



Enviro Compétences

COMITÉ SECTORIEL DE MAIN-D'ŒUVRE DE L'ENVIRONNEMENT



**POLITIQUE SUR LA SÉCURITÉ
DE L'INFORMATION**

20 juin 2024

Table des matières

PRÉAMBULE.....	1
1. OBJECTIFS	1
2. PORTÉE DE LA POLITIQUE.....	1
3. CLASSIFICATION DE L'INFORMATION.....	1
4. CONTRÔLE D'ACCÈS	2
5. POLITIQUE DE MOTS DE PASSE.....	2
6. MANIPULATION ET STOCKAGE DE L'INFORMATION.....	2
7. UTILISATION DES DISPOSITIFS.....	3
8. UTILISATION ACCEPTABLE.....	3
9. FORMATION ET SENSIBILISATION.....	3
10. RESPONSABILITÉ.....	3
11. APPLICATION DE LA POLITIQUE.....	4
12. MISE À JOUR DE LA POLITIQUE.....	4

Préambule

La politique sur la sécurité de l'information (ci-après la « Politique ») est adoptée en application de la Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (Loi 25), sanctionnée le 22 septembre 2021, modernisant ainsi l'encadrement applicable à la protection des renseignements personnels.

EnviroCompétences est assujéti à la Loi sur la protection des renseignements personnels et doit s'assurer du respect du nouvel encadrement applicable.

1. Objectifs

La présente Politique a pour objet de définir l'engagement d'EnviroCompétences en matière de protection de la confidentialité, de l'intégrité et de la disponibilité des actifs informationnels détenus par EnviroCompétences.

2. Portée de la politique

La présente Politique s'applique à tous les employés, les contractuels, les fournisseurs et toute autre personne tierce ayant accès aux actifs d'information d'EnviroCompétences.

3. Classification de l'information

EnviroCompétences reconnaît que toute l'information n'a pas la même importance. Par conséquent, le classement est regroupé sous trois catégories : confidentielle, à usage interne et public. La classification est basée sur le niveau de risque associé à la divulgation, à l'altération ou à la destruction de l'information. La classification détermine le niveau de protection, d'accès et de manipulation requis pour chaque catégorie d'information.

- **Confidentielle** : Toute information qui, si elle était divulguée ou modifiée, pourrait causer un préjudice financier, juridique ou de réputation à EnviroCompétences. Les exemples incluent les données clients, les informations financières, les stratégies d'entreprise, un renseignement personnel sensible.
- **À usage interne** : Toute information qui n'est pas confidentielle, mais qui est destinée à l'usage interne seulement. Les exemples incluent les mémos internes, certaines informations sur les employés et la documentation de projet.

- Publique : Toute information destinée à une diffusion publique. Les exemples incluent les communiqués de presse, les publications et les politiques de l'entreprise.

Pour l'application des présentes, un renseignement personnel sensible est un renseignement envers lequel il y a un haut degré d'attente raisonnable en matière de vie privée, p. ex. les renseignements médicaux, renseignements bancaires, renseignements biométriques, etc.

4. Contrôle d'accès

L'accès aux actifs d'information est restreint aux utilisateurs autorisés uniquement. EnviroCompétences utilise un système de contrôle d'accès basé sur les rôles (RBAC) qui accorde l'accès aux utilisateurs en fonction de leurs responsabilités professionnelles. Les droits d'accès sont accordés sur une base de besoin de savoir, ce qui signifie que les utilisateurs ne sont autorisés à accéder qu'aux informations dont ils ont besoin pour effectuer leurs tâches professionnelles.

5. Politique de mots de passe

Les mots de passe sont un mécanisme de sécurité essentiel pour protéger les actifs d'information. EnviroCompétences exige que tous les utilisateurs créent des mots de passe solides qui répondent aux exigences suivantes :

- Longueur minimale de 12 caractères ;
- Contient au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial ;
- Changé tous les 90 jours ;
- Les anciens mots de passe ne doivent jamais être réutilisés.

EnviroCompétences encourage le recours à l'utilisation d'un gestionnaire de mot de passe pour la génération de mots de passe solides ainsi que leurs rapatriements dans une base de données sécurisée.

6. Manipulation et stockage de l'information

Tous les actifs d'information, quelle que soit leur classification, doivent être manipulés et stockés de manière appropriée pour éviter l'accès non autorisé, la divulgation ou la perte. Les directives suivantes s'appliquent :

- Les informations confidentielles doivent être stockées dans des endroits sécurisés, tels que des bases de données cryptées ou des fichiers protégés par mot de passe ;
- Les informations à usage interne doivent être stockées dans des dossiers partagés restreints à l'accès des utilisateurs autorisés ;

- Les informations publiques peuvent être stockées dans des dossiers partagés accessibles à tous les utilisateurs ;
- Les actifs d'information doivent être régulièrement sauvegardés pour éviter la perte de données en cas d'incident ;
- Les données sensibles doivent être détruites de manière sécurisée lorsqu'elles ne sont plus nécessaires.

7. Utilisation des dispositifs mobiles

Les dispositifs mobiles, tels que les téléphones intelligents et les tablettes, peuvent contenir des actifs d'information de l'entreprise. Les utilisateurs de ces dispositifs doivent suivre les directives suivantes pour éviter la perte ou la divulgation de données :

- Les dispositifs mobiles doivent être protégés par un mot de passe ou une empreinte digitale pour empêcher l'accès non autorisé ;
- Le stockage d'informations sur les dispositifs mobiles n'est pas autorisé. Le mode de stockage infonuagique implanté par EnviroCompétences doit être utilisé ;
- Les utilisateurs doivent éviter d'utiliser des réseaux Wi-Fi publics non sécurisés pour accéder aux actifs d'information.

8. Utilisation acceptable

Tous les actifs, systèmes et ressources d'information doivent être utilisés uniquement à des fins professionnelles. L'utilisation personnelle n'est pas autorisée et EnviroCompétences contrôle l'installation de logiciels sur ses systèmes.

9. Formation et sensibilisation

EnviroCompétences s'engage à mettre en place des programmes de formation pour éduquer tous les employés, les contractuels, les fournisseurs et toute autre personne tierce ayant accès aux actifs d'information d'EnviroCompétences. Des activités de sensibilisation sont aussi déployées pour mettre de l'avant l'importance de la sécurité de l'information et le rôle que tous jouent dans la protection des actifs informationnels de l'entreprise.

EnviroCompétences s'engage aussi à réaliser à sa discrétion un audit en matière de cybersécurité de manière à lui permettre d'évaluer la sécurité des actifs informationnels détenus ainsi que mettre en plan un plan d'action visant à corriger les vulnérabilités identifiées.

10. Responsabilité

Chaque utilisateur d'EnviroCompétences est responsable de la protection des actifs d'information auxquels il a accès. Tout comportement inapproprié ou violation de cette politique peut entraîner des conséquences disciplinaires, y compris la résiliation de l'emploi et des poursuites judiciaires.

11. Application de la politique

La direction générale ainsi que le responsable de la protection des renseignements personnels sont responsables de l'application de la présente Politique.

Responsable de la protection des renseignements personnels :

Stéphanie Groulx
9501, avenue Christophe-Colomb, bureau 203
Montréal, (QC) H2M 2E3
adjointe_dir@envirocompetences.org

Pour toute demande, question ou commentaire dans le cadre de la présente politique, veuillez communiquer avec le responsable par courriel.

12. Mise à jour de la politique

La présente Politique entre en vigueur le jour de son adoption par le conseil d'administration. Elle sera révisée minimalement aux trois ans par la direction générale conjointement avec le responsable de la protection des renseignements personnels.

La présente Politique peut être révisée en tout temps et devra faire l'objet d'une révision advenant des modifications législatives. Toute modification sera communiquée par le responsable de la protection des renseignements personnels par le biais d'une note de service.

Note : Veuillez noter que l'emploi du genre masculin a pour but d'alléger la présente Politique et d'en faciliter la lecture.