POLITIQUE DE SÉCURITÉ DE L'INFORMATION

1er Janvier 2018

Créé par Jonathan Lavoie
Approuvé par Conseil Décisionnel

TABLE DES MATIÈRES

1 PRÉAMBULE 2

2 INTRODUCTION 2

2.1 Définitions et références 2
2.2 Objectifs 2
2.3 Champs d'application 2
2.3.1 Actifs informationnels 2
2.3.2 Utilisateurs 3
2.3.3 Activités 3

3 CADRE LÉGAL ET ADMINISTRATIF 3

4 PRINCIPES DIRECTEURS 3

5 RÔLES ET RESPONSABILITÉS 4

5.1 Le Conseil Décisionnel 4
5.2 Le directeur technique 4
5.3 Le responsable d'actif informationnel 5
5.4 L'utilisateur 5

6 DISPOSITIONS FINALES 6

6.1 Sanctions 6
6.2 Dérogation 6
6.3 Mise en oeuvre, suivi et révision 6
6.4 Adoption et date d'entrée en vigueur 6

1 PRÉAMBULE

Afin de mener à bien sa mission, Logiciels de Dépannage TowSoft (Ci-après nommé **TowSoft**) produit, emmagasine, traite, communique et élimine de l'information sous plusieurs formes. Cette information possède une valeur légale, administrative, économique ou patrimoniale.

TowSoft reconnait que ces informations, essentielles à ses activités d'administration, de développement et de recherche, doivent faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate, et ce, tout au long de leur cycle de vie. À cette fin, il convient de mettre en œuvre un ensemble cohérent de mesures de sécurité déterminé par une approche de gestion des risques de sécurité.

Ces mesures de sécurité se retrouvent dans différents documents, traitant de la sécurité de l'information, et l'ensemble de ces documents compose le « cadre régissant la sécurité de l'information », ci-après appelé le Cadre.

2 INTRODUCTION

2.1 Définitions et références

La définition des différents termes et abréviations utilisés dans cette politique et dans les autres documents composant le Cadre est consignée dans le Glossaire de sécurité de l'information de TowSoft. Les documents de référence du Cadre sont tous accessibles sur le site web de TowSoft dans la base de connaissance sur https://ww.towsoft.ca/base-de-connaissance.

2.2 Objectifs

La Politique de sécurité de l'information, ci-après appelée la Politique, est avant tout la démonstration du soutien et de l'engagement de TowSoft vis-à-vis de la sécurité de l'information et de sa prise de position ferme et claire quant aux mesures de sécurité à appliquer pour protéger ses actifs informationnels. Elle a été élaborée conformément aux obligations légales et administratives et selon les meilleures pratiques. Elle énonce les principes directeurs, identifie les acteurs concernés, précise leurs rôles et responsabilités en lien avec les principes de gestion de la sécurité de l'information énoncés.

- Les principaux objectifs de la présente Politique sont d'assurer :
- La conformité aux lois, politiques et règlements applicables;
- La disponibilité, l'intégrité et la confidentialité de l'information;
- La confidentialité des renseignements personnels des étudiants, des administrateurs, du personnel enseignant ou administratif de TowSoft et de ses partenaires d'affaires.

2.3 Champ d'application

La Politique s'applique aux actifs informationnels, utilisateurs et activités suivants :

2.3.1 Actifs informationnels

Les actifs informationnels visés sont ceux :

- Appartenant à TowSoft et exploités par elle;
- Appartenant à TowSoft, mais détenus par un partenaire, fournisseur ou autre intervenant;
- Appartenant à un partenaire, fournisseur ou autre intervenant et exploités par lui au profit de TowSoft.

2.3.2 Utilisateurs

Les utilisateurs sont :

- Les clients, les administrateurs, le personnel de développement et de formation ou le personnel administratif de TowSoft;
- Tout consultant, fournisseur, partenaire, organisme ou firme externe appelée à accéder ou à utiliser les actifs informationnels de TowSoft.

2.3.2 Activités

Les activités impliquant la cueillette, la consultation, la production, la transmission, la conservation et la destruction des actifs informationnels peu importe leur support, leur emplacement et le mode d'expression utilisés pour les rendre intelligibles, que ces activités soient conduites dans les locaux de TowSoft ou dans un autre lieu.

3 CADRE LÉGAL ET ADMINISTRATIF

La Politique s'inscrit, entre autres, dans le contexte législatif de :

- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12);
- Code civil du Québec (L.Q., 1991, c. 64);
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- Loi sur les archives (L.R.Q. c. A-21.1);
- Loi sur le droit d'auteur (L.R. 1985, c. C-42);
- Code criminel (L.R.C., 1985, ch. C-46).

4 PRINCIPES DIRECTEURS

Les principes directeurs suivants guident les actions de TowSoft en matière de gestion de la sécurité de l'information.

SEC-P1
S'appuyer sur la famille des normes internationales ISO-27000 qui proposent les meilleures pratiques en cette matière et fournissent à TowSoft des barèmes de comparaison avec des organisations similaires.

SEC-P2
S'assurer de bien connaître les actifs informationnels à protéger ainsi que leur degré de sensibilité et en identifier les responsables.

SEC-P3
Identifier les mesures de sécurité de l'information en fonction du degré de sensibilité des actifs informationnels et des risques et menaces pouvant affecter leur disponibilité, leur intégrité ou leur confidentialité. Ces mesures doivent couvrir la protection des actifs, la détection de tout usage abusif ou inapproprié, l'éradication des menaces et le recouvrement des activités de TowSoft possiblement compromises.

SEC-P4
Voir à ce que le niveau de mesures de sécurité à déployer permette d'atténuer les risques et de les maintenir à un niveau acceptable. Les mesures à déployer doivent également tenir compte du niveau de maturité de l'organisation et être cohérentes dans leur application.

SEC-P5

Protéger rigoureusement les renseignements personnels et s'assurer que les unités qui constituent des fichiers informatisés permanents contenant ce type de données déclarent leur existence au Bureau du secrétaire général, selon les modalités établies.

SEC-P6
Protéger également toute autre information confidentielle, tant dans sa conservation, son utilisation que sa destruction afin que cette dernière respecte les normes d'archivage prescrites par le Bureau du secrétaire général.

SEC-P7
Documenter clairement les attentes en fournissant au personnel et aux clents, un Cadre régissant la sécurité de l'information évolutif qui décrive l'ensemble des mesures, normes, processus, procédures ou guides traitant de ce sujet.

SEC-P8
Faire connaître au personnel et aux clients, les risques et les menaces affectant les actifs informationnels afin que chacun comprenne les attentes de TowSoft en cette matière, puisse reconnaître les incidents et les risques potentiels et développe des habilités et des compétences appropriées. Veiller également à ce que les intervenants comprennent leur rôle et responsabilités en matière de sécurité de l'information.

SEC-P9
Être à même d'effectuer des vérifications de l'existence et de l'efficacité des mesures de sécurité entourant les actifs informationnels, afin de s'assurer du respect des exigences énoncées dans le Cadre régissant la sécurité de l'information.

SEC-P10
Être à même d'effectuer des vérifications ciblées ou encore des enquêtes informatiques lorsque des activités contreviennent aux législations, aux politiques, aux règlements, aux conventions et aux ententes de TowSoft. Ce type d'interventions doit cependant être encadré par un processus rigoureux impliquant des personnes dûment habilitées à les réaliser.

SEC-P11
Se prémunir contre les interruptions de service prolongées en disposant d'un plan de continuité permettant d'assurer la remise en opération des services jugées essentiels en cas de sinistre majeur.

5 RÔLES ET RESPONSABILITÉS

5.1 Le conseil décisionnel

Le Conseil décisionnel a la responsabilité suivante:

- Adopte la Politique et le Règlement.

5.2 Le directeur technique

Le Directeur Technique a les responsabilités suivantes:

- Veille à l'exécution de la Politique;
- Veille à la mise en oeuvre des directives et des règlements;
- Approuve les demandes de dérogation à la Politique, à une directive ou à un règlement;
- Entérine l'identificaiton des responsables d'actif informationnel;
- Prend action, de façon diligente, lorsque des décisions sont requises à la suite d'une situation inattendue liée à la sécurité de l'information et qui exige un redressement rapide;
- Établi les objectifs du programme de sécurité, examine son rendement et son efficacité;
- Procède à des vérifications de conformité de la Politique;
- Approuve les normes et procédures;
- Élabore et propose un programme de sécurité de l'information;
- Rends compte au Conseil Décisionnel en matière de sécurité de l'information;

- Identifie des responsables d'actif informationel et des détenteurs d'actifs informationnel, les besoin de sécurité ainsi que les mesures de sécurité adéquates à mettre en place;
- Partage la vision de TowSoft en matière de sécurité de l'information avec le personnel et les fournisseurs;
- Informe le Conseil Décisionnel de tout manquement de la part d'un employé aux dispositions du Cadre, y compris la présente Politique;

5.3 Le responsable d'actif informationnel

Le rôle du responsable d'actif informationnel est de gérer du point de vue décisionnel et fonctionnel l'actif informationnel sous sa responsabilité de manière à ce qu'elle réponde aux besoins de sécurité identifiés. Il gère également du point de vue opérationnel l'actif informationnel sous sa responsabilité de manière à ce qu'elle réponde aux besoins de sécurité identifiés par le responsable de l'actif informationnel.

Ses principales responsabilités sont :

- Contribuer à l'identification, la localisation et le marquage de l'actif informationnel;
- Évaluer et réviser périodiquement la sensibilité de l'actif informationnel en termes de disponibilité, intégrité, confidentialité et de sa valeur;
- Désigner et réviser périodiquement les détenteurs de l'actif informationnel;
- Identifier les mesures de sécurité à mettre en place et s'assurer de leur bonne application;
- Rendre compte de l'état de la sécurité de l'actif informationnel au gestionnaire responsable de la sécurité de son unité;
- S'assurer de la réalisation des activités suivantes concernant l'actif informationnel :
    - L'analyse et l'évaluation des risques de sécurité;
    - La sensibilisation à la sécurité auprès de ses utilisateurs;
    - La vérification de conformité quant aux mesures mises en place pour le protéger;
    - La gestion d'un incident de sécurité.
- Localise et marque les actifs informationels;
- Protège adéquatement l'actif informationnel par la mise en place, le maintien et la mise à jour des mesures de sécurité identifiées;
- Rend compte de l'état de la sécurité de l'actif informationnel au Directeur Technique;
- Réalise L'analyse et l'évaluation des risques de sécurité;
- Réalise la sensibilisation à la sécurité auprès des utilisateurs;
- Vérifie la conformité quant aux mesures mises en place pour protéger l'actif;
- Gère les incidents de sécurité;
- Informe tout nouveau membre du personnel de sa responsabilité quant au respect de la présente Politique;
- Réalise les enquêtes informatiques;

5.4 L'utilisateur

La responsabilité de la protection des actifs informationnels de TowSoft incombe à tous les utilisateurs. Chacun d'eux est responsable de respecter la Politique ainsi que tous les autres documents du Cadre.

À cette fin, l'utilisateur doit notamment :

- Prendre connaissance et adhérer à la présente Politique;
- S'engager à utiliser les actifs informationnels de manière à respecter le Règlement de sécurité de l'information sur l'utilisation des actifs informationnels.

6 DISPOSITIONS FINALES

6.1 Sanctions

Toute contravention à la présente Politique peut entrainer, en plus des mesures prévues aux législations, règlements, politiques, conventions ou ententes, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste ou de l'omission:

1. L'annulation des privilèges d'accès aux actifs informationnels. L'annulation peut être effectuée sans préavis selon la nature et la gravité du manquement;
2. L'obligation de remboursement à TowSoft de toute somme que cette dernière serait dans l'obligation de défrayer suite à une utilisation non autorisée, frauduleuse ou illicite de ses services ou de ses actifs informationnels.

6.2 Dérogation

Aucune dérogation à la présente Politique n'est permise sans autorisation écrite du directeur technique.

6.3 Mise en oeuvre, suivi et révision

Le directeur technique est responsable de la coordination, de la mise en œuvre et de la mise à jour de la présente Politique qui doivent être réalisées tous les trois ans ou lors de changements significatifs qui pourraient l'affecter.

6.4 Adoption et date d'entrée en vigueur

La présente Politique est adoptée et entre en vigueur à la date de son adoption par le Conseil Décisionnel de TowSoft.