

Politique sur la sécurité des données

Description et objet

Les activités de Call2Recycle Canada inc. (« **Call2Recycle** ») dépendent en grande partie de l'information qui est traitée, produite et transmise. Comme toute autre organisation, Call2Recycle peut faire face à des menaces à la confidentialité, à l'intégrité et à la disponibilité de l'information. Ces menaces comprennent le vol d'identité et le vol de renseignements confidentiels, la fraude, l'espionnage industriel, le vol de propriété intellectuelle, l'utilisation, la divulgation et la destruction de renseignements, les défaillances techniques, les événements naturels et l'erreur humaine.

Afin de respecter ses obligations réglementaires et législatives, Call2Recycle adopte, met en œuvre, maintient et applique par les présentes la présente politique de sécurité des données qui établit la mise en œuvre de processus officiels de sécurité des données pour assurer la gestion des risques, la gestion de l'accès et la gestion des incidents relativement à ses renseignements confidentiels et personnels.

Dispositions générales

1. Objectif

- a. Cette politique est l'un des éléments clés pour assurer l'accomplissement de la mission et des objectifs commerciaux de Call2Recycle, pour protéger sa réputation et pour se conformer aux exigences légales, réglementaires et contractuelles applicables.
- b. L'objectif principal de cette politique est de communiquer la détermination et l'engagement de Call2Recycle à gérer les risques liés à la sécurité des données de façon efficace et efficiente. L'approche adoptée vise à identifier les parties prenantes et à définir leurs rôles ainsi qu'à sensibiliser les utilisateurs aux risques liés à la conception et à la mise en œuvre de mesures visant à protéger efficacement la sécurité des ressources d'information.

2. Champ d'application

- a. Cette politique s'applique à toutes les personnes physiques ou morales qui utilisent les ressources de Call2Recycle en matière d'information ou qui y accèdent.
- b. La présente politique s'applique à toutes les données que Call2Recycle détient dans l'exercice de ses fonctions ou qu'elle protège, tout au long de leur cycle de vie, peu importe leur forme, support et emplacement.

3. Lignes directrices

- a. Les principes qui orientent l'approche de Call2Recycle, la répartition des responsabilités et la nature des mesures prises et des moyens déployés sont les suivants :
 - i. Disponibilité
Au mieux de ses capacités, Call2Recycle assure la disponibilité des données qu'elle détient, afin que ces renseignements puissent être consultés en temps opportun et de la manière requise par toute personne autorisée.
 - ii. Intégrité
Au mieux de ses capacités, Call2Recycle assure l'intégrité de l'information afin qu'elle ne puisse pas être détruite ou altérée sans autorisation, et afin que le support d'information offre une stabilité et une durabilité appropriées.
 - iii. Confidentialité
Call2Recycle veille à ce que la divulgation des informations soit limitée aux personnes autorisées à y accéder, garantissant ainsi une stricte confidentialité. À cette fin, Call2Recycle recueille et conserve uniquement les renseignements énoncés dans sa politique de confidentialité; met en œuvre des contrôles d'accès et des profils pour s'assurer que seuls les personnes, les objets ou les entités technologiques identifiés comme ayant droit et autorisés ont accès aux renseignements, conformément aux lois et règlements; et s'assure que l'information, les documents, l'équipement ou les matériaux destinés à l'élimination, déclarés comme biens excédentaires, contenant des données obsolètes ou inutiles ou remises à un fournisseur de services pour leur entretien, recyclage, élimination, ou pour d'autres fins sont traités conformément à la procédure de traitement et d'élimination applicable.
 - iv. Responsabilité
La responsabilité de Call2Recycle s'applique aux biens, processus et systèmes d'information sous la responsabilité ou le contrôle du propriétaire, y compris ceux délégués à un tiers.
 - v. Proportionnalité
Call2Recycle met en place des mesures raisonnables pour garantir la confidentialité, l'intégrité et la disponibilité des ressources d'information, à un coût proportionnel au degré de sensibilité de l'information et aux risques sous-jacents.
 - vi. Sensibilisation

Call2Recycle doit s'assurer que ses employés connaissent les risques et les menaces qui peuvent affecter la sécurité des données, ce qui lui permet de repérer les incidents et les risques potentiels et de comprendre son rôle et ses responsabilités en matière de sécurité des données en développant les aptitudes et les compétences appropriées.

Dispositions particulières

4. Rôles et responsabilités

- a. Dans la présente politique et son application, les mandats suivants sont attribués à différentes parties prenantes :
 - i. Conseil d'administration : adopte la présente politique ainsi que toute modification qui y est apportée.
 - ii. Conseil d'administration : sert de principal forum de consultation sur les questions de sécurité des données pour Call2Recycle; formule des recommandations sur le cadre de gestion, les plans d'action et les examens; formule des propositions d'action en matière de sécurité des données; formule la politique de sécurité des données et ses mises à jour et coordonne sa mise en œuvre; participe à la mise en œuvre des mesures de gestion du risque relatif aux données; élabore et met en œuvre des processus officiels de sécurité des données; formule et met en œuvre des programmes de sensibilisation à la sécurité des données.
 - iii. Responsable de la protection des renseignements personnels : supervise le processus de gestion des risques liés à la sécurité des données et l'application de la présente politique; s'assure de l'adéquation des mesures en matière de sécurité des données en vigueur par rapport aux risques encourus; veille à ce que des mesures soient en place pour réduire les risques liés à la sécurité des données à un niveau jugé acceptable pour l'organisation; est informé des mesures prises par Call2Recycle dans le domaine de la sécurité des données; aide la direction à déterminer les orientations stratégiques et les priorités d'intervention; aide à la mise en œuvre du cadre normatif pour les ressources d'information et les mesures d'atténuation des risques; est le premier répondant de Call2Recycle pour la sécurité des données; est responsable de la déclaration, conformément aux exigences législatives et réglementaires.
 - iv. Service des ressources humaines : effectue, le cas échéant, des vérifications d'antécédents des candidats potentiels avant l'embauche et des membres du personnel impliqués dans la sécurité des données;

s'assure que les responsabilités des parties prenantes en matière de sécurité des données et de respect de la présente politique, ainsi que le cadre normatif des ressources d'information, sont inclus dans les descriptions de poste des membres du personnel; informe les nouveaux employés chez Call2Recycler et obtient d'eux leur engagement à respecter cette politique; impose des sanctions appropriées lorsque les politiques, les règles et le code de conduite en matière de sécurité des données sont violés;

- v. Service des TI : assure la sécurité des ressources d'information, tout au long de leur cycle de vie, en déployant des mesures de sécurité appropriées; élabore, intègre et maintient des mesures de protection appropriées au niveau de sensibilité de l'information concernée, ainsi qu'aux autres activités applicables; les exigences légales, réglementaires ou contractuelles, dans la conduite d'un projet de développement ou l'acquisition d'un système d'information.
- vi. Utilisateurs : se conforment à la présente politique de sécurité des données et à toute directive relative à la sécurité des données et à l'utilisation des ressources d'information; se conforment aux mesures de sécurité en vigueur, sans chercher à les contourner, les annuler ou les modifier.

Mesures administratives et sanctions

5. En cas de violation de la présente politique :

- a. L'utilisateur assumera personnellement les conséquences de toute violation de la présente politique, tout comme toute personne qui, par négligence ou omission, fait en sorte que l'information soit mal protégée.
- b. Tout collaborateur de Call2Recycle qui viole le cadre juridique, la présente politique ou les mesures de sécurité des données qui en découlent est passible de sanctions selon la nature, la gravité et les répercussions de la violation, en vertu de la loi ou des règles disciplinaires internes applicables, pouvant aller jusqu'au congédiement.
- c. De même, toute violation commise par un fournisseur, un partenaire, un invité, un consultant ou une organisation externes fera l'objet de sanctions comme stipulé dans le contrat signé avec Call2Recycle ou en vertu de dispositions juridiques applicables.
- d. Lorsqu'une vérification donne des raisons de croire qu'une loi ou un règlement a été violé, le responsable de la protection des renseignements personnels peut renvoyer le dossier à toute autre autorité compétente pour vérifier s'il existe des motifs de poursuite judiciaire, entre autres choses. Le responsable

de la protection des renseignements personnels peut transmettre à cette autorité tout renseignement recueilli au cours de la vérification ou de l'enquête.

- e. Outre les mesures prévues par les lois, règlements, politiques ou accords, toute violation de la présente politique peut entraîner, sans limitation, les conséquences suivantes, selon la nature, la gravité et les répercussions de l'acte ou de l'omission :
 - i. Annulation des privilèges d'accès aux ressources d'information de Call2Recycle. Cette annulation peut entrer en vigueur sans préavis, selon la nature et la gravité de la violation.
 - ii. L'obligation de rembourser Call2Recycle pour tout montant encouru en raison d'une utilisation non autorisée, frauduleuse ou illicite de ses services ou ressources d'information.

Dispositions finales

6. Révision

Cette politique doit être révisée au besoin, ou conformément aux changements en cours aux obligations législatives et réglementaires, en tenant compte des nouvelles orientations gouvernementales ainsi que de l'évolution des pratiques en matière de sécurité des données.

7. Application et surveillance de la politique

Le responsable de la protection des renseignements personnels est chargé de l'application de la présente politique.

8. Entrée en vigueur

Cette politique entrera en vigueur le 1^{er} juin 2023.