POLITIQUE DE SÉCURITÉ DE L'INFORMATION ET D'UTILISATION DES TECHNOLOGIES

Dernière version : Adoptée par la Société de transport du Saguenay le 22 septembre 2023.

La présente *Politique de sécurité de l'information et d'utilisation des technologies* (la « **Politique** ») prévoit les mesures et les mécanismes administratifs et de contrôle mis en place ou que mettra en place la Société de transport de Saguenay (la « **STS** ») afin de préserver la sécurité, la confidentialité et l'intégrité des données détenues par la STS.

La sécurité de l'information englobe les solutions techniques et administratives ainsi que les meilleures pratiques en matière d'utilisation des technologies visant à protéger les données détenues par la STS, incluant les renseignements personnels.

La Politique s'applique à la STS. Elle s'applique également à tous les employés de la STS, à toute personne fournissant des services au nom de la STS, à ses affiliés, à ses mandataires, et à toute(s) personne(s) agissant légalement au nom de la STS.

1. PRINCIPES DIRECTEURS

La STS s'engage à mettre en place les mesures appropriées dans le but d'assurer la sécurité des données qu'elle détient, incluant les renseignements personnels, et ce, conformément aux principes directeurs suivants :

1.1 Rôles et responsabilités des intervenants

L'efficacité des mesures de sécurité et de protection des données détenues par la STS, incluant les renseignements personnels, exige l'attribution claire de rôles et de responsabilités aux différents intervenants de la STS permettant une reddition de compte adéquate.

1.2 Formation et sensibilisation

L'aspect humain est un des éléments fondamental de la protection des données détenues par la STS, incluant les renseignements personnels. Il importe donc de sensibiliser le personnel de la STS eu égard aux principes directeurs de sécurité de l'information et aux menaces et aux conséquences d'une atteinte à la confidentialité.

1.3 Relève et continuité

La STS a l'intention d'assurer la continuité des activités nécessaires à la réalisation de sa mission en cas d'incident ou de défaillance majeure de ses systèmes ou procédures ayant un impact sur les renseignements jugés essentiels à la poursuite de ses activités.

2. CADRE DE GESTION

La présente Politique s'articule autour de trois (3) axes fondamentaux de gestion des données, incluant les renseignements personnels, soit la gestion des risques, la gestion de l'accès et la gestion des incidents.

2.1 Gestion des risques

La détermination des mesures propres à favoriser la sécurité et la protection des données détenues par la STS, incluant les renseignements personnels, s'appuie sur l'identification et l'évaluation périodique des risques qui en menacent la confidentialité, l'intégrité ou la disponibilité des données. La STS a mis et continuera à mettre en œuvre des mesures de sécurité et de protection raisonnables, compte tenu de la sensibilité des données visées, de la finalité de leur utilisation, de leur quantité, de leur répartition et du support utilisé.

2.2 Gestion de l'accès

La STS a mis et continuera à mettre en place diverses mesures d'encadrement et de contrôle relatives à l'accès aux données qu'elle traite, par les personnes autorisées, et ce, afin d'en préserver la sécurité, la confidentialité et l'intégrité, en portant une attention particulière à la protection des renseignements personnels.

L'accès aux données détenues par la STS est contrôlé par le directeur de la planification réseau, projets et électrification et des membres de son équipe sous sa supervision (le « **directeur des technologies de l'information** » en fonction des besoins professionnels et nécessaires à l'accomplissement des attributions de chaque employé.

2.3 Gestion des incidents

Le département de la planification réseau, projets et électrification (le « **département des technologies de l'information** » ou « **DTI** »), avec l'assistance du Comité sur l'accès à l'information et à la protection des renseignements personnels (« **CAIPRP** ») et du Responsable de l'accès aux documents et de la protection des renseignements personnels (le « **Responsable** ») assurent la gestion et l'exploitation de l'ensemble des systèmes d'information de la STS en déployant entre autres les mesures appropriées pour minimiser le risque de panne des systèmes et assurer le fonctionnement optimal de ceux-ci. Un plan de réponse aux cyberincidents est également mis en place pour répondre à toute atteinte aux mesures de sécurité de la STS ou à la confidentialité des renseignements personnels sous son contrôle.

3. PROPRIÉTÉ DE LA STS

L'ensemble des systèmes et équipements informatiques de la STS incluant, mais sans s'y limiter, les postes de travail, les serveurs, les ordinateurs portatifs, les postes téléphoniques (statiques et mobiles), les programmes ou logiciels (qu'ils soient installés sur les postes de travail ou sur les serveurs de la STS) et les équipements de réseautique mis à la disposition des employés sont la propriété exclusive de la STS.

4. UTILISATION DES TECHNOLOGIES PAR LES EMPLOYÉS DE LA STS

4.1 Utilisation des équipements informatiques

La STS fournit ou peut fournir à ses employés notamment, mais non limitativement, les équipements informatiques suivants : ordinateurs portables, tablettes, téléphones intelligents, clés USB, lecteurs externes, etc. Lorsqu'ils utilisent les équipements informatiques, les employés doivent respecter les règles suivantes :

- Les employés de la STS doivent préserver l'intégrité et la sécurité des systèmes et des équipements informatiques qui leur sont confiés, et ce, tant à l'intérieur qu'à l'extérieur des locaux de la STS.
- Les employés doivent respecter les contrôles de sécurité mis en place par la STS et utiliser adéquatement les outils et plateformes visant à assurer la sécurité des systèmes informatiques et de l'information, lesquels comprennent notamment l'utilisation d'un mot de passe sécurisé, d'un VPN, etc. De plus, les employés doivent, dans le cadre de leur utilisation d'outils et plateformes de partage de fichiers, prioriser toute procédure sécurisée telle que via la plateforme Microsoft OneDrive, le partage de courriel encrypté ou encore le partage par courriel de fichier avec mot de passe, etc.
- Seuls les logiciels, programmes ou systèmes d'exploitation installés par la STS sont autorisés sur les équipements informatiques fournis par la STS.

- Le téléchargement, l'installation ou l'utilisation de tout autre programme ou logiciel sur les équipements informatiques de la STS doit faire l'objet d'une autorisation préalable et spécifique du DTI, afin d'assurer la protection de la qualité du système informatique;
- Les employés quittant l'organisation verront leurs accès révoqués par le DTI à la fin de la dernière journée de travail;
- Les employés quittant l'organisation devront également remettre sans délai tous les équipements informatiques appartenant à la STS en leur possession.

4.2 Utilisation de la messagerie électronique

La STS fournit à certains de ses employés un compte de messagerie électronique professionnel. Lorsqu'ils utilisent leurs comptes, les employés doivent respecter les règles suivantes :

- Les employés de la STS doivent utiliser l'adresse courriel fournie par la STS pour toute communication effectuée dans le cadre ou à l'occasion de l'exercice de leurs fonctions;
- L'utilisation première du système de messagerie électronique est en principe exclusivement professionnelle. La STS en tolère toutefois l'usage occasionnel à des fins personnelles, à condition que cet usage n'entrave en rien la bonne conduite des affaires de l'organisation ou la productivité de l'employé et qu'il ne constitue pas une infraction à la présente Politique, à toute loi applicable, aux conventions collectives applicables ou à toute autre politique mise en œuvre par la STS. La STS peut, à tout moment, limiter ou interdire cet usage personnel, en modifiant la présente Politique.
- S'il fait usage de cette faculté, l'employé est tenu de supprimer, dans le corps du courriel, toute mention relative à la STS (telle que la signature automatique de la STS) et toute autre indication qui pourrait laisser croire à son destinataire que le message est rédigé par l'employé dans le cadre ou à l'occasion de l'exercice de ses fonctions.
- En raison de la nature confidentielle des affaires de la STS, il est strictement interdit de rediriger le service de réception du compte de messagerie électronique de la STS sur un service de messagerie Web utilisé pour des fins personnelles.
- La taille des fichiers transmis ou reçus en annexe à un courriel est limitée à la valeur par défaut de Microsoft Outlook (taille maximale d'envoi : 35 840 (Ko) et de réception : 36 864 (Ko).
- Les employés doivent vérifier les adresses électroniques associées à tous les courriels reçus afin d'éviter les tentatives d'ingénierie sociale incluant notamment les tentatives d'hameçonnage.
- Dans la mesure du possible, aucune donnée sensible protégée, y compris, mais sans s'y limiter, toute donnée qui se qualifie à titre de renseignement personnel, ne devrait généralement être partagée par courriel. En ce sens,

les employés de la STS doivent plutôt prioriser toute procédure sécurisée alternative telle que via la plateforme Microsoft OneDrive, ou à défaut, utiliser le partage de courriel encrypté ou encore le partage par courriel de fichier avec mot de passe, etc.

- Le compte de messagerie électronique de la STS ne peut être utilisé à des fins prohibées, décrites à l'article 5 ci-dessous.

4.3 Utilisation d'Internet

La STS fournit à certains de ses employés l'accès à l'Internet à des fins professionnelles. Lorsqu'ils parcourent l'Internet, les employés doivent respecter les règles suivantes :

- L'utilisation de l'Internet est en principe limitée à des fins professionnelles. L'exploration de l'Internet à des fins personnelles est toutefois tolérée, mais ne peut en rien porter atteinte au bon fonctionnement du réseau ou à la productivité des employés dans l'exercice de leurs fonctions. Elle se fera généralement en dehors du temps de travail, sous peine de mesures administratives ou disciplinaires conformément à l'article 6 de la présente Politique ou aux dispositions pertinentes de toutes autres politiques ou conventions collectives applicables, ou de toutes autres normes et/ou pratiques de la STS. La STS peut, à tout moment, limiter ou interdire cet usage personnel, en modifiant la présente Politique.
- L'accès à l'Internet ne peut se faire qu'en utilisant son propre compte réseau, c'est-à-dire la combinaison du code d'utilisateur et du mot de passe qui permet à l'employé d'accéder à son poste de travail et au réseau de la STS. Par conséquent, l'utilisation d'un autre compte n'est pas autorisée sans le consentement explicite et écrit du titulaire de ce compte.
- La STS se réserve le droit de bloquer à tout moment et sans avertissement préalable l'accès aux sites dont il juge le contenu illégal, offensant ou inapproprié.
- L'accès à l'Internet ne peut être utilisé à des fins prohibées, décrites à l'article 5 ci-dessous.

5. FINS PROHIBÉES

Il est strictement interdit d'utiliser les équipements informatiques, le système de messagerie électronique, l'accès à l'Internet et, plus généralement, l'infrastructure informatique de la STS en vue :

- de diffuser des informations confidentielles appartenant à la STS, à ses membres, à ses partenaires commerciaux ou aux employés, sauf dans le cadre de la conduite des affaires de la STS ou lorsqu'autorisé par celui-ci.
- de diffuser ou de télécharger, sans autorisation, des données protégées par le droit de la propriété intellectuelle, en violation des lois applicables.

- de télécharger des fichiers en format audio ou vidéo en vue de les visionner hors connexion, ou d'accéder à des stations de radio ou de télévision Internet, sauf dans les cas spécifiquement permis par la STS ou lorsque ceci est nécessaire pour l'accomplissement de son travail.
- d'utiliser ou d'accéder à des sites Web de tiers de toute nature ou des applications de réseaux sociaux, sauf dans les cas spécifiquement tolérés ou autorisés par la STS eu égard à la conduite de ses activités ou lorsque ceci est nécessaire pour l'accomplissement de son travail.
- de visiter des sites de jeux de hasard ou des sites de rencontres personnelles.
- de partager des données ou des fichiers via un service de stockage en nuage (i.e. SkyDrive, Google Drive, etc.), sauf dans les cas spécifiquement autorisés par la STS eu égard à la conduite de ses activités ou lorsque ceci est nécessaire pour l'accomplissement de son travail, auquel cas, le transfert doit être priorisé via la plateforme Microsoft OneDrive, ou sinon via les plateformes Microsoft SharePoint Online, Google Drive ou exceptionnellement via WeTransfer.
- participer dans un but lucratif à une activité professionnelle non autorisée par la STS.
- transmettre des propos qui pourraient être jugés obscènes, abusifs, sexuellement explicites ou menaçants.
- rediriger tout message électronique en l'absence de but professionnel légitime ou dans des circonstances de nature à porter préjudice à la STS ou à l'auteur du message d'origine.
- transmettre un message électronique ou consulter des sites Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment tout message ou site Internet à caractère érotique ou pornographique ou discriminatoire.
- participer à des « chaînes de lettres » et le « spamming » (envoi massif de messages non sollicités).
- participer à des réseaux de communication en direct (« chat »), ou exprimer tout commentaire sur un babillard électronique ou dans un forum de discussions, sauf si cette activité est nécessaire pour l'accomplissement de son travail, ou lorsqu'elle est expressément autorisée par le supérieur immédiat.
- procéder à l'achat de biens ou de services aux frais de la STS, sans autorisation préalable et préférablement écrite.
- utiliser une fausse identité pour tout accès au réseau de la STS ou à l'Internet, ou pour toute transaction électronique.
- utiliser les technologies afin d'émettre, de véhiculer ou de retransmettre des propos politiques partisans, ou dans le cadre de toute activité associée à un parti politique.
- enregistrer sur le système informatique de la STS (en copie locale, sur un serveur « P », etc.) de la documentation (documents, courriels ou autres) contenant des renseignements personnels.

- plus généralement, utiliser les équipements informatiques, le service de messagerie électronique de la STS ou l'Internet dans le cadre d'une activité illégale, quelle qu'elle soit.

Cette énumération n'est pas limitative.

Il est strictement interdit de tenter de désactiver, détruire ou contourner les systèmes de contrôle et de sécurité mis en place par la STS sur les systèmes et équipements informatiques dont elle est propriétaire.

6. MESURES DE CONTRÔLE ET D'INDIVIDUALISATION

6.1 Mesures de contrôle

6.1.1 Contrôle de l'utilisation de l'Internet

La STS peut effectuer en temps réel un contrôle des sites Internet consultés par ses employés.

Lorsque, à l'occasion d'un contrôle en temps réel, d'un contrôle général ou en consultant d'autres sources d'information, la STS constate une anomalie ou a des motifs raisonnables de croire qu'il y a un abus d'utilisation, il se réserve le droit de procéder à l'identification d'un employé, conformément à la procédure décrite à l'article 6.2 ci-dessous.

6.1.2 Contrôle du courrier électronique

Les messages électroniques stockés sur le(s) serveur(s) de messagerie électronique de la STS sont archivés manuellement, en cas de besoin. Les copies archivées de ces courriels seront conservées pendant une période limitée, tel que requis par la loi.

Sur la base d'indices généraux tels, la fréquence, le nombre, la taille et les pièces jointes des messages électroniques, certaines mesures de contrôle pourront être prises par la STS vis-à-vis de ces courriels.

Si la STS a des motifs raisonnables de croire qu'il existe un usage anormal ou interdit du système de messagerie électronique, il procédera à l'identification de l'employé concerné, dans le respect de la procédure décrite à l'article 6.2 ci-dessous.

6.2 Mesures d'individualisation

Par « individualisation », on entend le traitement des données collectées lors d'un contrôle en vue de les attribuer à un employé identifié ou identifiable.

6.2.1 Individualisation directe

La STS procédera à une individualisation directe de l'employé s'il suspecte, constate ou a des motifs raisonnables de croire à :

- la commission de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui.
- la violation de la réputation ou des intérêts économiques, commerciaux et financiers de la STS, auxquels est attaché un caractère de confidentialité.
- une menace à la sécurité et/ou au bon fonctionnement technique des systèmes informatiques et/ou du réseau de l'organisation, incluant le contrôle des coûts afférents, ainsi que la protection physique des installations de l'entreprise.

Le cas échéant, les sanctions appropriées seront prises à l'encontre de l'employé visé, selon les normes et/ou pratiques de la STS, et sans porter préjudice aux droits et recours de la STS pour tous les dommages qu'il pourrait encourir du fait des gestes posés par l'employé visé, conformément à l'article 7 de la présente Politique et/ou à toutes autres politiques ou conventions collectives applicables, ou à toutes autres normes et/ou pratiques de la STS.

6.2.2 Individualisation indirecte

S'il suspecte, constate ou a des motifs raisonnables de croire à un manquement à la présente Politique, la STS pourra en aviser l'ensemble des employés par le biais de la messagerie électronique.

7. MESURES ADMINISTRATIVES ET DISCIPLINAIRES

La STS peut, à titre d'employeur, émettre toutes mesures administratives ou disciplinaires, allant jusqu'au congédiement, à l'encontre d'un employé si celui-ci a contrevenu à la présente Politique, et ce, conformément entre autres à toutes politiques ou conventions collectives applicables, ou à toutes autres normes et/ou pratiques de la STS.

8. DISPOSITION DES CONVENTIONS COLLECTIVES

La présente politique ne peut être interprétée comme allant à l'encontre des dispositions des politiques et des conventions collectives applicables.

POLITIQUE DE DE SÉCURITÉ DE L'INFORMATION ET D'UTILISATION DES TECHNOLOGIES

ANNEXE « A »

Convention d'utilisation des technologies de l'information à la STS

Je soussigné(e) _____, employé(e) de la Société de transport du Saguenay, reconnais avoir pris connaissance de la *Politique de sécurité de l'information et d'utilisation des technologies*, et m'engage à en respecter les diverses dispositions.

_____

NOM (EN LETTRES MAJUSCULES)

_____

FONCTION(S) AU SEIN DE LA STS

_____ _____

SIGNATURE DATE