DIRECTIVE DU COMMISSAIRE 226	Entrée en vigueur : 2013-08-19 Examen le plus récent : 2013-08-19 Prochain examen prévu : 2015-08-01

Utilisation des ressources électroniques

ALIGNEMENT DES PROGRAMMES	Services internes
BUREAU(X) DE PREMIÈRE RESPONSABILITÉ	Sous-commissaire principal
VERSION ÉLECTRONIQUE	• http://infonet/cds/cds/226-cd-fra.pdf • http://infonet/cds/cds/226-cd-eng.pdf • http://www.csc-scc.gc.ca/text/plcy/cdshtm/226-cd-fra.shtml • http://www.csc-scc.gc.ca/text/plcy/cdshtm/226-cd-eng.shtml
INSTRUMENTS HABILITANTS	• Politique sur la sécurité du gouvernement du Conseil du Trésor (2012) • Politique d'utilisation des réseaux électroniques du Conseil du Trésor (1998)
BUT	• Assurer l'utilisation appropriée des ressources électroniques du Service correctionnel du Canada (SCC)
CHAMP D'APPLICATION	S'applique aux employés du SCC, ainsi qu'à toute autre personne ayant reçu l'autorisation d'utiliser les ressources électroniques du SCC (ci-après appelés les personnes autorisées)

CONTENU

10 – 12	Surveillance courante
13 – 14	Surveillance accessoire
15 – 16	Surveillance d'activités illégales et de comportements inacceptables
17 – 19	Mesures disciplinaires et sanctions
20	Demandes de renseignements
Annexe A	Renvois et définitions

RESPONSABILITÉS

1. Le dirigeant principal de l'information :

   a. établira les procédures à suivre pour autoriser l'accès aux ressources électroniques du SCC

   b. établira un processus pour veiller à ce que les personnes autorisées reçoivent une formation adéquate et de l'information appropriée sur la bonne utilisation de ces ressources

   c. établira des procédures de surveillance et désignera les personnes qui surveilleront l'utilisation des ressources électroniques.

2. Le directeur, Sécurité de la technologie de l'information :

   a. fournira des directives et des renseignements sur l'interprétation des règles régissant l'utilisation légale et acceptable des ressources électroniques du SCC

   b. veillera à ce que les rapports d'activités illégales ou inacceptables soupçonnées ayant trait à l'utilisation des ressources électroniques du SCC fassent l'objet d'une enquête conformément au paragraphe 6.1.7 de la Politique sur la sécurité du gouvernement du Conseil du Trésor.

3. Les gestionnaires signaleront au directeur, Sécurité de la technologie de l'information, ou au gestionnaire régional, Sécurité de la technologie de l'information au palier régional, toute activité illégale ou inacceptable soupçonnée ayant trait à l'utilisation des ressources électroniques du SCC. L'agent national de sécurité du Ministère et les membres du personnel responsables des activités de sécurité ministérielle au niveau régional en seront informés.

4. Sur la recommandation du directeur, Sécurité de la technologie de l'information, et de l'agent de sécurité du Ministère, les gestionnaires demanderont des conseils juridiques sur toute utilisation des ressources électroniques du SCC soupçonnée d'être illégale ou inacceptable.

5. Les personnes autorisées à utiliser les ressources électroniques du SCC :

   a. se conformeront aux lois, aux politiques du gouvernement, aux directives et à toutes autres instructions publiées par le SCC, sur l'utilisation des ressources électroniques

   b. prendront des mesures raisonnables pour contrôler l'utilisation de leurs mot de passe, code d'utilisateur ou comptes informatiques, et notamment assumeront la responsabilité des poursuites ou des frais découlant d'une utilisation non autorisée des ressources électroniques

   c. utiliseront les dispositifs de sécurité informatique (p. ex., chiffrement, protection antivirus et protection des données) fournis par le SCC

   d. veilleront à ce que leurs communications effectuées au moyen des ressources électroniques du SCC ne fassent pas mal paraître le SCC ou le gouvernement du Canada et soient conformes à toute politique régissant la conduite professionnelle et l'utilisation des médias sociaux

   e. signaleront toute activité illégale ou inacceptable qu'elles soupçonnent à leur(s) gestionnaire(s)

   f. obtiendront des éclaircissements du directeur, Sécurité de la technologie de l'information, en cas de doute quant au caractère acceptable et légal d'une utilisation prévue des ressources électroniques.

UTILISATIONS AUTORISÉES DES RESSOURCES ÉLECTRONIQUES

Utilisation pour le travail officiel

6. Les ressources électroniques doivent être utilisées pour le travail officiel qui comprend, entre autres, la création, la manipulation, le stockage et la transmission des éléments ci-dessous ainsi que leur accès :

   a. les messages électroniques (courriels)

   b. les documents ou renseignements électroniques qui se trouvent sur les ressources électroniques gérées par le SCC

   c. l'information sur le site intranet du SCC (InfoNet)

   d. l'information sur Internet.

Utilisation à des fins personnelles

7. L'utilisation à des fins personnelles des ressources électroniques du SCC par les personnes autorisées n'est permise que dans les circonstances suivantes :

a. elle a lieu pendant le temps destiné aux besoins personnels au cours des heures normales de travail

b. elle n'occasionne pas de coûts additionnels non autorisés au SCC

c. elle respecte les règles de conduite professionnelle et les interdictions relatives au comportement illégal et inacceptable indiquées dans la présente politique et ailleurs

d. elle est effectuée uniquement au moyen de produits informatiques autorisés et installés par le personnel autorisé de la Gestion de l'information/Technologie de l'information du SCC

e. elle n'oblige pas le SCC à assurer une protection accrue de la confidentialité de l'information personnelle stockée, transmise ou traitée, c'est-à-dire au-delà des mesures déjà en place

f. elle permet au SCC de lire le contenu des communications et des fichiers ainsi que d'avoir accès aux renseignements personnels, comme le prévoit la section « Surveillance » de la présente directive.

UTILISATIONS INTERDITES DES RESSOURCES ÉLECTRONIQUES

8. Il est interdit aux personnes autorisées de se servir des ressources électroniques du gouvernement pour :

   a. utiliser, transmettre ou stocker des jeux électroniques ou autres logiciels de divertissement

   b. exploiter ou soutenir leur propre entreprise privée ou pour aider des membres de leur famille, des amis ou d'autres personnes à mener de telles activités, ou

   c. se livrer à des activités illégales ou inacceptables, ou pour stocker ou transmettre des renseignements y afférents, à moins d'en avoir expressément obtenu l'autorisation dans le cadre d'une enquête officielle.

9. L'accès des délinquants aux ressources électroniques du SCC est interdit, sauf lorsqu'il est expressément autorisé par une politique du SCC à des fins approuvées, par exemple un programme d'éducation ou de travail, en conformité avec les règles régissant la protection des renseignements personnels (voir la Directive du commissaire 730 – Affectations aux programmes et paiements aux détenus).

SURVEILLANCE

Surveillance courante

10. Les membres du personnel désignés par le dirigeant principal de l'information effectueront la surveillance courante des ressources électroniques dans le but d'évaluer le rendement, de protéger la disponibilité, l'intégrité, la confidentialité, la valeur et l'objet de l'utilisation des biens du gouvernement ainsi que de veiller à ce que les politiques gouvernementales soient respectées. La surveillance courante peut comporter les tâches suivantes :

    a. établir la taille et le type des fichiers soupçonnés de causer des problèmes

    b. établir les profils d'utilisation

    c. établir l'identité de l'expéditeur et du destinataire prévu ainsi que le sujet de courriels

    d. dépister les virus

    e. effectuer des recherches par mots-clés dans les réseaux, les systèmes informatiques et les supports électroniques de stockage de données.

11. Les ressources électroniques du SCC enregistrent automatiquement l'identité des personnes qui en font usage ainsi que leurs activités.

12. Des copies des fichiers et des courriels (incluant les « ébauches ») sont automatiquement sauvegardées et conservées quotidiennement.

Surveillance accessoire

13. Dans toute la mesure du possible, le SCC cherche à préserver le droit à la vie privée des particuliers. Toutefois, les utilisateurs devraient être conscients que leur utilisation des ressources électroniques du SCC n'est pas privée. Bien que le SCC ne lise habituellement pas les courriels ou le contenu des fichiers, il peut, dans certaines circonstances, surveiller les activités et les comptes d'utilisateurs particuliers, y compris, entre autres, les sessions de connexion, les communications, les courriels et le contenu des fichiers.

14. Toute surveillance individuelle doit être autorisée à l'avance par le directeur, Sécurité de la technologie de l'information, le directeur général, Sécurité, ou le commissaire adjoint, Gestion des ressources humaines, sauf :

    a. dans les cas visés à l'alinéa 15a

    b. dans les cas où une telle surveillance est requise par la loi, ou

c. lorsque ce type de surveillance est nécessaire pour répondre à des situations d'urgence légitimes.

Surveillance d'activités illégales et de comportements inacceptables

15. S'il existe des motifs raisonnables de soupçonner qu'une personne autorisée fait un mauvais usage des ressources électroniques, y compris pendant leur utilisation à des fins personnelles, une surveillance, comportant notamment la lecture du contenu de ses courriels ou autres fichiers, peut être exercée sans préavis dans les circonstances suivantes :

    a. la personne autorisée a volontairement rendu des fichiers électroniques ou des courriels accessibles au SCC ou au public

    b. la surveillance est nécessaire pour protéger l'intégrité, assurer la sécurité et/ou éliminer le risque de responsabilité civile du SCC

    c. il existe des motifs raisonnables de soupçonner que la personne autorisée s'est servi des ressources électroniques du SCC lors de la violation d'une politique du SCC ou autre politique du gouvernement

    d. il existe des motifs raisonnables de soupçonner que la personne autorisée se sert des ressources électroniques pour mener une activité illégale ou inacceptable

    e. la surveillance courante des activités générales et des profils d'utilisation révèle des activités inhabituelles ou excessives dans un compte d'utilisateur, ou

    f. sur réception d'un mandat ou autre instrument juridique provenant d'un organisme d'application de la loi.

16. Les personnes qui sont tenues de lire le contenu de communications électroniques dans le cadre d'une enquête doivent préserver la confidentialité de l'information et n'utiliser celle-ci qu'à des fins autorisées.

MESURES DISCIPLINAIRES ET SANCTIONS

17. Le SCC peut prendre des mesures disciplinaires ou imposer des sanctions dans les cas d'activité illégale et/ou inacceptable ayant trait à l'utilisation de ses ressources électroniques. Les mesures disciplinaires seront proportionnelles à la gravité et aux circonstances de l'activité illégale et/ou inacceptable. Lorsque des mesures disciplinaires s'imposent, il faut consulter les Relations de travail pour que la prise de mesures disciplinaires soit uniforme dans l'ensemble du SCC.

18. Les mesures disciplinaires peuvent inclure :

    a. une réprimande verbale ou écrite

b. des restrictions d'accès aux ressources électroniques

c. examen de la cote de fiabilité ou de l'autorisation de sécurité de la personne en cause

d. la suspension de l'employé ou la cessation d'emploi.

19. Après avoir consulté les Services juridiques, le SCC signalera aux autorités chargées de l'application de la loi toute activité illégale soupçonnée concernant l'utilisation de ses ressources électroniques.

DEMANDES DE RENSEIGNEMENTS

20. Division de la politique stratégique
Administration centrale
Courriel : Gen-NHQPolicy-Politi@csc-scc.gc.ca

Le Commissaire,

Original signé par:
Don Head

ANNEXE A

RENVOIS ET DÉFINITIONS

RENVOIS

Lois connexes

Loi sur l'accès à l'information
Loi sur le droit d'auteur
Loi sur le système correctionnel et la mise en liberté sous condition
Règlement sur le système correctionnel et la mise en liberté sous condition
Code criminel
Loi sur la responsabilité civile de l'État et le contentieux administratif
Loi sur la Bibliothèque et les Archives du Canada
Loi sur la protection des renseignements personnels
Loi sur la protection de l'information

Politiques et publications du Conseil du Trésor

Politique de communication du gouvernement du Canada
Directive sur les pertes de fonds et de biens
Guide de revue de la gestion des renseignements détenus par le gouvernement
Politique sur l'accès à l'information
Politique sur la sécurité du gouvernement
Politique sur la prévention et la résolution du harcèlement
Politique sur la protection de la vie privée
Politique d'utilisation des réseaux électroniques
Politique de télétravail
Code de valeurs et d'éthique du secteur public

Politiques et guides du SCC

DC 041 – Enquêtes sur les incidents
DC 060 – Code de discipline
DC 225 – Sécurité en matière de technologie de l'information
DC 568 – Gestion de l'information et des renseignements de sécurité
DC 568-1 – Consignation et signalement des incidents de sécurité
DC 730 – Affectation aux programmes et rétribution des détenus

Guide de sécurité de l'information
Ordinateurs portatifs – Mise en garde
Manuel des procédures de sécurité ministérielle – Sécurité des renseignements et des biens
Règles de conduite professionnelle au Service correctionnel du Canada

DÉFINITIONS

Activité illégale : actes criminels, infractions à des lois fédérales et provinciales non pénales à caractère réglementaire et actions qui rendent une personne autorisée ou un établissement passible de poursuites au civil. Pour des exemples, voir l'annexe A de la Politique d'utilisation des réseaux électroniques du Conseil du Trésor.

Activité inacceptable : toute activité non conforme aux politiques du SCC, du Conseil du Trésor ou autre politique gouvernementale (pour des exemples, voir l'annexe B de la Politique d'utilisation des réseaux électroniques du Conseil du Trésor), ou non conforme aux restrictions de l'utilisation à des fins personnelles des réseaux, telles qu'elles sont énoncées dans la présente politique et à l'annexe C de la politique du Conseil du Trésor susmentionnée.

Médias sociaux : plateformes Web interactives qui permettent aux participants ayant des profils d'utilisateurs/profils sociaux distincts de créer, partager et interagir avec un contenu créé par les utilisateurs, y compris des textes, des images ainsi qu'un contenu audio et vidéo (p. ex., Facebook, Twitter, YouTube et d'autres technologies de collaboration, comme les sites Wiki, Google Docs).

Personnes autorisées : les employés du SCC ainsi que les entrepreneurs et toute autre personne qui ont reçu d'une autorité du SCC l'autorisation d'accéder aux ressources électroniques du SCC.

Ressources électroniques : tout équipement, système interconnecté ou sous-système d'équipement qui est utilisé pour automatiquement acquérir, stocker, manipuler, gérer, faire circuler, contrôler, afficher, commuter, échanger, transmettre ou recevoir des données ou de l'information. Dans le contexte du présent document, le terme « ressources électroniques » désignent toutes les ressources électroniques qui appartiennent au SCC et sont gérées par lui.

Utilisation à des fins personnelles : utilisation qui ne s'inscrit pas dans le cadre du travail officiel ni d'une autre activité autorisée.