# Procédure sur les incidents de confidentialité

Le 30 août 2023

Direction des affaires juridiques et corporatives

SHDM

SOCIÉTÉ D'HABITATION
ET DE DÉVELOPPEMENT
DE MONTRÉAL

# Table des matières

# Section I – Dispositions préliminaires

## 1.1. Définitions

Dans la présente procédure, les expressions et les mots suivants signifient :

**CAI** : Commission d'accès à l'information du Québec.

**Employé** : personne qui a un lien d'emploi ou de stage avec la SHDM.

**Incident**: désigne l'accès, l'utilisation ou la communication non autorisés par la loi d'un renseignement personnel ou la perte ou l'altération, accidentelle ou non, et toute autre atteinte à la protection d'un tel renseignement. Il correspond à un incident de confidentialité au sens de la Loi sur l'accès.

**Loi sur l'accès :** *Loi sur l'accès à l'information et la protection des renseignements personnels (RLRQ* c.A-2.1*)* et ses amendements.

**Registre des incidents** : désigne le registre qui contient tous les éléments relatifs à un Incident, que son signalement soit requis ou non. Ce document est requis en vertu de la Loi sur l'accès. Veuillez consulter l'Annexe A.

**Renseignement personnel :** désigne toute information qui se rapporte à une personne physique et qui permet, directement ou indirectement, de l'identifier. Ces Renseignements personnels peuvent inclure, sans s'y limiter : le nom, l'adresse, le numéro de téléphone, l'adresse courriel, la photo, le numéro d'assurance sociale, la date et le lieu de naissance, le numéro de compte bancaire ou de carte de crédit, le dossier médical, les antécédents scolaires, les diplômes et les antécédents professionnels. Les Renseignements personnels sont confidentiels. Sauf exception prévues par la loi, ils ne peuvent être communiqués sans le consentement de la personne concernée.

**RPRP** : désigne la personne responsable de la protection des renseignements personnels au sein de la SHDM et désignée comme telle auprès de la CAI. En son absence, le responsable substitut de la protection des renseignements personnels exerce les responsabilités du RPRP.

## 1.2. Objet

La présente procédure (ci-après la « **Procédure** ») vise à fournir des directives sur la façon d'intervenir en cas d'Incident touchant les systèmes informatiques, les activités ou les actifs informationnels de la Société d'habitation et de développement de Montréal (ci-après la « **SHDM** »), conformément à la Politique sur l'accès à l'information et la protection des renseignements personnels de la SHDM (ci-après la « **Politique** ») et à Loi sur l'accès.

La présente Procédure s'applique :

- à tout Employé de la SHDM, sans égard à son statut d'emploi;
- à tout dirigeant, administrateur et ressource externe.

# Section II – Processus de gestion des Incidents

## 2.1. Signalement d'un Incident

### 2.1.1. Formulaire de dénonciation

Toute personne qui a un motif de croire que s'est produit un Incident doit aviser sans délai le RPRP en transmettant un courriel à l'adresse courriel acces.info@shdm.org. Si l'Incident pourrait affecter les systèmes informatiques, le Bureau des technologies de l'information doit immédiatement être avisé également en ajoutant en copie conforme l'adresse courriel supportinfo@shdm.org ou encore en téléphonant au 514 380-2126. Dès qu'il en a l'occasion, l'auteur du signalement doit compléter avec son supérieur immédiat, la première partie du Formulaire de déclaration d'un incident disponible sur le RÉSO et le transmettre à l'adresse courriel acces.info@shdm.org.

## 2.2. Évaluation de l'incident

### 2.2.1. Évaluation initiale

Le RPRP effectue une évaluation initiale de l'incident en s'assurant d'abord qu'il s'agit réellement d'un incident de confidentialité.

S'il ne s'agit pas d'un incident de confidentialité et que les systèmes informatiques de la SHDM sont affectés, l'incident est pris en charge par le Bureau des technologies de l'information et la présente procédure n'est pas applicable.

S'il s'agit d'un incident de confidentialité, une évaluation préliminaire du degré de gravité de l'Incident est réalisée par le RPRP. Si l'Incident affecte également les systèmes informatiques, l'évaluation préliminaire est réalisée en collaboration avec un Employé du Bureau des technologies de l'information.

Le tableau de classement des Incidents ci-dessous présente divers facteurs devant aider le RPRP et l'Employé du Bureau des technologies de l'information, si applicable, à classer un Incident. Certains des facteurs ne s'appliquent pas nécessairement à tous les Incidents et d'autres facteurs pourraient servir lors de l'évaluation initiale.

| Facteurs relatifs à l'Incident | Degré de gravité de l'Incident | | |
|---|---|---|---|
| | 1er degré | 2e degré | 3e degré |
| **Effets sur les personnes concernées et les actifs informationnels** | Touche peu de personnes ou de systèmes et ne cause pas d'indisponibilité des actifs informationnels | Effet à l'échelle d'un service ou indisponibilité à court terme des actifs informationnels | Effet à l'échelle de la SHDM ou interruption de la disponibilité de l'information et/ou des processus pour une période de temps excédant 72 heures |
| **Effets sur le public** | Aucun | Effet potentiel | Effet indéniable |
| **Mesures de remédiation** | Solutions disponibles | Faibles mesures de remédiation | Aucune mesure de remédiation |
| **Chiffrement ou anonymisation des renseignements touchés** | Algorithme de chiffrement et contrôle par clés robustes | Algorithme et/ou contrôle par clés faibles | Aucun chiffrement, ou chiffrement facilement déchiffrable |
| **Procédure de résolution des problèmes techniques** | Disponible et bien définie | Procédure de résolution mal définie, solutions disponibles | Aucune procédure de résolution ni aucune autre solution disponible |
| **Sensibilité des renseignements** | Faible | Moyenne | Élevée |

| Facteurs relatifs à l'Incident | Degré de gravité de l'Incident | | |
|---|---|---|---|
| | 1er degré | 2e degré | 3e degré |
| **Incident devant potentiellement être signalé à la CAI, aux personnes concernées ou une autorité de réglementation ou agence d'application de la loi** | Non | Possible | Oui |

Si un Incident présente des caractéristiques qui correspondent à plusieurs colonnes de gravité, la gravité de l'Incident correspond à la gravité la plus élevée. Par exemple, si un Incident touche un service ayant un lien avec des Renseignements personnels sensibles (deuxième degré de gravité) et a un effet public indéniable (troisième degré de gravité), l'Incident doit être classé dans la catégorie du troisième degré de gravité.

Le classement des Incidents est un processus dynamique. La gravité d'un Incident peut évoluer au fur et à mesure que l'enquête révèle de nouveaux faits.

Dès l'évaluation initiale, tout employé concerné sera avisé des mesures à prendre afin de contenir l'Incident. Lorsque possible et lorsqu'applicable, l'employé du Bureau des technologies de l'information doit prendre les actions prévues au paragraphe 9.3 du Guide de sécurité de l'information.

### 2.2.2. Enquête et gestion de l'Incident

Si de l'avis du RPRP et de l'Employé du Bureau des technologies de l'information, le cas échéant, l'Incident nécessite de faire appel à une équipe de gestion des Incidents (ci-après l'« **Équipe** ») en raison, notamment, de la gravité de l'Incident, cette équipe est formée comme suit :

**Rôle et fonctions principales de l'Équipe**

**L'Équipe**

- Lorsque sollicitée, recueille toutes les informations pertinentes et prend les décisions, avec le RPRP, pour gérer l'Incident dans le meilleur intérêt des personnes concernées.
- Gère tous les aspects de nature stratégique et opérationnelle liés à l'Incident.
- Détermine la répartition des ressources de la SHDM et établit la marche à suivre dans les relations avec les différents intervenants et personnes concernées (citoyens, fournisseurs, autorités réglementaires, service de police, courtier d'assurance, média, etc.).
- Rédige les communications contenant des renseignements factuels sur l'Incident.

**Le RPRP**

- Lors d'un Incident, le RPRP coordonne la mise en place du plan de réponse, en collaboration avec le directeur des affaires juridiques et corporatives et, si nécessaire, avec un conseiller juridique externe.
- Il agit comme point de contact principal des communications relatives à l'Incident et s'assure du respect des obligations légales de la SHDM à l'égard de l'Incident.
- Il doit être consulté à toutes les étapes de la gestion de l'Incident pour garantir la préservation du secret professionnel.

## Rôle et fonctions principales de l'Équipe

**L'Équipe**

- Lorsque sollicitée, recueille toutes les informations pertinentes et prend les décisions, avec le RPRP, pour gérer l'Incident dans le meilleur intérêt des personnes concernées.
- Gère tous les aspects de nature stratégique et opérationnelle liés à l'Incident.
- Détermine la répartition des ressources de la SHDM et établit la marche à suivre dans les relations avec les différents intervenants et personnes concernées (citoyens, fournisseurs, autorités réglementaires, service de police, courtier d'assurance, média, etc.).
- Rédige les communications contenant des renseignements factuels sur l'Incident.

**Le chef des technologies de l'information**

- Le chef - technologies de l'information s'occupe de tous les aspects techniques de l'Incident lorsque l'Incident touche les systèmes informatiques de la SHDM.
- Il doit notamment procéder à l'analyse de l'Incident, gérer les risques techniques qui y sont associés et mettre en place des mesures de protection et de récupération adéquates.

**Le directeur des affaires juridiques et corporatives**

- En collaboration avec le RPRP, le directeur des affaires juridiques et corporatives conseille la SHDM pour lui permettre de remplir ses obligations légales et pour l'accompagner dans la gestion du risque juridique.

Dépendamment de la gravité d'un Incident, les membres suivants pourraient être ajoutés à l'Équipe :

Le conseiller communications et marketing, afin d'établir des stratégies de communication et remplir les obligations de notification de manière optimale.

Une personne responsable de la gestion des demandes et plaintes éventuelles de personnes concernées, tel que le conseiller expérience client.

Une personne agissant comme point de contact principal auprès des Employés et gérant tous les aspects des ressources humaines entourant l'Incident.

Une personne responsable de la mise en œuvre opérationnelle des décisions prises par l'Équipe et de l'évaluation des conséquences de l'Incident pour la SHDM.

Des cadres des directions ou équipes principalement touchées.

Des membres du comité de direction.

La nature de l'Incident pourrait nécessiter de remanier la composition de l'Équipe, que ce soit en ce qui concerne ses membres, leurs rôles ou leurs responsabilités.

Le RPRP, de concert avec l'Équipe, s'il y a lieu, coordonne la collecte et la préservation des éléments de preuve, afin d'être en mesure de répondre aux questions « qui, quoi, quand, où, pourquoi et comment ? » à l'égard de chaque Incident.

L'objectif est de déterminer la cause fondamentale de l'Incident, ainsi que son étendue et ses effets. La SHDM pourrait devoir procéder à une enquête de cybersécurité et interroger tout Employé ayant connaissance de l'Incident. L'Équipe évaluera si la SHDM devrait avoir recours à des acteurs externes pour l'enquête de cybersécurité.

Le directeur des affaires juridiques et corporatives devra également déterminer s'il est approprié de présenter une réclamation en vue de recouvrer les coûts associés à l'Incident ou pour obtenir de l'aide de l'assureur dans la gestion de l'Incident. Il peut être essentiel de déclarer l'Incident aux assureurs le plus rapidement possible afin d'éviter un refus de réclamation.

L'Équipe détermine également s'il y a lieu d'appliquer d'autres politiques et procédures de la SHDM.

Si l'on soupçonne qu'un Employé a participé à l'Incident, la tenue d'une enquête sur le lieu de travail pourrait être nécessaire. Il faudra alors tenir compte des aspects liés au droit du travail et de la nécessité de faire appel au directeur des ressources humaines, des communications et de l'expérience-client et au directeur des affaires juridiques et corporatives.

L'Équipe assure le suivi continu afin de déterminer si quelque chose d'autre peut être fait pour circonscrire les effets de l'Incident et y mettre fin.

En cas d'Incidents majeurs qui peuvent perturber les activités pour une période excédant 72 heures, le Plan de reprise après sinistre et redondance sera invoqué afin de s'assurer de la reprise des activités dans les meilleurs délais. La cellule de crise prévue au Plan de reprise après sinistre et redondance pourrait alors se substituer à l'Équipe.

## 2.3. Évaluation du risque de préjudice sérieux et signalement

Le RPRP et la Direction des affaires juridiques et corporatives doivent déterminer si les personnes ou entités touchées, y compris la Direction générale de la SHDM, les autorités de réglementation, les organismes chargés de l'application de certaines lois, les personnes physiques ou les Employés devraient être avisés de l'Incident.

Un signalement peut être approprié dans les cas suivants :

- la SHDM y est tenue contractuellement;
- la SHDM y est tenue en vertu de la Loi sur l'accès;
- Les personnes concernées, une fois avisées de l'Incident, auraient intérêt à prendre des mesures de protection;
- Le type de gravité de l'Incident est tel que l'on s'attendrait raisonnablement à ce qu'il fasse l'objet d'un signalement.

### 2.3.1. Signalement requis en vertu de la Loi sur l'accès et évaluation du risque de préjudice sérieux

Afin d'établir si la SHDM doit aviser la CAI ou les personnes concernées de la survenance d'un Incident, il est nécessaire de procéder à l'évaluation du risque de préjudice. À cette étape, le RPRP doit être consulté.

En effet, la SHDM aura des obligations de signalement seulement lorsque l'Incident présente un risque de préjudice sérieux pour les personnes concernées.

Le risque de préjudice sera généralement considéré comme tel si l'Incident présente un risque pour les personnes concernées, leurs biens ou s'il pourrait autrement nuire à leurs intérêts de façon importante (par exemple, s'il y a un risque important d'atteinte à la réputation des personnes touchées).

Dans le cadre de cette évaluation, la SHDM doit notamment tenir compte des éléments suivants :

- ✓ La sensibilité des renseignements concernés par l'Incident ;
    - Plus le degré de sensibilité est élevé, plus le risque que le préjudice soit sérieux est important.
- ✓ Les conséquences appréhendées de leur utilisation ;
    - À titre d'exemple, si des renseignements d'identité ont été exfiltrés (tels que le numéro d'assurance sociale, le nom ou encore l'adresse d'une personne), le vol d'identité ou une fraude financière pourraient résulter d'une utilisation malhonnête de ces renseignements.
- ✓ La probabilité qu'ils soient utilisés à des fins préjudiciables ;
    - À titre d'exemple, les éléments suivants indiquent la probabilité haute ou faible que les renseignements soient utilisés à des fins préjudiciables :

| Haut risque | Faible risque |
|---|---|
| ✓ L'Incident résulte d'un acte intentionnel (par opposition à une divulgation accidentelle).<br>✓ Une entité malveillante ou qui présente un risque pour la réputation de la personne concernée a pris possession des Renseignements personnels.<br>✓ Les renseignements ont été communiqués à un nombre important de personnes.<br>✓ Les renseignements n'ont pas pu être récupérés.<br>✓ Les renseignements sont facilement accessibles (par exemple, en l'absence de chiffrement adéquat).<br>✓ Un préjudice s'est effectivement matérialisé. | ✓ Les renseignements sont entre les mains d'entités restreintes ou connues qui se sont engagées à détruire ou ne pas divulguer les renseignements.<br>✓ Les renseignements ont été exposés à des personnes ou des entités peu susceptibles de les communiquer de façon préjudiciable (par exemple, dans le cadre d'une communication accidentelle à un mauvais destinataire).<br>✓ Les renseignements compromis ou inaccessibles ont été récupérés.<br>✓ Les renseignements sont adéquatement chiffrés, anonymisés ou autrement difficiles d'accès. |

- ✓ La quantité de renseignements impliqués et le nombre de personnes visées.

La grille d'évaluation initiale de l'Incident au paragraphe 2.2.1 peut servir à évaluer le risque de préjudice. Si, à la suite de l'évaluation, la SHDM conclut à la présence d'un tel risque, elle devra alors aviser, avec diligence, la CAI et les personnes dont les Renseignements personnels sont concernés par l'Incident.

Si les personnes concernées doivent être avisées, le RPRP et la Direction des affaires juridiques et corporatives déterminent également le mode et les détails de l'avis conformément à la Loi sur l'accès et au Règlement sur les incidents de confidentialité.

### 2.3.2. Autres communications

D'autres signalements ou communications pourraient être nécessaires ou utiles dans le cadre de la gestion de l'Incident, par exemple, à des partenaires d'affaires et fournisseurs de services, à certaines autorités, comme les services de police et aux assureurs.

Voici une liste de facteurs pertinents à prendre en considération pour déterminer dans quelles circonstances certains tiers devraient être avisés :

〉 **Partenaires d'affaires et fournisseurs de service**

- ✓ Déterminer quels partenaires d'affaires et fournisseurs sont concernés.
- ✓ Déterminer le type de renseignements compromis et s'ils ont été chiffrés (et si la clé de chiffrement a été compromise).
- ✓ Déterminer s'il est raisonnablement probable qu'un préjudice soit causé à des partenaires d'affaires, des mandataires, des fournisseurs ou à des tiers.
- ✓ Passer en revue les contrats pour déterminer si la divulgation est requise.
- ✓ Travailler avec la Direction des affaires juridiques et corporatives pour déterminer quelles parties doivent être avisées et comment la communication doit être effectuée.
- ✓ Examiner s'il y a lieu de demander à un Employé qui a un lien avec ce tiers d'établir une communication proactive avant la communication officielle de l'Incident.
- ✓ S'assurer que l'Employé a en main des questions et réponses ainsi que des points de discussion.
- ✓ Examiner s'il y a lieu de diriger les demandes de renseignements supplémentaires de ces tiers vers un point de contact désigné par la SHDM.

〉 **Personne physique**

- ✓ Déterminer le type de renseignements compromis et s'ils ont été chiffrés (et si la clé de chiffrement a été compromise).
- ✓ Déterminer s'il est raisonnablement probable qu'un préjudice soit causé à une personne.
- ✓ Consulter la Direction des affaires juridiques et corporatives pour déterminer quelles personnes doivent être avisés et pour rédiger l'avis à donner.
- ✓ Examiner s'il y a lieu de diriger les demandes de renseignements supplémentaires des personnes vers un point de contact désigné par la SHDM.

〉 **Autorités de réglementation**

- ✓ Examiner s'il y a lieu d'aviser les organismes chargés de prévenir, détecter ou réprimer le crime ou les infractions aux lois, si un vol ou un autre crime est soupçonné.
- ✓ Consulter la Direction des affaires juridiques et corporatives pour déterminer quels types d'avis sont requis et rédiger les avis qui doivent être donnés.

〉 **Assureurs**

- ✓ Passer en revue les polices d'assurance pour déterminer si un avis est requis.
- ✓ Consulter la Direction des affaires juridiques et corporatives pour déterminer s'il est approprié de présenter une réclamation en vue de recouvrer les coûts associés à l'Incident. Il peut être essentiel de déclarer l'Incident aux assureurs le plus rapidement possible afin d'éviter un refus de réclamation.

〉 **Fournisseurs de cartes de crédit, institutions financières ou agences d'évaluation de la solvabilité**

- ✓ Déterminer si la SHDM a besoin de l'assistance de fournisseurs de cartes de crédit, d'institutions financières ou d'agences d'évaluation du crédit pour communiquer avec des personnes ou atténuer les préjudices (services de surveillance du crédit).

〉 **Médias**

- ✓ S'il y a lieu, la SHDM diffuse des communiqués de presse. Dans des circonstances exceptionnelles, une conférence de presse pourrait être tenue pour répondre à des questions au sujet de l'Incident et de ses effets. L'équipe des communications a la responsabilité d'organiser la tenue de la conférence de presse et de communiquer avec les représentants des médias qui veulent y assister.
- ✓ Les Employés ne doivent pas communiquer avec les médias (y compris en publiant des messages sur les médias sociaux), sans l'autorisation de l'Équipe et de la Direction des affaires juridiques et corporatives.

## 2.4. Tenue du Registre et prévention

Une fois l'enquête terminée, le RPRP fait un rapport sur l'Incident aux intervenants concernés, conformément aux lois applicables (notamment en matière de protection des Renseignements personnels), et en collaboration avec la Direction des affaires juridiques et corporatives.

Quelle que soit la gravité apparente d'un Incident, le RPRP doit documenter l'Incident. La SHDM doit notamment conserver les informations suivantes au Registre des incidents :

- Date ou période de l'Incident ;
- Circonstances entourant l'Incident ;
- Date ou période de prise de connaissance de l'Incident ;
- Nombre de personnes visées ou approximation ;
- Description des éléments qui amènent à conclure à un risque sérieux ou non ;
- Date de transmission à la CAI (s'il y a lieu) ;
- Mesures prises pour limiter les préjudices.

Le Formulaire de déclaration d'un Incident doit également inclure une justification des décisions prises en réponse à l'Incident, en particulier lorsque celui-ci n'est pas signalé à la CAI ou aux personnes concernées.

Le Registre des Incidents et le Formulaire de déclaration d'un incident doivent être conservés pour une période minimale de cinq (5) ans suivant la prise de connaissance de l'Incident, tel que prévu au Règlement sur les Incidents de confidentialité.

Une fois les mesures prises afin de limiter et d'atténuer les risques associés à l'Incident, la mise en place de mesures de protection à long terme peut être nécessaire. On examine s'il y a lieu de procéder à la vérification des protocoles de sécurité techniques et physiques, selon le cas. Le RPRP et le chef – technologies de l'information révisent et actualisent les pratiques internes en tenant compte de l'enquête sur l'Incident.

### 2.5. Reddition de comptes

Le Registre des incidents est produit annuellement au comité de gouvernance, des ressources humaines et des communications ainsi qu'au comité d'audit, de finances et de gestion des risques.

## Section III – Dispositions finales

### 3.1. Entrée en vigueur

La présente Procédure entre en vigueur à la suite de l'adoption de la Politique.

# *Annexe A*
# *Modèle de registre des incidents de confidentialité*

| No de Dossier | RP visés par l'incident | Circonstances de l'incident | Date/période incident | Nombre de personnes concernées | Description des éléments qui amènent la SHDM à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées | (si risque de préjudice sérieux) : date de transmission des avis à la commission et aux personnes concernées | Mesures adoptées à la suite de l'incident afin de diminuer les risques qu'un préjudice soit causé |
|---|---|---|---|---|---|---|---|
| **XXXX-XXXX** | | | | | a) Niveau de sensibilité des renseignements concernés :<br><br>b) Utilisations malveillantes possibles des renseignements :<br><br>c) Conséquences appréhendées de leur utilisation :<br><br>d) Probabilité qu'ils soient utilisés à des fins préjudiciables :<br><br>e) Autres éléments : | | |

| No de Dossier | RP visés par l'incident | Circonstances de l'incident | Date/période incident | Nombre de personnes concernées | Description des éléments qui amènent la SHDM à conclure qu'il existe ou non un risque qu'un préjudice sérieux soit causé aux personnes concernées | (si risque de préjudice sérieux) : date de transmission des avis à la commission et aux personnes concernées | Mesures adoptées à la suite de l'incident afin de diminuer les risques qu'un préjudice soit causé |
|---|---|---|---|---|---|---|---|
| **XXXX-XXXX** | | | | | a) Niveau de sensibilité des renseignements concernés :<br><br>b) Utilisations malveillantes possibles des renseignements :<br><br>c) Conséquences appréhendées de leur utilisation :<br><br>d) Probabilité qu'ils soient utilisés à des fins préjudiciables :<br><br>e) Autres éléments : | | |

.

SHDM

**SOCIÉTÉ D'HABITATION ET DE DÉVELOPPEMENT DE MONTRÉAL**

800, boulevard De Maisonneuve Est
Bureau 2200
Montréal (Québec)  H2L 4L8
Téléphone : 514 380-7436

**shdm.org**