Appel à Recycler Canada, Inc.

Soyez inspirant; changez les habitudes.MC

Politique de prise en charge des incidents en matière de confidentialité et plan d'intervention en cas d'incident de confidentialité

Objectif et champ d'application

La présente politique sur la prise en charge des incidents liés à la confidentialité et le plan d'intervention en cas d'incident a pour objet de s'assurer que Call2Recycle Canada Inc. (« **Call2Recycle** ») est prête à gérer les incidents liés à la protection de la vie privée et les cyberincidents de façon efficace et conformément aux nouvelles obligations imposées par le « Loi modernisant des dispositions législatives en matière de protection des renseignements personnels », communément appelée « projet de loi 25 ».

Ce document décrit la politique générale de Call2Recycle pour la prise en charge des incidents en matière de confidentialité et le plan d'intervention en cas d'incident de confidentialité. Il définit la structure, les rôles et les responsabilités, les types d'incidents courants et l'approche pour se préparer aux incidents liés à la protection des renseignements personnels et à la cybersécurité, les cerner, les contenir et en tirer des leçons afin de réduire au minimum les répercussions de ces incidents.

L'objectif de la politique et du plan d'intervention en cas d'incident est de veiller à ce que Call2Recycle soit organisée de manière à répondre efficacement aux incidents liés à la protection des renseignements personnels ou à la cybersécurité.

La présente politique et le plan d'intervention en cas d'incident s'appliquent à tous les réseaux, systèmes et données de Call2Recycle, ainsi qu'aux parties prenantes (y compris les employés et les fournisseurs tiers) qui y ont accès.

Le présent document définit les capacités de traitement et d'intervention en cas d'incident et indique l'intervention appropriée en cas d'incident de cybersécurité courant. Le présent document ne vise pas à fournir une liste détaillée de toutes les activités à exécuter en réponse aux incidents de cybersécurité, mais plutôt à donner un aperçu général des étapes essentielles à suivre en cas de cyberincident.

Définitions

Incident de confidentialité : un incident de confidentialité est défini comme suit :

(1) accès non autorisé par la loi aux renseignements personnels;
(2) utilisation non autorisée par la loi des renseignements personnels;
(3) communication non autorisée par la loi des renseignements personnels;
(4) perte de renseignements personnels ou toute autre atteinte à la protection de ces renseignements.

Personne responsable de la protection des renseignements personnels : la personne responsable de la protection des renseignements personnels se définit comme la personne exerçant l'autorité la plus élevée qui veille à ce que le projet de loi 25 soit mis en œuvre et respecté. Cette personne exerce la fonction de responsable de la protection des renseignements personnels; elle peut déléguer par écrit l'entièreté ou une partie de cette fonction à la personne de son choix.

Renseignements personnels : tout renseignement qui a trait à une personne physique et qui permet de l'identifier.

Maliciel : terme générique qui décrit tout programme ou code malveillant nuisible aux systèmes informatiques.

Virus : un virus peut infecter l'ordinateur et d'autres appareils, mais il peut aussi réapparaître et infecter les appareils d'autres personnes, y compris ceux qui figurent dans une liste de contacts.

Ver : logiciel malveillant qui n'est pas attaché à un fichier et qui peut s'activer lui-même pour faire des copies sans qu'aucune action ne soit requise.

Cheval de Troie : maliciel déguisé en logiciel licite.

Logiciels espions ou logiciels publicitaires : des logiciels malveillants qui recueillent des renseignements personnels sur les activités en ligne de l'utilisateur au profit d'un tiers.

Rançongiciel : logiciel malveillant qui verrouille l'appareil et les données qu'il contient et réclame une somme d'argent en menaçant de supprimer l'ensemble des données.

Personnes-ressources

La responsabilité de la sécurité des renseignements confidentiels, y compris les renseignements personnels, incombe à tous. En cas d'incident de confidentialité, la personne-ressource est :

Michael Partab
437-290-0096
privacy@call2recycle.ca

Si la personne-ressource n'est pas disponible, veuillez communiquer avec :

Grace Wu
437-900-8546
gwu@call2recycle.ca

Cabinet d'informatique mandaté en cas de problèmes informatiques :

Viviane Wans
416-307-2855
vwans@call2recycle.ca

En cas d'incident de confidentialité critique, une cellule de crise se réunira rapidement et sera composée des personnes mentionnées dans le tableau ci-dessous.

Rôle	Nom	Titre	Téléphone	Adresse courriel
Responsable de la protection des renseignements personnels	Michael Partab	Responsable de la protection des renseignements personnels	437-290-0096	privacy@call2recycle.ca
Gestion de la sécurité des ordinateurs et des serveurs	Viviane Wans	Directrice, Gestion des affaires	416-307-2855	vwans@call2recycle.ca
Gestion des communications	Jon McQuaid	Vice-président, Marketing, Communications et Innovation	647-484-2672	jmcquaid@call2recycle.ca

Types d'incidents de confidentialité

Il se peut qu'un incident de cybersécurité ou de confidentialité ne soit pas immédiatement reconnu comme tel; cependant, certains indicateurs peuvent être des signes d'une atteinte à la sécurité, d'un système compromis ou d'une activité non autorisée, ou des signes de mauvaise utilisation dans l'environnement de votre tiers ou de votre fournisseur de services tiers.

Soyez toujours à l'affût des signes indiquant qu'un incident de sécurité s'est produit ou est en cours. Certains de ces indicateurs sont décrits ci-dessous :

1. Connexion au système et activités excessives dans le système inhabituelles, en particulier à partir de tout identifiant d'utilisateur (compte utilisateur) inactif.
2. Accès à distance excessif ou inhabituel au sein de votre organisation. Cela peut comprendre le personnel ou des fournisseurs tiers.

3. L'apparition de tout nouveau réseau sans fil (Wi-Fi) visible ou accessible depuis votre environnement.
4. Activité inhabituelle liée à des logiciels malveillants, à des fichiers suspects ou à des fichiers nouveaux ou non approuvés et à des programmes exécutables. Cela pourrait se produire sur vos réseaux ou vos systèmes, y compris les systèmes Web.
5. Enregistreurs de clés matérielles ou logicielles connectés ou installés dans les systèmes.
6. Activité suspecte ou inhabituelle dans les systèmes en ligne ou comportement de ceux-ci, comme les sites de commerce électronique.
7. Reçu de commerçant perdu, volé ou égaré ou autre document indiquant le numéro complet de carte de paiement ou le code de sécurité de la carte (numéro à trois ou quatre chiffres imprimé sur la carte).
8. Ordinateurs, disques durs ou autres supports perdus, volés ou égarés qui contiennent des données de carte de paiement ou d'autres données sensibles.

Prévention précoce

Les recommandations suivantes doivent être suivies :

- Avoir recours à l'authentification à deux facteurs ou à toute autre méthode d'authentification plus sécuritaire pour accéder à tout serveur ou logiciel hébergeant des données confidentielles ou sensibles, y compris des renseignements personnels.
- Organiser des simulations d'incidents relatifs aux renseignements personnels.
- Interdire le stockage de documents sur le disque dur de l'ordinateur. Les documents doivent être stockés sur les serveurs infonuagiques appropriés.
- Être à l'affût des tentatives d'hameçonnage, des courriels frauduleux ou des courriels contenant des documents suspects, et demander aux employés d'aviser le responsable de la protection des renseignements personnels dans de tels cas.
- Utiliser des mots de passe variés avec des chiffres, des lettres et des symboles en alternance.
- Veiller à ne pas utiliser le même mot de passe à répétition.
- Obtenir l'approbation d'un représentant de l'entreprise avant de télécharger un logiciel sur l'ordinateur.
- Donner de la formation, au besoin, pour permettre aux employés de mieux repérer les courriels ou les fichiers suspects.
- Valider les informations qui doivent être archivées et celles qui peuvent être détruites.
- Détruire correctement l'information qui n'est plus valide ou nécessaire.
- Envisager d'établir une adresse électronique interne pour que les employés puissent rapidement identifier et signaler les problèmes de cybersécurité, afin d'éviter que les courriels ne soient éparpillés.

- Souscrire à une assurance contre les risques en matière de cybersécurité et les atteintes à la confidentialité.
- Établir un modèle de communication des incidents lorsque l'organisme de réglementation doit être avisé.
-

Niveaux de gravité des incidents

Catégorie	Indicateurs	Champ d'application
1 – Critique	Perte/vol de données, maliciel	Généralisé ou au sein de serveurs critiques, ou perte de données, vol de données, accès ou utilisation non autorisé des données
2 – Élevé	La menace théorique se concrétise	Généralisé ou au sein de serveurs critiques, ou perte de données, vol de données, accès ou utilisation non autorisé des données
3 – Modéré	Hameçonnage par courriel ou infection par propagation générale	Généralisé
4 – Faible	Hameçonnage localisé (souvent une demande financière)	Hôte individuel ou personne

Plan d'action

Événement	Exemple	Procédure à suivre	Niveau de gravité
Perte d'un appareil électronique	L'employé perd ou se fait voler son téléphone cellulaire ou son ordinateur de travail	Procédure A	Faible à élevé
Accès ou utilisation non autorisés	Une personne obtient un accès physique ou informatique non autorisé au réseau, au système ou aux données (envoi d'un courriel au mauvais destinataire)	Procédure B	Faible à élevé
Maliciel	Installation de maliciels (p. ex., virus, ver, cheval de Troie ou autre code)	Procédure C	Critique

Incapacité d'accéder à l'information (rançongiciel)	Type particulier de maliciel qui infecte un ordinateur et affiche des messages demandant le paiement d'une somme d'argent en échange de la récupération du système.	Procédure D	Modéré à élevé
Accès non autorisé malveillant	Vol de données personnelles client/salarié	Procédure E	Critique

Procédure A

1. Aviser le responsable de la protection des renseignements personnels dès que la perte ou le vol se produit.
2. Modifier immédiatement les mots de passe du compte courriel de l'employé et de tout serveur en nuage, et s'assurer que l'authentification à deux facteurs ou toute autre méthode d'authentification plus sûre est activée.
3. Vérifier si les documents contenant des renseignements personnels se trouvaient sur le disque dur de l'ordinateur.
    a. Dans le cas des renseignements personnels :
        i. Existe-t-il un risque de dommage sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        ii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

    b. Si aucun renseignement personnel n'a été compromis, **passez à l'étape 4**.

    c. S'il n'est pas possible de déterminer avec certitude le type de renseignements auxquels la personne a eu accès
        i. Traiter l'événement comme s'il s'agissait de renseignements personnels
        ii. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.

iii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée).

4. Consigner l'événement dans le registre des incidents de confidentialité sans délai.
5. Être à l'affût des événements suspects ou des courriels suspects dans les semaines ou les mois suivant la perte ou le vol de l'appareil.
6. Mettre en œuvre des mesures préventives raisonnables pour toute situation future.

Procédure B

1. Aviser le responsable de la protection des renseignements personnels dès qu'on découvre qu'une personne a eu un accès non autorisé.
2. Bloquer immédiatement l'accès à la personne concernée ou demander à cette personne de supprimer toutes les données obtenues et de fournir une confirmation de destruction.
3. Déterminer quels renseignements ont fait l'objet de l'incident de confidentialité, au besoin, en faisant appel à une entreprise de TI spécialisée.
    a. Dans le cas des renseignements personnels :
        i. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        ii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

    b. Si aucun renseignement personnel n'a été compromis, **passer à l'étape 4**.

    c. S'il n'est pas possible de déterminer avec certitude le type de renseignements auxquels la personne a eu accès
        i. Traiter l'événement comme s'il s'agissait de renseignements personnels
        ii. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        iii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

4. Effectuer un suivi interne pour comprendre comment la situation s'est produite et mettre en œuvre des mesures préventives raisonnables.
5. Consigner l'événement dans le registre des incidents de confidentialité sur-le-champ.

Procédure C

1. Ne prendre aucune mesure (ne jamais entrer de renseignements personnels ou bancaires) et aviser immédiatement le responsable de la protection des renseignements personnels.
2. Le responsable de la protection des renseignements personnels communiquera immédiatement avec un cabinet de TI et suivra ses recommandations.
3. Informer les employés de l'attaque informatique en cours et transmettre sur-le-champ les recommandations du cabinet de TI.
4. Déterminer quelle information a fait l'objet de l'incident de confidentialité avec l'aide du cabinet spécialisé en TI.
    a. Dans le cas des renseignements personnels :
        i. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        ii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

    b. Si aucun renseignement personnel n'a été compromis, **passer à l'étape 5**.

    c. S'il n'est pas possible de déterminer avec certitude le type de renseignements auxquels la personne a eu accès
        i. Traiter l'événement comme s'il s'agissait de renseignements personnels
        ii. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        iii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

5. Effectuer un suivi interne pour comprendre comment la situation s'est produite et mettre en œuvre des mesures préventives raisonnables.

6. Consigner l'événement dans le registre des incidents de confidentialité sur-le-champ.

Procédure D

1. Ne prendre aucune mesure (ne jamais entrer de renseignements personnels ou bancaires) et aviser immédiatement le responsable de la protection des renseignements personnels.
2. Le responsable de la protection des renseignements personnels communiquera immédiatement avec un cabinet de TI et suivra ses recommandations.
3. Avertir les employés qu'une tentative de rançongiciel est en cours et leur demander d'être très vigilants.
4. Évaluer avec l'aide du cabinet de TI si des renseignements personnels ont pu être compromis par le rançongiciel.
    a. Dans le cas des renseignements personnels :
        i. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        ii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

    b. Si aucun renseignement personnel n'a été compromis, **passer à l'étape 5**.

    c. S'il n'est pas possible de déterminer avec certitude le type de renseignements auxquels la personne a eu accès
        i. Traiter l'événement comme s'il s'agissait de renseignements personnels
        ii. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        iii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

5. Effectuer un suivi interne pour comprendre comment la situation s'est produite et mettre en œuvre des mesures préventives raisonnables.
6. Consigner l'événement dans le registre des incidents de confidentialité sur-le-champ.

Procédure E

1. Aviser immédiatement le responsable de la protection des renseignements personnels.
2. Le responsable de la protection des renseignements personnels communiquera immédiatement avec un cabinet de TI et, si nécessaire la police pour déclarer le vol de données.
3. Bloquer l'accès à l'ordinateur pour tous les employés pendant jusqu'à ce qu'un accès sécurisé soit ré-établi et aviser le personnel de la situation et leur dire d'être vigilants.
4. Évaluer avec l'aide du cabinet de TI si des renseignements personnels ont pu être compromis.
    a. Dans le cas des renseignements personnels :
        i. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        ii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

    b. Si aucun renseignement personnel n'a été compromis, **passer à l'étape 5**.

    c. S'il n'est pas possible de déterminer avec certitude le type de renseignements auxquels la personne a eu accès

        i. Traiter l'événement comme s'il s'agissait de renseignements personnels
        ii. Existe-t-il un risque de dommages sérieux? Pour évaluer les dommages, quelle est la sensibilité de l'information concernée, les conséquences appréhendées de son utilisation et la probabilité qu'elle soit utilisée à des fins nuisibles? Il est conseillé de faire appel à des experts pour déterminer s'il y a un risque de préjudice grave.
        iii. En cas de risque de préjudice grave : aviser l'organisme de réglementation et toute personne concernée (à condition qu'aucune enquête ne soit entravée)

5. Effectuer un suivi interne pour comprendre comment la situation s'est produite et mettre en œuvre des mesures préventives raisonnables.
6. Consigner l'événement dans le registre des incidents de confidentialité sur-le-champ.
7. Prendre des mesures raisonnables pour améliorer les mesures de sécurité des TI.
8. Préparer un plan de communication en prévision des questions des clients ou des employés touchés par le vol de données.