Procédure de gestion des incidents de confidentialité

HAN-
DROITS

Objectif

La présente procédure vise à encadrer la gestion des incidents de confidentialité afin de :

- Protéger les renseignements personnels détenus par l'organisation
- Réduire les risques de préjudice aux personnes concernées
- Assurer la conformité à la Loi 25
- Documenter et améliorer les pratiques de sécurité de l'information

Portée

Cette procédure s'applique à :

- Tous les employés, contractuels et bénévoles
- Tous les renseignements personnels détenus ou traités par Han-Droits
- Tout incident impliquant un accès, une utilisation, une communication ou une perte non autorisée de renseignements personnels

Définition d'un incident de confidentialité

Constitue un incident de confidentialité toute situation impliquant :

- L'accès non autorisé de renseignements personnels
- L'utilisation ou la communication non autorisée de renseignements personnels
- La perte ou le vol de renseignements personnels

Exemples :

- Envoi d'un courriel à la mauvaise personne
- Perte d'un ordinateur ou document contenant des données personnelles
- Piratage ou accès non autorisé à un système
- Divulgation accidentelle d'informations sensibles

Principes généraux

Toute personne doit signaler immédiatement tout incident réel ou potentiel. La protection des personnes concernées est prioritaire. Chaque incident doit être documenté dans un registre interne. Une évaluation du risque de préjudice doit être réalisée. Les mesures correctives doivent être appliquées sans délai.

Responsabilités

Employés et bénévoles

- Signaler immédiatement tout incident ou soupçon d'incident à la direction
- Coopérer à l'analyse et aux mesures correctives

Direction

- Évaluer la gravité et le risque de préjudice
- Mettre en place les mesures de mitigation
- Déterminer si une déclaration à la CAI et/ou aux personnes concernées est requise
- Tenir le registre des incidents

Responsable de la protection des renseignements personnels

- Superviser la gestion des incidents
- Assurer la conformité à la Loi 25
- Coordonner les communications externes si nécessaire

Procédure de gestion d'un incident

Étape 1 – Détection et signalement
Toute personne doit signaler immédiatement l'incident à la direction ou au responsable désigné.

Étape 2 – Contention de l'incident. L'organisation prend sans délai des mesures pour :

- Limiter la portée de l'incident
- Sécuriser les systèmes ou documents
- Empêcher toute aggravation

Étape 3 – Évaluation du risque. Une analyse est effectuée pour déterminer :

- La sensibilité des renseignements
- La probabilité d'utilisation malveillante
- La gravité des conséquences pour les personnes concernées

Étape 4 – Décision de notification. Selon l'évaluation :

- La Commission d'accès à l'information (CAI) est avisée, au besoin
- Les personnes concernées sont informées, si nécessaire

Étape 5 – Notification. Si requis, l'organisation informe :

- La CAI du Québec
- Les personnes concernées (de façon claire et sécuritaire)

Les informations transmises incluent :

- Description de l'incident
- Renseignements touchés
- Mesures prises et recommandations pour limiter les risques

Étape 6 – Registre des incidents. Tous les incidents, qu'ils soient mineurs ou majeurs, sont consignés dans un registre incluant :

- Date et description
- Type de données concernées
- Analyse du risque
- Mesures prises
- Décisions de notification et suivi

Procédure de gestion d’un incident

Étape 7 – Mesures correctives et prévention. Après chaque incident, l’organisation met en place des mesures pour éviter la répétition, telles que :

- Amélioration des pratiques de sécurité
- Formation du personnel
- Ajustement des procédures internes
- Renforcement des contrôles d’accès

Confidentialité

Tous les incidents et informations liés sont traités de façon confidentielle et ne sont accessibles qu’aux personnes autorisées.

Révision de la procédure

La présente procédure est révisée au minimum tous les deux (2) ans ou lors de changements législatifs ou organisationnels importants.

Entrée en vigueur
DATE