STO Société de transport de l'Outaouais

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

ARTICLE 1 PRÉAMBULE

La présente politique énonce les principes, les droits et les obligations touchant les actifs informationnels de la Société. Elle inclut la catégorisation et la protection de l'information, la gestion de la sécurité informatique ainsi que l'usage des ressources informationnelles par les employés et administrateurs de la Société, dans l'exercice de leurs fonctions.

ARTICLE 2 FONDEMENTS

En vertu de la résolution CA-2019-056, la Société s'est dotée d'une Politique cadre portant sur les communications organisationnelles et la gestion des ressources informationnelles, de laquelle découle la présente politique.

ARTICLE 3 OBJECTIFS

La présente politique regroupe les énoncés de principes généraux et les rôles et responsabilités des intervenants en matière de sécurité des actifs informationnels et de protection des renseignements personnels. Elle affiche une prise de position claire de la Société quant aux mesures de sécurité considérées comme essentielles pour assurer les objectifs suivants :

- la confidentialité de l'information notamment les renseignements personnels relatifs aux clients et au personnel de la Société, en limitant l'accès aux seules personnes autorisées à en prendre connaissance;
- l'intégrité de l'information de façon à ce qu'elle soit adéquate et ne soit pas détruite ou altérée, sans autorisation;
- la disponibilité de l'Information de manière à ce qu'elle soit accessible et utilisable en temps voulu par les entités autorisées;
- l'irrévocabilité afin d'assurer qu'une action est indéniable et clairement attribuée à l'entité qui l'a générée;
- la conformité aux lois et règlements applicables.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

ARTICLE 4 CHAMP D'APPLICATION

La présente politique s'applique à :

- tous les employés de la Société, tous les membres du Conseil d'administration ainsi qu'à toute autre personne dûment autorisée qui a recours aux actifs informationnels de la Société dans l'exercice de ses fonctions;

- l'ensemble des actifs informationnels :

  - appartenant à la Société et exploités par elle ou par un fournisseur de services ou un tiers;

  - appartenant à un fournisseur de services ou un tiers et exploités par lui au profit de la Société.

- toutes les activités impliquant la manipulation ou l'utilisation des actifs informationnels de la Société dans ses locaux, à distance ou dans un autre lieu.

ARTICLE 5 DÉFINITIONS

Actif informationnel

Système d'Information, réseau de télécommunications, banque de données, information numérique, technologie de l'information et documents imprimés générés par les technologies de l'information.

Autorisation

Attribution de droits d'accès par un propriétaire aux actifs informationnels sous sa responsabilité.

Besoin de savoir

Principe stipulant qu'un utilisateur ne devrait avoir accès qu'aux informations nécessaires pour accomplir les tâches liées à son travail.

Catégorisation

Exercice qui permet de déterminer les cotes en termes de disponibilité, intégrité et confidentialité pour chaque actif informationnel.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

Confidentialité

Propriété d'une information à ne pas être divulguée à des personnes non autorisées.

Cycle de vie de l'information

Toutes les étapes d'existence de l'information (la définition, la création, l'enregistrement, le traitement, la diffusion, la conservation et la destruction).

Disponibilité

Propriété d'une information d'être accessible et utilisable au moment voulu par un utilisateur.

Incident lié à la sécurité des actifs informationnels

Évènement indésirable ayant une potentialité non-négligeable de compromettre les activités de la Société et de menacer la sécurité des actifs informationnels.

Information

Renseignement consigné sur un support quelconque.

Information numérique

Information consignée sur un support numérique.

Intégrité

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation.

Mesure de sécurité

Moyen organisationnel, technologique, humain ou juridique permettant d'assurer l'atteinte des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

Plan de continuité des activités

Plan qui vise à redémarrer l'activité d'une organisation le plus rapidement possible avec le minimum de perte de données après un sinistre touchant les systèmes informatiques.

Plan de sauvegarde

Plan contenant les règles relatives à tous les aspects de la sauvegarde informatique.

STO Société de transport de l'Outaouais

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

Procédure

Ensemble des étapes à franchir, des moyens à mettre en œuvre et des méthodes à suivre dans l'exécution d'une tâche.

Propriétaire

Employé cadre à qui est attribuée la responsabilité d'assurer la sécurité d'un actif informationnel.

Registre d'autorité

Registre où sont consignés les propriétaires de chaque actif informationnel.

Registre de catégorisation

Registre où sont consignées les cotes attribuées en termes de disponibilité, d'intégrité et de confidentialité. Ces cotes permettent de déterminer les mesures de sécurité appropriées pour chaque actif informationnel.

Renseignement personnel

Renseignement, quel que soit son support, concernant une personne physique et qui permet de l'identifier.

Sécurité des actifs informationnels

Assurance, par un ensemble de mesures de sécurité, de rencontrer les objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des personnes et des dispositifs et de l'irrévocabilité des actions qu'ils posent.

Séparation des tâches

Principe qui stipule qu'aucun utilisateur ne peut avoir un ensemble de privilèges qui lui permettent d'abuser d'un système.

Super utilisateur

Employé, nommé par un propriétaire d'un actif informationnel, pour administrer cet actif.

Système d'information

Ensemble des outils et moyens pour collecter, stocker, traiter et traiter l'information.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

Technologie de l'information

Technique de l'informatique qui permet d'emmagasiner, de manipuler, de produire et de transmettre l'information sous toutes les formes : texte, image, son, vidéo.

Utilisateur

Employé, membre du Conseil d'administration ou toute personne dument autorisée à accéder aux actifs informationnels.

ARTICLE 6 RÔLE ET RESPONSABILITÉS

6.1 GOUVERNANCE DE LA SÉCURITÉ DE L'INFORMATION

Cette section présente l'organisation fonctionnelle de la sécurité des actifs informationnels de la Société.

6.1.1 Directeur général (DG)

Le directeur général :

- est le premier responsable des actifs informationnels de la Société;
- recommande au Comité de gestion d'approuver les orientations générales en matière de sécurité de l'information, la présente politique et tout changement qui lui est apporté;
- apporte les appuis humains, financiers et logistiques nécessaires pour la mise en œuvre de la présente politique, son application et le bon fonctionnement du cadre de gestion de la sécurité de l'information (CGSI);
- nomme un responsable de la sécurité de l'information (RSI);
- désigne les propriétaires des actifs informationnels;
- s'assure de l'application de la présente politique et de la mise en place de mesures de sécurité permettant de réduire les risques de sécurité de l'information à un niveau acceptable;

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

6.1.2 Responsable de la sécurité de l'information (RSI)

À titre de représentant délégué du directeur général, le RSI gère et coordonne la sécurité de l'information au sein de la Société. Il :

- élabore et met en œuvre le cadre de gestion de la sécurité l'information (CGSI);
- soumet :
  - les orientations, les politiques, les procédures, les priorités d'actions, les éléments de reddition de comptes, pour validation par le Comité de gestion;
  - la présente politique ainsi que ses modifications au Comité de gestion (CG);
- veille à :
  - la mise en œuvre de la présente politique;
  - la sensibilisation et la formation du personnel en matière de sécurité de l'Information;
  - ce que la Société ait un plan de continuité des activités consigné et éprouvé.
- s'assure de :
  - la réalisation de la catégorisation des actifs informationnels ainsi que des analyses de risques en matière de sécurité de l'information lorsque nécessaire;
  - la prise en charge des exigences de sécurité de l'information lors de la réalisation de projets de développement ou de l'acquisition de systèmes d'Information;
- s'informe des besoins en matière de sécurité de l'information auprès des gestionnaires, leur propose des solutions et assure leurs mises en œuvre;
- produit annuellement, et au besoin, les bilans et les rapports relatifs à la sécurité de l'Information au sein de la Société.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

6.1.3 Gestionnaires

Les gestionnaires :

- connaissent les risques de sécurité de l'information des processus d'affaires sous leur responsabilité;
- informent et sensibilisent leur personnel quant au cadre de la gestion de la sécurité de l'information;

- déclarent tout événement qui pourrait représenter une menace sur la sécurité des actifs informationnels de la Société.

- Lorsqu'ils sont propriétaires, les gestionnaires :

  - s'impliquent dans l'ensemble des activités relatives à la sécurité de l'information;

  - catégorisent leurs actifs informationnels et s'assurent que les mesures de sécurité adéquates leur sont appliquées;

  - s'assurent que leurs noms et les actifs informationnels dont ils sont propriétaires sont consignés dans le registre d'autorité et dans le registre de catégorisation;

  - déterminent les règles d'accès à leurs actifs informationnels;

  - autorisent toute dérogation aux règles d'accès de leurs actifs informationnels;

  - sensibilisent les utilisateurs de leurs actifs informationnels aux besoins de sécurité de l'information qu'ils manipulent;

  - analysent, en collaboration avec le RSI, les incidents liés à la sécurité de l'information concernant leurs actifs informationnels et proposent des solutions.

6.1.4 Responsable de l'accès à l'Information et de la protection des renseignements personnels (RAIPRP)

Le RAIPRP a un rôle de conseiller auprès du RSI afin de s'assurer que les mesures de sécurité mises en place permettent de respecter la *Loi sur l'accès aux documents des établissements publics et sur la protection des renseignements personnels*;

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

6.1.5 Super utilisateurs

Les super utilisateurs :

- assurent le fonctionnement sécuritaire des actifs informationnels dont ils ont la responsabilité;
- contrôlent l'accès logique aux actifs informationnels dont ils ont la responsabilité d'utilisation.

6.1.6 Utilisateurs

Les utilisateurs :

- doivent respecter le cadre de gestion de la sécurité de l'information, et déclarent toute violation des mesures de sécurité ou toute anomalie pouvant menacer la sécurité des actifs informationnels de la Société;

- utilisent les actifs informationnels en se limitant aux fins pour lesquelles ils sont destinés et dans le cadre des accès qui leur sont accordés. Lorsqu'un utilisateur a une raison valable d'y déroger, il doit obtenir une autorisation formelle du propriétaire de l'actif informationnel en question.

6.1.7 Direction des ressources informationnelles (DRI)

Le rôle de la DRI à l'égard de la sécurité de l'information est d'agir en tant que fournisseur de service.

Elle :

- assure la mise en application des exigences de sécurité des actifs informationnels de la Société durant tout le cycle de vie de l'information numérique;

- restreint les accès de son personnel aux seules informations indispensables à l'exercice de leurs fonctions;

- collabore à l'élaboration et à la mise à jour du registre d'autorité et du registre de catégorisation;

- contribue à l'élaboration et la mise en œuvre de politiques et procédures en matière de sécurité de l'information;

- assure la surveillance des systèmes et le suivi des journaux;

- assure l'application du plan de sauvegarde et de récupération des données;
- crée et met à jour le registre des incidents;
- élabore et tient à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications;
- collabore avec le RSI et lui fournit le soutien technique nécessaire;
- s'assure de la mise au rebut sécuritaire des supports de l'information.

6.1.8 Direction des ressources humaines (DRH)

La DRH :

- informe tout nouvel employé de ses obligations découlant du cadre de gestion de la sécurité de l'information;
- en collaboration avec le RSI, veille à la formation et la sensibilisation des utilisateurs à la sécurité de l'information;
- collabore avec les propriétaires et la DRI dans l'élaboration et l'application des processus de gestion des accès.

6.1.9 Direction de l'approvisionnement (DAPP)

La DAPP :

- veille à l'intégration des exigences de sécurité de l'information dans les ententes et les contrats.

ARTICLE 7 ÉNONCÉ DE POLITIQUE

7.1 PRINCIPES GÉNÉRAUX DE SÉCURITÉ DES ACTIFS INFORMATIONNELS

La présente politique est fondée sur les énoncés généraux suivants :

- la protection des actifs informationnels de la Société s'appuie sur l'implication continue de tous les employés et les membres du Conseil d'administration;

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

- la gestion de la sécurité des actifs informationnels repose sur une approche globale et intégrée de la gestion du risque. Cette approche tient compte des aspects humains, organisationnels, financiers, juridiques et techniques;

- les mesures de sécurité doivent assurer la confidentialité, l'intégrité, la disponibilité des informations, l'irrévocabilité des actions, ainsi que la continuité des activités.

7.1.1 Organisation de la sécurité des actifs informationnels

- les rôles et les responsabilités relatifs à la sécurité des actifs informationnels doivent être clairement définis et documentés. Cela permet d'établir, puis contrôler la mise en œuvre de la sécurité des actifs informationnels au sein de la Société;

- les activités relatives à la sécurité des actifs informationnels doivent être coordonnées par des intervenants représentatifs des différentes directions de la Société;

- les exigences en matière d'engagements de confidentialité ou de non-divulgation doivent être identifiées et réexaminées régulièrement.

7.1.2 Gestion des actifs informationnels

- les actifs informationnels de la Société doivent être inventoriés;

- un propriétaire doit être désigné pour chaque actif informationnel;

- les actifs informationnels doivent être catégorisés pour indiquer le besoin, les priorités et le niveau souhaité de protection lors de leur manipulation;

- un registre d'autorité et un registre de catégorisation doivent être créés pour y consigner les informations précitées.

7.1.3 Sécurité liée aux ressources humaines

- les utilisateurs doivent connaitre leurs responsabilités et convenir des fonctions qui leur sont assignées afin de diminuer le risque de fraude, de vol ou d'usage inadéquat des équipements et / ou des données;

- un programme continu de sensibilisation et de formation à la sécurité des actifs informationnels doit être mis en place à l'intention des utilisateurs des actifs informationnels de la Société.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

7.1.4 Sécurité physique

- les moyens nécessaires doivent être mis en place pour empêcher tout accès physique non autorisé, tout dommage ou intrusion dans les locaux de la Société;

- les actifs informationnels critiques doivent être hébergés dans des zones sécurisées et protégés physiquement contre les accès non autorisés et les dommages.

7.1.5 Acquisition, développement et exploitation

- la gestion de la sécurité des actifs informationnels doit être incluse et appliquée tout au long du processus menant à l'acquisition, au développement, à l'utilisation, au remplacement ou la destruction d'un actif informationnel par ou pour la Société;

- les politiques et les procédures permettant l'utilisation sécuritaire des actifs informationnels doivent être documentées et mises en œuvre;

- le principe de séparation des tâches doit être appliqué;

- la catégorisation doit être incluse dans la phase spécification des exigences de chaque projet de développement ou d'acquisition afin de déterminer les mesures de sécurité appropriées.

7.1.6 Contrôle d'accès

- l'accès continu aux actifs informationnels par les membres du Conseil d'administration, les usagers, les employés et les autres utilisateurs autorisés, doit être assuré;

- les règles de contrôle d'accès tiennent compte de la politique globale de la sécurité des actifs informationnels et des politiques qui en découlent;

- le principe du besoin de savoir doit être appliqué en tout temps lors de l'attribution d'accès aux informations. Les accès aux actifs informationnels doivent être attribués à l'utilisateur autorisé en fonction de ce qui lui est strictement nécessaire pour l'exécution de ses tâches;

- l'accès aux renseignements personnels par le personnel de la Société doit être autorisé au préalable et contrôlé.

7.1.7 Gestion des incidents liés à la sécurité des actifs informationnels

- un processus de gestion des incidents liés à la sécurité des actifs informationnels (signalement, remontée d'informations et réponse) doit être établi, définissant les mesures à prendre à la réception d'un signalement d'un incident lié à la sécurité des actifs informationnels;

- les utilisateurs doivent être informés de l'existence d'une procédure de signalement des incidents de sécurité des actifs informationnels et d'un responsable à contacter le cas échéant;

- un registre d'incidents doit être créé pour y consigner les incidents liés à la sécurité des actifs informationnels.

7.1.8 Continuité des activités

- un plan de continuité des activités doit être consigné par écrit et éprouvé afin d'assurer la reprise des activités des systèmes d'information nécessaires à la mission de la Société en cas de sinistre majeur (panne électrique prolongée, incendie, cyber-attaque, inondation, etc.).

7.1.9 Conformité

- la conformité aux exigences légales, réglementaires et contractuelles concernant l'utilisation du matériel soumis à des droits de propriété intellectuelle et l'utilisation des logiciels propriétaires, doit être assurée.

ARTICLE 8 SONDAGES

8.1 PRINCIPES APPLICABLES À TOUS LES SONDAGES

8.1.1 Évaluation préalable

Avant d'effectuer tout sondage, une évaluation sérieuse doit être faite de :

- la nécessité de recourir au sondage;

- l'aspect étique du sondage compte tenu, notamment, de la sensibilité des renseignements personnels recueillis et de la finalité de leur utilisation.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

8.1.2 Critère de nécessité

Toute personne ou organisme qui effectue un sondage pour le bénéfice de la Société, le (« Sondeur »), qui implique un partage ou une collecte de données personnelles doit limiter au strict minimum ce partage ou cette collecte. Ainsi, ne peuvent être partagés ou collectés, que les renseignements personnels qui sont absolument nécessaires pour répondre à l'objectif visé par le sondage.

8.1.3 Obligation d'informer

Avant de recueillir un renseignement personnel auprès d'un tiers, le Sondeur doit au préalable s'identifier et informer ce tiers au début du sondage :

- du nom et de l'adresse de la Société;
- de l'usage auquel les renseignements personnels sont destinés et des catégories de personnes qui auront accès à ces renseignements;
- du caractère obligatoire ou facultatif de la demande.

8.1.4 Gestion des résultats

Dans la gestion des résultats du sondage, le Sondeur doit assurer que :

- les renseignements personnels ne seront utilisés qu'aux seules fins pour lesquelles ils ont été recueillis;
- les renseignements personnels ne seront accessibles qu'aux seules personnes pour qui ils sont nécessaires dans l'exercice de leurs fonctions;
- la publication des résultats ne contiendra aucun renseignement personnel;
- les renseignements personnels ne seront pas versés dans d'autres fichiers de renseignements personnels;
- le mandat qui est à l'origine du sondage est respecté.

8.1.5 Destruction des renseignements personnels

Au terme de la réalisation d'un sondage, le Sondeur doit remettre à la Société s'il est un mandataire de cette dernière et doit supprimer le plus rapidement possible les renseignements personnels utilisés ou recueillis lorsque ceux-ci ne sont plus nécessaires pour la réalisation du mandat à l'origine du sondage.

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

ARTICLE 9 TRAITEMENT DES PLAINTES

9.1 PROCESSUS DE TRAITEMENT DES PLAINTES RELATIVES À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

9.1.1 Intérêt requis

Toute personne ou groupe de personnes peut porter plainte relativement à la sécurité des actifs informationnels de la Société, incluant la protection des renseignements personnels.

9.1.2 Transmission de la plainte

Toute plainte doit être transmise à l'adresse suivante : rsi@sto.ca

9.1.3 Contenu de la plainte

Une plainte doit contenir les informations suivantes :

- la date;
- l'identification et les coordonnées du plaignant :
  - nom;
  - adresse;
  - numéro de téléphone;
  - adresse courriel.
- exposé des motifs au soutien de la plainte;
- le cas échéant, tout document et toute autre information pertinente au soutien de la plainte.

9.1.4 Traitement de la plainte

Sur réception d'une plainte, le RSI procède à l'examen de celle-ci. Il doit, si ses vérifications et analyses démontrent que la plainte est fondée, accepter la plainte et prendre les mesures appropriées pour y donner suite. Dans le cas contraire, il doit rejeter la plainte.

9.1.5 Décision

Le RSI transmet sa décision au plaignant par voie électronique au plus tard trente (30) jours suivant la réception de la plainte.

STO Société de transport de l'Outaouais

Politique portant sur la sécurité des actifs informationnels et la protection des renseignements personnels

ARTICLE 10 ABROGATION

La présente politique abroge et remplace la Politique sur la sécurité des actifs informationnels (numéro 3.21).

ARTICLE 11 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur lors de son adoption par le Comité de gestion de la Société.

CETTE POLITIQUE A ÉTÉ ADOPTÉE AU COMITÉ DE GESTION DU 6 FÉVRIER 2024