de représailles ne sera tolérée à l'encontre d'un déclarant ayant agi de bonne foi, conformément aux lois applicables sur la protection des lanceurs d'alerte.

7 Suivi et amélioration

Chaque signalement fait l'objet d'un enregistrement et est intégré au processus global d'amélioration continue de la politique de sécurité de l'information.

8 Références

- PAS (Plan Assurance Sécurité) de HPL Easypitch & RGPD
- Politique de protection des données Easypitch SAS
- Politique de protection des données Easypitch HPL
- Loi n° 2016-1691 sur la transparence et la lutte contre la corruption (« Loi Sapin II ») — en lien avec la protection des lanceurs d'alerte.