POLITIQUE
DE CONFIDENTIALITÉ ET DE SÉCURITÉ DE L'INFORMATION

Entrée en vigueur le 21 octobre 2021

Le Tremplin, Centre pour personnes immigrantes et leurs familles

39 rue Guenette, Lévis (Québec) G6V 5M9 • 418 603-3512

TABLE DES MATIÈRES

Annexe 1 — Déclaration d'engagement par le personnel, les bénévoles du Tremplin quant au respect des règles de confidentialité et de sécurité de l'information. Document non joint.

1 CONTEXTE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) et de la Directive sur la sécurité de l'information gouvernementale (DSIG) créent des obligations aux organismes publics. Bien que n'étant pas un organisme public, Le Tremplin a choisi de se munir d'une politique de confidentialité et de sécurité de l'information, ci-après appelée : la « Politique »

La Politique permet au Tremplin d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il a créée ou reçue (et dont il est le gardien). Cette information liée à notre clientèle ou à nos ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image du Tremplin

2 DÉFINITIONS

2.1 Actif informationnel

Ce terme désigne tant l'information consignée dans un document que le système qui permet de la prendre en charge. L'actif informationnel peut être constitué de documents technologiques ou de documents en format papier ou encore d'une banque de données. Il peut s'agir aussi d'une technologie de l'information, d'une installation, d'un bien informatique ou d'un ensemble de ces éléments.

2.2 Catégorisation des actifs informationnels

La catégorisation des actifs informationnels en matière de sécurité de l'information est un processus qui permet d'évaluer le degré de sensibilité des renseignements que détient Le Tremplin, dans le but d'en déterminer le niveau de protection, en égard aux risques potentiels aux chapitres de la disponibilité, de l'intégrité, de la confidentialité, de l'authentification et de l'irrévocabilité.

Le Tremplin peut ainsi tenir compte du degré de sensibilité déterminé de ses actifs informationnels pour mettre en œuvre les mesures lui permettant de se conformer à ses obligations légales, d'éviter des pertes financières, d'atteindre ses objectifs en ce qui a trait à la prestation de services et de maintenir et de rehausser la confiance des citoyens et des entreprises à l'égard de ses services.

La catégorisation d'un actif informationnel sert donc de base pour sécuriser le support sur lequel les renseignements sont conservés : papier, numérique, enregistrement, audiovisuel, etc.

2.3 Cycle de vie de l'information

Le cycle de vie de l'information consiste en l'ensemble des étapes que franchit une information depuis sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du Tremplin.

2.4 Document

Ce terme désigne un ensemble d'information qui se trouve sur un support. Elle peut être communiquée au moyen de quelque mode d'écriture que ce soit. Une banque de données doit être considérée comme un ''document'' au fin de l'application de la Politique.

2.5 Gestion des incidents

Le processus de la gestion des incidents permet de préparer l'organisation en vue de la prise en charge d'incidents susceptibles de compromettre la sécurité de l'information, depuis cette prise en charge jusqu'au retour à la normale. Il prévoit, le cas échéant, l'escalade jusqu'aux autorités ministérielles ou gouvernementales. Il prévoit également l'arrimage avec d'autres processus du Tremplin pour les cas spéciaux.

2.6 Incident touchant la sécurité de l'information à portée gouvernementale

Ce terme désigne une conséquence observable de la concrétisation d'un risque quant à la sécurité de l'information à portée gouvernementale. Une intervention concertée sur le plan gouvernemental est alors nécessaire.

2.7 Règle

Sous ce terme général sont compris la présente Politique, les cadres de gestion et directives à venir ainsi que les lois et les règlements en vigueur, notamment la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et le Code criminel.

2.8 Renseignements personnels et confidentiels

Les renseignements personnels se définissent selon l'énoncé qui suit : « Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier ».

La Commission d'accès à l'information du Québec a précisé les trois critères énoncés dans cet article et permettant d'établir qu'un renseignement est personnel ou non :

- Il doit s'agir d'un *renseignement* (l'information doit faire connaître quelque chose);
- Le renseignement *doit concerner* (avoir trait à) une personne physique ;
- Il doit permettre *d'identifier* cette personne (de la reconnaître par rapport à quelqu'un d'autre ou à différentes classes ou catégories d'individus, ou encore de reconnaître sa nature).

2.9 Sécurité physique

La sécurité physique concerne la protection de l'accès physique à des lieux, à de l'équipement, à du matériel, à des documents et à des personnes.

3 CADRE LÉGAL ET ADMINISTRATIF

3.1 La Politique s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne;
- Le Code civil du Québec ;
- La Loi concernant le cadre juridique des technologies de l'information ;
- Le Code criminel;
- La Directive sur la sécurité de l'information gouvernementale;
- La Loi sur les archives

4 CHAMP D'APPLICATION

La présente Politique s'adresse aux utilisatrices et utilisateurs de l'information, c'est–à-dire à tout membre du personnel, peu importe son statut, à toute personne physique ou morale qui, à titre de bénévole, d'élève, de partenaire, de personne-ressource, de prestataire de services, à la clientèle, aux membres, qui utilisent les actifs informationnels du Tremplin ou y ont accès, ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que Le Tremplin détient dans l'exercice de ses fonctions, que sa conservation soit assurée par elle-même ou par un tiers.

5 OBJECTIFS

La présente Politique a pour objectif d'affirmer l'engagement du Tremplin à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le Tremplin doit veiller à :

- La disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;

- L'intégrité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;

- La confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, Le Tremplin, par cette Politique, vise à orienter et à déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information du Tremplin (réf. « Déclaration d'engagement par les membres du personnel quant au respect des règles de confidentialité et de sécurité de l'information »).

6 PRINCIPES GÉNÉRAUX

Les principes qui guident les actions du Tremplin en matière de sécurité de l'information sont les suivants :

a) Reconnaître l'importance de la Politique et de confidentialité et de sécurité de l'information ;

b) S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité ;

c) Reconnaître que l'environnement technologique des actifs informationnels est en changement constant et interconnecté avec le monde ;

d) Protéger le cycle de vie de l'Information ;

e) S'assurer que chaque membre du personnel n'ait accès qu'à l'information confidentielle requise pour accomplir ses tâches (caractère de nécessité);

f) Encadrer l'utilisation des actifs informationnels par un cadre de gestion précis et adapté au rôle de chacun des utilisatrices et utilisateurs ;

g) Sensibiliser et former les utilisatrices et utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle de leurs obligations en la matière.

7 RÔLES ET RESPONSABILITÉS

7.1 Direction générale

La Direction générale du Tremplin est première responsable de la confidentialité et de la sécurité de l'information.

7.2 Comité pour la confidentialité et la sécurité de l'information

Le comité pour la confidentialité et la sécurité de l'information est composé du RSI (responsable de la confidentialité et la sécurité de l'information) et des responsables de la coordination de chaque département. Il a pour objectif d'assister le RSI dans la mise en place et l'application du cadre de gestion de la confidentialité et la sécurité de l'information pour assurer la protection du Tremplin et être conforme à la réglementation. Le comité voit à :

- Voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion :
- S'assure que les exigences en matière de confidentialité et sécurité de l'information sont prises en compte dans tout processus notamment dans nos relations avec tout fournisseur, partenaire, invité, organisme ou firme externe;
- Rapporte au directeur général toute menace ou tout incident afférent à la confidentialité et la sécurité de l'information ;
- Collabore à la mise en œuvre de toute mesure visant à améliorer la confidentialité et la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'actif informationnel ;
- Rapporte au directeur général tout problème lié à l'application de la Politique, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de cette Politique.

7.3 Responsable de la confidentialité et de la sécurité de l'information (RSI)

La personne ayant le rôle de RSI est nommée par la direction générale et relève de celle-ci. Ses principales responsabilités sont :

- S'assurer que tout membre du personnel du Tremplin soit avisé de la Politique de confidentialité et de sécurité de l'information et obtient son engagement au respect de la Politique
- Conseiller le directeur général sur les orientations stratégiques en matière de confidentialité et de sécurité de l'information;
- Assurer la coordination et la cohérence des actions de la sécurité de l'information menées au sein du Tremplin par les intervenantes et intervenants internes et externes ;

- Communiquer et coordonner la mise en œuvre des processus ;
- Rendre compte des incidents auprès du directeur général ;
- S'assurer que le comité assure une surveillance.

7.4 Utilisatrices et utilisateurs

Les utilisatrices et utilisateurs sont les personnes qui ont accès aux renseignements personnels et qui se servent de ces informations dans le cadre de leur travail. Qu'ils soient impliqués dans l'administration, membres du conseil d'administration, membres du personnel ou bénévoles, ils ont l'obligation de protéger les actifs informationnels mis à leur disposition dans le cadre de leurs fonctions. L'information visée est celle que le Tremplin détient dans le cadre de ses activités, que sa conservation soit assurée par elle-même ou par un tiers. Les formats de l'information visée sont numériques et non numériques. À cette fin, les utilisatrices et utilisateurs du Tremplin doivent :

a) Prendre connaissance de la présente Politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer, en signant le document de déclaration d'engagement ;
b) Utiliser, dans le cadre des droits d'accès qui leurs sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés ;
c) Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver ;
d) Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister ;
e) Signaler immédiatement à leur supérieur tout acte dont ils ont connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du Tremplin.

8 DROIT DE REGARD ET SANCTIONS

Lorsqu'une utilisatrice ou un utilisateur contrevient à la présente Politique, au cadre de gestion ou aux directives en découlant, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste.

Le Tremplin a un droit de regard sur l'emploi des actifs informationnels par les utilisatrices et utilisateurs, notamment par le contrôle de leurs droits d'accès à l'information. De ce fait, toute leur expectative en matière de protection de la vie privée s'en trouve restreinte.

Toute personne qui enfreint une règle applicable à la protection ou à la sécurité de l'information s'expose à tout recours permis par la loi et/ou à des sanctions administratives selon le cas.

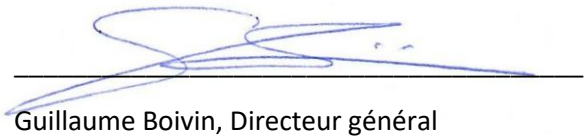
9 DISPOSITIONS FINALES

a. La présente Politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 21 octobre 2021.

b. La ou le RSI s'assure de la mise en œuvre des dispositions de la présente Politique et des directives d'application

c. La présente Politique doit être révisée à l'occasion de changements qui pourraient l'affecter

d. La présente Politique sert de complément au cadre de gestion de la confidentialité et de la sécurité de l'information. Les obligations qui en découlent sont précisées dans des directives.



Guillaume Boivin, Directeur général

Lévis, le 21 octobre 2021

Date