Service de l'accès et de la protection de l'information
600, rue Fullum, Suite 1.100 UO 3210
Montréal (Québec) H2K 3L6

Notre référence : 2404 536

Le 7 juin 2024

OBJET : Votre demande en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (c. A-2.1) concernant des politiques de gestion

Monsieur,

Nous avons effectué l'étude de votre demande, reçue le 30 avril 2024 et visant à obtenir les documents suivants :

1. **« La directive concernant le droit à l'avocat (…) »**

La politique de gestion **PG-GEN-19** « *Obligations en cas d'arrestation ou de détention et déclaration extrajudiciaire* » a déjà fait l'objet d'une demande d'accès à l'information (n/réf : 2204 462). Nous vous invitons donc à consulter le document qui est diffusé sur le site internet de la Sûreté du Québec à partir du lien suivant : https://www.sq.gouv.qc.ca/wp-content/uploads/2022/07/2022-06-21-droit-avocat.pdf

2. **« La directive concernant les notes du policier (…) »**

La politique de gestion **PG-GEN-39** « *Notes du policier - calepins de notes* » a déjà fait l'objet d'une demande d'accès à l'information (n/réf : 2308 250). Nous vous invitons donc à consulter le document qui est diffusé sur le site internet de la Sûreté du Québec à partir du lien suivant : https://www.sq.gouv.qc.ca/wp-content/uploads/2023/08/2023-08-24-pol-gest-prise-notes-policiers.pdf

3. **« Toute directive liée à l'utilisation d'un téléphone cellulaire (…) »**

Nous vous transmettons, ci-joint en conformité avec la *Loi sur l'accès*, la seule politique de gestion pertinente que nous avons repéré, soit la **PG-RI-02** « *Utilisation des équipements et services technologiques* ».

Si vous avez besoin d'assistance pour comprendre la présente décision, nous vous invitons à contacter le soussigné en écrivant à l'adresse du Service de l'accès et de la protection de l'information : accesdocuments@surete.qc.ca

Vous trouverez, ci-joint, l'avis relatif au recours en révision prévu à la section III du chapitre IV de la *Loi sur l'accès*.

Veuillez agréer, Monsieur, nos salutations distinguées.

ORIGINAL SIGNÉ
Zaki M. Grigancine
Responsable de l'accès aux documents
et de la protection des renseignements personnels

P O L I T I Q U E D E G E S T I O N

	Utilisation des équipements et services technologiques	**PG-RI-02**
	Direction des ressources informationnelles	Dernière mise à jour : 2018-06-05 Révision prévue : 2023-06-05 **RESTREINT** Page **1**

1. Introduction

1.1. Contexte

1.1.1. Dans un environnement où les technologies de l'information occupent une place de plus en plus importante et centrale au travail quotidien, la Sûreté se doit d'aviser ses utilisateurs des comportements attendus de leur part quant à l'utilisation des biens et services technologiques qu'elle met à leur disposition et des actifs informationnels auxquels ces différents outils leur permettent d'accéder.

1.1.2. L'usage des biens et services technologiques en milieu de travail est encouragé par la Sûreté pour :

1.1.2.A. améliorer la qualité des services rendus;

1.1.2.B. accroitre la productivité;

1.1.2.C. accéder à de multiples informations de nature privée ou publique;

1.1.2.D. favoriser la mobilité du personnel dans le cadre de leurs fonctions.

1.2. Objectifs

La présente politique vise à :

1.2.1. encadrer l'utilisation des technologies de l'information en précisant les attentes comportementales pour une utilisation responsable, sécuritaire, judicieuse et éthique;

1.2.2. soutenir la mise en application de la politique-cadre en sécurité de l'information;

1.2.3. sensibiliser et responsabiliser les utilisateurs des outils technologiques en ce qui a trait aux différents enjeux sécuritaires et éthiques associés à l'emploi de ceux-ci.

1.3. Portée

1.3.1. La présente politique concerne l'utilisation de tout bien ou service technologique, notamment ceux permettant la communication ou l'accès à des contenus informationnels (de nature publique ou privée, interne ou externe à la Sûreté).

1.3.2. Comme l'utilisation des outils technologiques implique un aspect sécurité, cette politique de gestion partage des points en commun avec la politique de gestion sur la sécurité de l'information.

1.4. Destinataires

Les employés de la Sûreté et ses mandataires (toute autre personne physique ou morale dûment autorisée à utiliser les outils technologiques de la Sûreté).

2. Définitions

2.1. **Actif informationnel :** l'ensemble des documents et des informations, numériques ou non, des banques de données, des systèmes d'information acquis ou constitués par la Sûreté et sous sa responsabilité ou celle de ses partenaires.

2.2. **Bien et service technologiques** : l'ensemble des biens et services technologiques est nommé ***outils technologiques***. Ils représentent les moyens techniques, matériels ou logiciels associés à l'infrastructure informatique de l'organisation et ayant pour objectif la collecte, le traitement, la transmission et la conservation de l'information. Ces outils permettent aux utilisateurs de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transférer l'information.

D'une façon non exhaustive, sont considérés comme des biens technologiques : les équipements de téléphonie (fixe, mobile, satellitaire), de radiocommunication et de télécommunication (RENIR/RITP/ SIRP), de vidéoconférence et de câblodistribution, les ordinateurs (fixe, portable, véhiculaire, incluant les supports mémoire internes ou amovibles) et leurs périphériques (imprimante, multifonction, numériseur), les serveurs, les logiciels et les programmes.

D'une façon non exhaustive, sont considérés comme des services technologiques : les services de communication et de collaboration (téléphonie, vidéoconférence, radiocommunication, réseaux, Internet, courrier électronique, câblodistribution) de gestion de données (stockage, partage), les applications et systèmes informatiques **(ex. :** banques de données).

2.3. Chiffrement : action qui permet de transformer une communication au moyen d'une clé de chiffrement, afin de la rendre incompréhensible par quiconque ne possédant pas cette clé.

2.4. Jeton de sécurité : élément d'identification et d'authentification qui prend la forme d'une clé USB permettant l'accès au réseau informatique de la Sûreté pour un seul et unique utilisateur.

3. Principes généraux

3.1. Règles d'accès aux outils technologiques

3.1.1. Accès au réseau informatique

3.1.1.A. Toute personne se voit attribuer dès son entrée en poste à la Sûreté, une adresse électronique et l'accès au réseau informatique de la Sûreté, limités à l'exercice de ses fonctions.

3.1.1.B. Pour accéder au réseau informatique de la Sûreté, tout utilisateur doit posséder un jeton de sécurité et un mot de passe associé.

3.1.2. Octroi des biens et attribution des accès aux services technologiques

3.1.2.A. Les biens technologiques et les accès aux services sont attribués en fonction de standards adoptés par l'organisation en concertation avec les responsables des différentes unités organisationnelles. Ces standards sont reliés à la prestation de services attendue, à l'unité concernée et au profil du poste SAGIR de l'utilisateur (corps d'emploi).

3.1.2.B. Les outils technologiques octroyés peuvent être sous la responsabilité d'un utilisateur unique (**ex. :** téléphone cellulaire, jeton de sécurité) ou partagé par plusieurs personnes (répertoires communs, imprimantes multifonctions).

3.1.2.C. Si la nature du travail l'exige, des dérogations aux standards établis sont possibles, mais les demandes en ce sens doivent être transmises à la DRI par l'adjoint du DGA de la grande fonction de laquelle relève l'unité concernée.

3.1.2.D. Toute autre demande ne concernant pas les biens et services standardisés doit être transmise à la DRI par le responsable de la direction concernée.

3.1.3. Retour des biens et retrait des accès aux services technologiques

Les biens doivent expressément être remis à la Sûreté et les accès doivent être retirés lorsque survient un des évènements suivants :

3.1.3.A. changement au niveau de la prestation de services attendue (**ex. :** occuper un nouveau poste ne requérant pas les mêmes accès ou équipements). Les gestionnaires, l'actuel et le précédent de l'utilisateur et la DRI, selon le cas, doivent s'assurer que les accès ainsi que les biens et services technologiques sont retirés ou donnés en accord avec le nouveau niveau de prestation de l'utilisateur;

3.1.3.B. fin du lien d'emploi ou contractuel (**ex. :** départ à la retraite, mutation, fin de contrat);

3.1.3.C. autres considérations à la discrétion de la Sûreté (**ex. :** pour des enjeux de sécurité, mesures disciplinaires, absence de longue durée). La DRI doit toujours être avisée.

3.1.4. Propriété des outils technologiques

Tous les outils technologiques mis à la disposition d'un utilisateur demeurent la propriété de la Sûreté ou de ses partenaires dans le cas où ces outils sont loués.

3.2. Règles d'utilisation des outils technologiques

3.2.1. Utilisation responsable

La Sûreté compte sur la responsabilisation des personnes pour l'utilisation adéquate de leurs outils technologiques.

3.2.1.A. L'utilisateur doit faire bon usage et protéger adéquatement les outils technologiques mis à sa disposition. Ainsi, un utilisateur pourrait être tenu responsable de bris infligés aux outils qui lui sont fournis par la Sûreté à la suite d'un usage abusif, négligent ou inapproprié.

3.2.1.B. Afin d'éviter les bris et les pertes d'équipement, le matériel informatique fixe (**ex. :** ordinateur, appareil multifonction, terminal de câblodistribution) ne doit pas être déplacé sans une autorisation préalable de la DRI.

3.2.1.C. L'utilisateur qui emploie les outils technologiques doit le faire dans le respect :

a. des règles et des pratiques en matière de protection et de sécurité de l'information;

b. des règles et consignes établies dans la Carte des services en ressources informationnelles (**ex. :** consignes à suivre en cas de virus informatique);

c. des règles et procédures d'utilisation telles que définies ou illustrées dans la documentation afférente (**ex. :** guides, aide-mémoires) des différents biens et services technologiques (**ex. :** *Manuel des politiques et des procédures du CRPQ, Guides et procédures SIRP, Code d'éthique sur l'utilisation du RENIR*);

d. de la configuration technologique des outils mis à sa disposition;

e. des mises à jour demandées pour chaque type d'outil.

3.2.1.D. L'utilisateur qui emploie les outils technologiques mis à sa disposition par la Sûreté ne peut le faire pour :

a. tenter d'accéder à des informations pour lesquelles il ne détient pas les autorisations;

b. créer, expédier ou réexpédier tout message électronique ou fichier contenant un élément susceptible d'affecter le fonctionnement des outils mis à sa disposition ou d'un réseau gouvernemental auquel il est relié;

c. télécharger des fichiers lourds (**ex. :** films, grand nombre de pages Web) ou faire des envois massifs de courriels non essentiels ou non reliés à l'exercice de ses fonctions à la Sûreté;

d. divulguer des informations stratégiques de la Sûreté à un tiers non autorisé.

3.2.2. Utilisation sécuritaire

3.2.2.A. En plus du jeton de sécurité et du mot de passe nécessaires pour accéder au réseau informatique de la Sûreté ou de ses partenaires, incluant les différents ministères et organismes du gouvernement du Québec, des codes d'accès ou mots de passe supplémentaires peuvent être requis pour consulter ou utiliser certains actifs informationnels accessibles sur le réseau de la Sûreté. Ces mesures de contrôle des accès visent principalement à assurer la sécurité de ces actifs.

3.2.2.B. Pour bien protéger le réseau informatique de la Sûreté et les actifs informationnels (**ex. :** courriels, systèmes informatisés, bases de données, applications) auxquels il accède, l'utilisateur doit :

a. préserver l'accès à son jeton de sécurité et conserver le caractère confidentiel des codes d'accès et mots de passe dont il est le détenteur exclusif;

Note : Les précautions prises à cet égard permettent d'éviter les dangers d'une usurpation d'identité, le risque de commission d'actes frauduleux ou prohibés sous son nom (numéro de matricule) et protègent les informations auxquelles l'utilisateur a accès.

b. se familiariser et veiller en tout temps au respect des règles et procédures d'utilisation des outils technologiques tels que définis dans les différents documents de référence (**ex. :** procédures, politiques de gestion, guides, aide-mémoires) mis à sa disposition;

c. éviter d'installer toute application ou logiciel sur les outils technologiques de la Sûreté sans en obtenir l'autorisation préalable de la DRI;

d. aviser son gestionnaire dans les plus brefs délais et suivre les consignes, telles que décrites dans la Carte de services en ressources informationnelles ou les documents de référence disponibles sur l'intranet de la Sûreté, dès que survient un incident ou un évènement susceptible d'affecter la sécurité des informations ou des infrastructures technologiques;

Note : Les cas les plus fréquents impliquent le bris, la perte et le vol d'équipement (incluant les biens technologiques personnels pouvant contenir de l'information sensible appartenant à la Sûreté, tels les clés USB ou les ordinateurs personnels), les bris de sécurité, la propagation de logiciels malveillants sur le réseau de la Sûreté (**ex. :** virus ou ver informatique, rançongiciel, cheval de Troie) et la perte ou le vol de données.

e. respecter les règles de catégorisation des informations (*public – restreint – confidentiel – secret – très secret*) et prendre les mesures appropriées selon la cote de confidentialité attribuée (**ex. :** procédure de chiffrement lors de transfert d'informations) pour toute information circulant sur les outils technologiques de la Sûreté. Ces règles sont détaillées dans la *Grille de référence pour la catégorisation de l'information*, disponible sur l'intranet de la Sûreté.

3.2.3. Utilisation raisonnable, judicieuse et éthique

3.2.3.A. Utilisation à des fins personnelles

a. L'utilisation raisonnable des outils technologiques à des fins personnelles est permise (à l'exception des équipements de radio communications strictement réservés au travail policier), notamment parce qu'elle est susceptible de faciliter la conciliation entre les obligations du travail et celles de la vie personnelle. Une utilisation est dite *raisonnable* lorsqu'elle n'engendre pas de coûts additionnels pour la Sûreté.

b. Cette utilisation représente une responsabilisation des utilisateurs en vertu des valeurs organisationnelles de la Sûreté et des règles éthiques de la fonction publique et ne peut être faite au détriment de l'obligation d'assiduité et des devoirs liés à la prestation de travail attendue et doit respecter les autres règles énoncées dans cette politique.

c. En aucun cas, ces outils ne peuvent être utilisés dans le cadre de l'exploitation d'une entreprise externe à la Sûreté, pour un profit personnel, ou pour commettre une fraude, une infraction, ou toute autre action susceptible de poursuites criminelles ou civiles.

Note : Il est important de souligner qu'une utilisation à des fins personnelles non judicieuses de certains outils technologiques (**ex. :** téléphones cellulaires ou tablettes) peut entraîner des coûts additionnels non négligeables pour la Sûreté (**ex. :** frais d'itinérance lors de séjours à l'étranger, téléchargement de vidéos de divertissement). Ceux-ci sont susceptibles d'être réclamés aux utilisateurs. (Voir par. **3.4.1.**)

3.2.3.B. Utilisation éthique

L'utilisateur doit :

a. suivre les règles d'éthique dans l'utilisation du courriel, d'un collecticiel et des services Internet telles que définies dans la *directive gouvernementale* à ce sujet;

b. respecter ses devoirs de réserve, de loyauté et de discrétion dans ses communications;

c. respecter les droits d'auteur ainsi que la propriété intellectuelle (**ex. :** lors d'une communication à l'aide d'un logiciel de présentation ou de traitement de textes, éviter le plagiat en citant expressément les sources, s'il y a lieu) :

i. tous les utilisateurs doivent se conformer aux exigences légales sur l'utilisation des logiciels et progiciels à l'égard desquels il pourrait y avoir des droits de propriété intellectuelle ainsi que sur l'utilisation des produits logiciels propriétaires. L'utilisation des logiciels et progiciels doit être conforme à la Loi sur le droit d'auteur;

ii. les reproductions de logiciels ou de progiciels doivent respecter les licences d'utilisation en vertu du droit d'auteur ou à des fins de copie de sécurité. L'usage de reproductions illicites de logiciels ou progiciels appartenant à la Sûreté est interdit;

iii. le personnel autorisé uniquement peut utiliser les logiciels et progiciels de la Sûreté dans les environnements technologiques autorisés.

3.3. Mises en garde

3.3.1. Toute personne accédant au réseau informatique de la Sûreté consent à la surveillance de ses activités par l'employeur et toute information stockée ou qui circule sur les outils technologiques fournis constitue une information à laquelle la Sûreté a également accès.

3.3.2. L'utilisation de certains outils électroniques de la Sûreté, comme le courriel ou la radiocommunication, peut permettre à des interlocuteurs externes d'identifier la Sûreté. Des risques importants sont alors présents :

3.3.2.A. les informations transmises par l'intermédiaire de ces outils ne sont pas systématiquement protégées. Elles sont susceptibles d'être interceptées, lues, voire modifiées, par une tierce personne;

3.3.2.B. l'identité du transmetteur peut être révélée et les effets potentiels d'une utilisation sans discernement sur la réputation et la crédibilité de l'organisation sont alors bien réels;

3.3.2.C. l'application de mesures de sécurité appropriées (**ex. :** procédure de chiffrement) et une saine dose de prudence ont une importance vitale pour l'organisation. Ainsi, l'utilisateur doit s'abstenir de visiter ou de s'inscrire à, par l'intermédiaire du réseau ou d'une adresse courriel identifiant la Sûreté, des sites à caractère douteux qui pourraient porter préjudice ou nuire à la réputation de la Sûreté.

3.3.3. L'utilisateur doit également savoir que le contenu de tout courriel, reçu ou expédié, lié au domaine d'affaires de la Sûreté est susceptible de faire l'objet d'une demande d'accès à l'information.

3.3.4. Le privilège d'utilisation des outils de communication électronique est susceptible d'être révoqué en tout temps.

3.4. Mesures de contrôle

3.4.1. Des rapports d'activités, notamment d'utilisation des services d'Internet, de téléphonie mobile, ou d'accès aux contenus des systèmes ou bases de données, sont périodiquement ou ponctuellement remis aux gestionnaires. Toute utilisation jugée hors norme ou inappropriée des outils technologiques dans le cadre d'activités professionnelles normales peut faire l'objet de vérifications, d'une enquête interne ou d'une surveillance accrue. Également, les coûts supplémentaires encourus par la Sûreté lors de telles utilisations sont susceptibles d'être réclamés à l'utilisateur.

3.4.2. L'accès à certains sites Internet à caractère litigieux ou haineux demeure en tout temps contrôlé, voire bloqué. Des dérogations peuvent être accordées lorsque le visionnement ou l'accès au contenu de ces sites sont faits dans le cadre du travail (**ex. :** travaux d'enquête sur la pornographie juvénile). Les demandes de dérogations en ce sens doivent être transmises à la DRI par le responsable de la direction concernée.

3.4.3. Tout accès non autorisé ou toute action prohibée sur le réseau informatique de la Sûreté est passible de sanctions pouvant aller jusqu'au congédiement, à la résiliation de contrat ou d'entente ou à des poursuites judiciaires.

3.4.4. La mise en œuvre de ces mesures doit être faite conformément à la loi, notamment à l'égard de la protection de la vie privée ainsi que des renseignements personnels et confidentiels.

Le directeur général par intérim,

Copie conforme à l'original

Yves Morency

Documents reliés à cette politique de gestion

Autres documents :

- Carte des services en ressources informationnelles (disponible sur l'intranet)
- Grille de référence pour la catégorisation de l'information (disponible sur l'intranet)

Directive gouvernementale :

- Directive sur l'utilisation éthique du courriel, d'un collecticiel et des services Internet par le personnel de la fonction publique

Ont été annulées

Politiques de gestion :

- **DIR. GÉN. – 41** Utilisation et administration du jeton de sécurité (2015-09-11)
- **DIR. GÉN. – 58** Règles de conduite sur l'utilisation des outils de communication électronique (2012-01-20)
- **DIR. GÉN. – 60** Mode d'utilisation et gestion du courriel (2015-05-29)
- **TÉLÉCOM – 01** Téléphonie (1999-06-04)
- **TÉLÉCOM – 02** Radiocommunication et équipements de radiocommunication SIRP (2015-12-18)
- **TÉLÉCOM – 21** Service de télémessagerie (boîte vocale) (2001-06-15)