



COMMISSIONER'S DIRECTIVE
DIRECTIVE DU COMMISSAIRE

| | |
|-----------------------------|---|
| Number - Numéro: 226 | Date 2000-05-01 Page: 1 of/de 8 |
|-----------------------------|---|

USE OF ELECTRONIC NETWORKS

UTILISATION DES RÉSEAUX ÉLECTRONIQUES

POLICY OBJECTIVES

1. To promote the lawful and appropriate use of Correctional Service Canada (CSC) electronic network.
2. To encourage authorized individuals to use the electronic network to carry out the legal mandate and Mission of the CSC in accordance with Treasury Board policy.

AUTHORITY

3. This policy is issued pursuant to Treasury Board Policy on the Use of Electronic Networks, February 12, 1998.

SCOPE

4. Authorized users are CSC employees and those contractors, consultants or third parties who are granted access to CSC's electronic network.
5. Offenders shall not be authorized to access CSC's electronic network.
6. This policy applies to activities and conduct performed by individuals authorized to use CSC's electronic network. Use of networks includes, but is not limited to:
 - a. creating and transmitting electronic mail messages (e-mail);
 - b. creating, transferring, accessing and manipulating electronic records;
 - c. accessing information contained on the Infonet or the Internet (World Wide Web);
 - d. posting information on the Internet.

OBJECTIFS DE LA POLITIQUE

1. Promouvoir l'utilisation légitime et appropriée du réseau électronique du Service correctionnel du Canada (SCC).
2. Encourager les personnes autorisées à utiliser le réseau électronique pour réaliser le mandat légal et la Mission du SCC conformément à la politique du Conseil du Trésor.

INSTRUMENT HABILITANT

3. La présente politique est émise conformément à la « Politique d'utilisation des réseaux électroniques » du Conseil du Trésor, datée du 12 février 1998.

PORTÉE

4. Les utilisateurs autorisés sont les employés du SCC et les contractuels, consultants ou tiers à qui est accordé l'accès au réseau électronique du SCC.
5. Les délinquants ne sont pas autorisés à avoir accès au réseau électronique du SCC.
6. La présente politique porte sur les activités et la conduite des personnes autorisées à utiliser le réseau électronique du SCC. L'utilisation des réseaux comprend, entre autres :
 - a. la création et la transmission de messages par courrier électronique (courriel);
 - b. la création, le transfert et la gestion de dossiers sur support informatique, ainsi que l'accès à ces derniers;
 - c. l'accès à de l'information contenue sur l'Infonet ou l'Internet (World Wide Web);
 - d. la publication d'information sur l'Internet.



APPROVED USES OF ELECTRONIC NETWORKS

- 7. Electronic networks shall be used for official business.
- 8. The personal use of CSC's electronic network by authorized individuals is permitted only when such use:
 - a. occurs on the individual's personal time within normal working hours;
 - b. does not incur any direct cost to the CSC;
 - c. observes the prohibitions against unlawful and unacceptable conduct outlined elsewhere in this policy;
 - d. employs authorized applications installed by CSC authorized IM/IT personnel.
- 9. Electronic networks shall not be used to operate games or other entertainment software under any circumstances.

UNLAWFUL AND UNACCEPTABLE CONDUCT

- 10. CSC's electronic network shall not be used to conduct any unlawful activity, including criminal offences. A non-comprehensive list of unlawful activities is included in Annex "A".
- 11. CSC's electronic network shall not be used to conduct any activity that, while legal, is unacceptable. A non-comprehensive list of unacceptable activities is included in Annexes "B" and "C".

**UTILISATION APPROUVÉE
DES RÉSEAUX ÉLECTRONIQUES**

- 7. Les réseaux électroniques doivent être utilisés pour le travail officiel.
- 8. L'utilisation à des fins personnelles du réseau électronique du SCC par les personnes autorisées n'est permise que dans les cas suivants :
 - a. elle a lieu pendant le temps consacré aux activités personnelles durant les heures normales de travail;
 - b. elle n'entraîne pas de coûts directs pour le SCC;
 - c. elle respecte les interdictions relatives au comportement illégal et inacceptable dont les grandes lignes sont indiquées ailleurs dans la présente politique;
 - d. elle est effectuée à l'aide de logiciels autorisés, installés par le personnel autorisé en GI-TI.
- 9. Les réseaux électroniques ne doivent en aucun cas servir à exécuter des logiciels de jeu ou de divertissement.

COMPORTEMENT ILLÉGAL ET INACCEPTABLE

- 10. Le réseau électronique du SCC ne doit pas être utilisé pour se livrer à des activités illégales, y compris des infractions criminelles. Une liste non exhaustive des activités illégales est incluse à l'annexe A.
- 11. Le réseau électronique du SCC ne doit pas être utilisé pour mener des activités qui, tout en étant légales, sont inacceptables. Une liste non exhaustive des activités inacceptables est incluse aux annexes B et C.



**RESPONSIBILITIES OF INDIVIDUALS
AUTHORIZED TO USE CSC ELECTRONIC
NETWORK**

- 12. Individuals authorized to use CSC's electronic network are responsible for abiding by the law and government policies as set out by Treasury Board (Use of Electronic Networks) and the CSC by:
 - a. taking reasonable measures to control the use of their password, user identification or computer accounts;
 - b. being aware of information technology security issues as published from time to time by the Manager of Information Technology Security;
 - c. using information technology security features (encryption, virus protection) provided by the CSC;
 - d. communicating in a manner that reflects positively on the standards of the CSC;
 - e. obtaining clarification from the Director, Information Management/Information Technology Strategic Support when in doubt whether a planned use is acceptable and lawful according to this policy.

DISCIPLINARY MEASURE AND SANCTIONS

- 13. CSC will report suspected unlawful use of its electronic network to law enforcement authorities following consultation with its legal advisors.
- 14. CSC may take disciplinary measures or sanctions in cases of unlawful and/or unacceptable use of its network. Disciplinary measures will be commensurate with the seriousness and circumstances of the incident.

**RESPONSABILITÉS DES PERSONNES
AUTORISÉES À UTILISER LE RÉSEAU
ÉLECTRONIQUE DU SCC**

- 12. Les personnes autorisées à utiliser le réseau électronique du SCC sont tenues de respecter la loi ainsi que les politiques gouvernementales telles que celles énoncées par le Conseil du Trésor (utilisation des réseaux électroniques) et le SCC :
 - a. en prenant des mesures raisonnables pour contrôler l'utilisation de leurs mot de passe, code d'utilisateur ou comptes;
 - b. en prenant connaissance des questions de sécurité relatives à la technologie de l'information, publiées de temps à autre par le gestionnaire de la Sécurité de la technologie de l'information;
 - c. en utilisant les dispositifs de sécurité informatique (chiffrement, protection contre les virus) fournis par le SCC;
 - d. en communiquant de manière à projeter une image favorable des normes du SCC;
 - e. en obtenant des éclaircissements du directeur du Soutien stratégique de la gestion de l'information-technologie de l'information en cas de doute quant au caractère acceptable et légal d'une utilisation prévue des réseaux, conformément à la présente politique.

MESURES DISCIPLINAIRES ET SANCTIONS

- 13. Après avoir consulté ses conseillers juridiques, le SCC signalera l'utilisation présumée illégale de son réseau électronique aux autorités chargées de l'application des lois.
- 14. Le SCC peut prendre des mesures disciplinaires ou imposer des sanctions dans l'éventualité d'une utilisation illégale ou inacceptable de son réseau. Les mesures disciplinaires seront proportionnelles à la gravité et aux circonstances de l'incident.



15. Disciplinary measures may include:
- a. an oral or written reprimand;
 - b. limitations on access to the electronic network;
 - c. suspension or termination of employment.
16. Sanctions to be taken against contractors or other individuals authorized to use CSC's network shall be specified in a conditions of use agreement.

MANAGEMENT RESPONSIBILITIES

17. Managers are responsible for reporting instances of suspected unlawful or unacceptable uses of CSC's electronic network to the Manager of Information Technology Security or equivalent.
18. The Manager of Information Technology Security or equivalent shall investigate reports of suspected unlawful or unacceptable uses of CSC's electronic network in accordance with Chapter 2-1, Section 16 of the Government Security Policy.
19. The Assistant Commissioner, Corporate Services or Regional Deputy Commissioner is responsible for seeking legal advice in cases of suspected unlawful or unacceptable uses of CSC's electronic network.
20. The Director General, Information Management Services is responsible for:
- a. providing training or information on using networks effectively and efficiently;
 - b. establishing procedures for granting access to CSC's electronic network;
 - c. establishing procedures for granting access to the Internet via CSC's electronic network;

15. Les mesures disciplinaires peuvent inclure :
- a. une réprimande verbale ou écrite;
 - b. des restrictions d'accès au réseau électronique;
 - c. la suspension de l'employé ou la cessation d'emploi.
16. Les sanctions imposables aux contractuels et aux autres personnes autorisées à utiliser le réseau du SCC seront prévues dans l'entente concernant les conditions d'utilisation.

RESPONSABILITÉS DES GESTIONNAIRES

17. Il incombe aux gestionnaires de signaler au gestionnaire de la Sécurité de la technologie de l'information, ou au titulaire d'un poste équivalent, les cas d'utilisation présumée illégale ou inacceptable du réseau électronique du SCC.
18. Le gestionnaire de la Sécurité de la technologie de l'information, ou le titulaire d'un poste équivalent, est tenu d'enquêter sur les cas qui lui sont signalés d'utilisation présumée illégale ou inacceptable du réseau électronique du SCC, conformément à la section 16 du chapitre 2-1 de la Politique du gouvernement concernant la sécurité.
19. Il incombe au commissaire adjoint des Services corporatifs ou au sous-commissaire régional d'obtenir des conseils juridiques sur les cas d'utilisation présumée illégale ou inacceptable du réseau électronique du SCC.
20. Il incombe au directeur général des Services de gestion de l'information :
- a. d'offrir de la formation ou des renseignements sur l'utilisation efficace et efficiente des réseaux;
 - b. d'établir les règles régissant l'autorisation d'accès au réseau électronique du SCC;
 - c. d'établir les règles régissant l'autorisation d'accès à l'Internet via le réseau électronique du SCC;



| | |
|-----------------------------|--|
| Number - Numéro: 226 | Date 2000-05-01 Page: 5 of/de 8 |
|-----------------------------|--|

- d. approving the individuals who are authorized to monitor the use of electronic networks.
- 21. The Director, Information Management/ Information Technology Strategic Support is responsible for:
 - a. providing information on this policy;
 - b. providing information on the interpretation of lawful and acceptable use of CSC's electronic network.
- 22. Directors and Managers (at National and Regional Headquarters) and heads of operational units are responsible for endorsing individual applications for access to the global Internet (World Wide Web). Applications shall be supported by a business case.

MONITORING

- 23. Electronic networks may be monitored for operational reasons to determine whether the networks are operating efficiently, to isolate and resolve problems, and to assess compliance with government policy. In addition, periodic and random checks of the networks for specific operational purposes can occur and the resulting information can be analyzed.
- 24. Normal routine analysis does not involve reading the content of electronic mail or files. However, if due to routine analysis or a complaint, there are reasonable grounds to believe that an authorized individual is misusing the network, the matter shall be referred for further investigation and action that may involve special monitoring and/or reading the content of individual electronic mail and files.

- d. d'approuver la désignation des personnes autorisées à surveiller l'utilisation des réseaux électroniques.
- 21. Le directeur du Soutien stratégique de la gestion de l'information-technologie de l'information est chargé :
 - a. de fournir des renseignements sur la présente politique;
 - b. de fournir des renseignements sur l'interprétation des règles régissant l'utilisation légale et acceptable du réseau électronique du SCC.
- 22. Il incombe aux directeurs et aux gestionnaires (aux administrations centrale et régionales) ainsi qu'aux chefs des unités opérationnelles d'approuver les demandes d'accès à l'Internet (World Wide Web). Les demandes doivent être appuyées par une analyse de rentabilisation.

SURVEILLANCE

- 23. Les réseaux électroniques peuvent être surveillés à des fins opérationnelles afin de déterminer s'ils fonctionnent de façon efficiente, pour cerner et régler les problèmes et pour vérifier si la politique est respectée. En outre, des vérifications au hasard des réseaux peuvent être menées de façon périodique pour des motifs opérationnels précis. Les renseignements ainsi obtenus peuvent être analysés.
- 24. Les analyses de données ne nécessitent généralement pas la lecture du contenu des messages envoyés par courrier électronique et des fichiers de données. Toutefois, si, à la suite d'une analyse ordinaire ou d'une plainte, il existe des motifs raisonnables de croire qu'une personne autorisée utilise le réseau à mauvais escient, le cas sera signalé en vue d'une enquête approfondie et de la prise de mesures particulières pouvant inclure la lecture du contenu des messages envoyés par courrier électronique et des fichiers de données.



25. Whenever individuals involved in an investigation are obliged to read the content of electronic communications, they must keep the information confidential and use it only for authorized purposes. This investigation must be conducted in accordance with the *Charter of Rights and Freedoms*, the *Privacy Act*, and the *Criminal Code*.

Regular Monitoring

26. Regular monitoring will occur for work-related reasons only to assess network performance, to protect government resources and to ensure compliance with government policies.

27. Regular monitoring may involve:

- a. identifying the size and type(s) of file(s) suspected of causing problems;
- b. identifying patterns of usage;
- c. determining the originator, intended recipient and subject line of e-mail messages;
- d. testing for viruses;
- e. key word searches of files on network servers or on computer storage devices.

Incidental Monitoring

28. CSC's electronic network automatically logs the identity of individuals and their activities while on the network.

25. L'employé qui doit lire le contenu des communications électroniques dans le cadre d'une enquête à laquelle il participe ne peut divulguer les renseignements qui y figurent qu'à des fins autorisées. L'enquête doit être menée conformément à la *Charte canadienne des droits et libertés*, à la *Loi sur la protection des renseignements personnels* et au *Code criminel*.

Surveillance régulière

26. La surveillance régulière est effectuée uniquement pour des motifs liés au travail dans le but d'évaluer le rendement du réseau, de protéger les ressources de l'État et de vérifier si les politiques gouvernementales sont respectées.

27. La surveillance régulière comporte :

- a. la détermination de la taille et du type des fichiers soupçonnés de causer les problèmes;
- b. la détermination des tendances d'utilisation;
- c. la détermination des expéditeurs, des destinataires et de l'objet des messages de courrier électronique;
- d. des tests antivirus;
- e. des recherches de mots clés dans les fichiers des serveurs du réseau ou dans la mémoire de l'ordinateur.

Surveillance accessoire

28. Le réseau électronique du SCC enregistre automatiquement l'identité des personnes et leurs activités dans le réseau.



29. Copies of files and e-mail records (including "deleted" records) are automatically backed up and retained on a daily basis. This information may be accessible under the *Access to Information Act* and *Privacy Act*, subject to exemptions under those Acts.

29. Des copies de fichiers et d'enregistrements de courrier électronique (y compris ceux « supprimés ») font l'objet d'une sauvegarde automatique et sont conservées quotidiennement. On peut avoir accès à cette information en vertu de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*, sous réserve des exceptions prévues par ces lois.

**Monitoring for Unlawful Activity/
Unacceptable Conduct**

30. If there are reasonable grounds to believe that an authorized individual is misusing the network, monitoring without notice, including viewing the content of individual electronic mail records or other files, may occur.

**Surveillance d'activités illégales ou
de comportements inacceptables**

30. S'il existe des motifs raisonnables de croire qu'une personne autorisée fait un mauvais usage du réseau, il se peut que des mesures de surveillance sans préavis soient prises à son égard, notamment la consultation du contenu de ses fichiers de courrier électronique ou d'autres fichiers.

AUDIT

31. Compliance with this policy shall be subject to regular internal audits.

VÉRIFICATION

31. Des vérifications internes seront menées périodiquement afin de vérifier si la présente politique est respectée.

RELATED LEGISLATION AND POLICIES

- 32. - *Financial Administration Act*;
- *Access to Information Act*;
- *Privacy Act*;

- *Charter of Rights and Freedoms*;
- *National Archives of Canada Act*;
- *Official Secrets Act*;
- *Criminal Code*;
- *Export and Import Permits Act*;

- *Crown Liability and Proceedings Act*;

- *Copyright Act*;
- *Trade-Marks Act*;
- *Patent Act*;
- *Canadian Human Rights Act*;
- *Official Languages Act*.

LOIS ET POLITIQUES CONNEXES

- 32. - *Loi sur la gestion des finances publiques*;
- *Loi sur l'accès à l'information*;
- *Loi sur la protection des renseignements personnels*;
- *Charte canadienne des droits et libertés*;
- *Loi sur les Archives nationales du Canada*;
- *Loi sur les secrets officiels*;
- *Code criminel*;
- *Loi sur les licences d'exportation et d'importation*;
- *Loi sur la responsabilité civile de l'État et le contentieux administratif*;
- *Loi sur le droit d'auteur*;
- *Loi sur les marques de commerce*;
- *Loi sur les brevets*;
- *Loi canadienne sur les droits de la personne*;
- *Loi sur les langues officielles*.



CROSS-REFERENCES

33. Treasury Board Policy and Publications

- Conflict of Interest and Post-Employment Code for the Public Service;
- Harassment in the Workplace Policy;
- Government Security Policy;
- Government Communications Policy;
- Government of Canada Internet Guide;
- Management of Government Information Holdings Policy;
- Access to Information Policy;
- Privacy and Data Protection Policy;
- Policy on the Use of Electronic Networks;
- Telework Policy;
- Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown.

34. CSC Policy

- Security Manual – Information Technology Security;
- Information Classification and Scheduling Plan;
- Code of Discipline;
- Standards of Professional Conduct.

Commissioner,

RENOIS

33. Politiques et publications du Conseil du Trésor

- Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique;
- Politique sur le harcèlement en milieu de travail;
- Politique du gouvernement concernant la sécurité;
- Politique du gouvernement en matière de communications;
- Guide d'Internet du gouvernement du Canada;
- Politique sur la gestion des renseignements détenus par le gouvernement;
- Politique sur l'accès à l'information;
- Politique sur la protection des renseignements personnels;
- Politique d'utilisation des réseaux électroniques;
- Politique sur le télétravail;
- Politique sur les pertes de fonds et infractions et autres actes illégaux commis contre la Couronne.

34. Politiques du SCC

- Manuel de sécurité – Sécurité des technologies de l'information;
- Plan de classification et calendrier de conservation de l'information;
- Code de discipline;
- Règles de conduite professionnelle.

Le Commissaire,

Original signed by / Original signé par :

Ole Ingstrup



UNLAWFUL ACTIVITY (Non-Exhaustive List of Examples)

1. For the purposes of this policy, "unlawful activity" is interpreted broadly to include actions that could result in sanctions of different kinds in a court of law.
2. Some activity gives rise to criminal offences, but unlawful activity includes more than just what is criminal. It also includes activity that violates non-criminal, regulatory statutes (only a small proportion of statutes provides for criminal offences). Some regulatory statutes state that anyone who violates their provisions has committed an offence, but other statutes do not create specific offences. However, whether or not an offence is set out in a specific regulatory statute, it is still unlawful to fail to observe statutory requirements.
3. Further, s. 126 of the *Criminal Code* states that anyone who wilfully violates an Act of Parliament for which no offence is specified has committed an offence. Provincial laws have similar provisions.
4. Finally, some activities are neither criminal nor violations of specific regulatory statutes, but they can result in lawsuits brought by persons who are harmed by those acts. In such cases, the courts can find that a defendant is in breach of the laws applicable in a province and can penalize the person with an enforceable monetary award of damages to be paid to the plaintiff. These are known as civil actions. Where there is civil liability of an employee, and when the employee's activity falls within the scope of his or her duties, the employer can also be liable for monetary damages.

ACTIVITÉS ILLÉGALES (Liste d'exemples non exhaustive)

1. Aux fins de la présente politique, l'expression « activité illégale » est interprétée au sens large : elle comprend donc les actes passibles de différentes peines devant les tribunaux.
2. Certaines activités illégales sont des actes criminels et d'autres pas, puisqu'elles peuvent être de simples infractions qui violent des lois non pénales à caractère réglementaire (seule une infime proportion des lois prévoient des actes criminels). Or, certaines lois à caractère réglementaire disposent que quiconque ne les respecte pas a commis une infraction, alors que d'autres ne prévoient pas d'infractions précises. Néanmoins, qu'il soit fait état ou non d'une infraction dans une loi à caractère réglementaire particulière, il demeure illégal de ne pas respecter une obligation établie en vertu d'une loi.
3. En outre, l'article 126 du *Code criminel* dispose que quiconque contrevient volontairement à une loi fédérale sans qu'une peine y soit expressément prévue commet un acte criminel. Les lois provinciales renferment des dispositions analogues.
4. Enfin, certaines activités ne sont ni des actes criminels ni des infractions à une loi à caractère réglementaire donnée, bien que leurs auteurs puissent être passibles de poursuites par les personnes qu'ils ont lésées. En pareils cas, les tribunaux peuvent juger que le défendeur a enfreint les lois applicables dans une province et lui imposer l'obligation de verser des dommages-intérêts au demandeur. De telles activités constituent des poursuites au civil. Quand la responsabilité civile de l'employé est retenue et que ses activités s'inscrivent dans le cadre de ses fonctions, l'employeur peut, lui aussi, devoir payer des dommages-intérêts.



Reporting Requirements

5. Note that government institutions are required to report suspected illegal activity to the appropriate law enforcement agency (unless their legal advisor advises that the matter is too minor), under the following policies and guidelines:
 - a. Chapter 2-1, article 16.5 of the Government Security Policy (article 16.4 states that security breaches must be reported to the deputy head of the institution);
 - b. Chapter 4-7 of the Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown.
6. Also, under paragraph 80(e) of the *Financial Administration Act*, a person is guilty of an offence if he or she collects, manages or disburses public money; and knows or suspects that any other person has committed fraud against Her Majesty or has contravened the *Financial Administration Act*, its regulations, or any revenue law of Canada; and fails to report, in writing, that knowledge or suspicion to a superior officer.

Criminal Offences

7. The following are examples of criminal activity that could take place on electronic networks.
 - a. **Child pornography:** possessing, downloading or distributing any child pornography (see s. 163.1 of the *Criminal Code*).
 - b. **Copyright:** infringing on another person's copyright without lawful excuse – the *Copyright Act* provides for criminal prosecutions and civil actions in such cases (see also "copyright" under violations of federal and provincial statutes).

Exigences de déclaration

5. Il convient de souligner que les institutions gouvernementales sont tenues d'informer les organismes policiers intéressés des activités illégales qu'elles soupçonnent (à moins que leurs conseillers juridiques considèrent la question comme trop mineure), en application des politiques et lignes directrices suivantes :
 - a. chapitre 2-1, article 16.5 de la Politique du gouvernement concernant la sécurité (l'article 16.4 stipule que les manquements à la sécurité doivent être signalés à l'administrateur général de l'institution);
 - b. chapitre 4-7 de la Politique sur les pertes de fonds et infractions et autres actes illégaux commis contre la Couronne.
6. En outre, l'alinéa 80e) de la *Loi sur la gestion des finances publiques* dispose que commet une infraction quiconque perçoit, gère ou dépense des fonds publics; sait ou soupçonne qu'une autre personne a commis une fraude contre Sa Majesté ou a enfreint la *Loi sur la gestion des finances publiques*, son règlement ou toute loi fiscale du Canada; et ne communique pas par écrit ce qu'il sait ou soupçonne à un supérieur.

Actes criminels

7. Voici des exemples d'activités criminelles susceptibles de se produire sur les réseaux électroniques.
 - a. **Pornographie juvénile :** Avoir en sa possession, télécharger ou distribuer de la pornographie juvénile (voir l'article 163.1 du *Code criminel*).
 - b. **Droit d'auteur :** Porter atteinte au droit d'auteur d'autrui sans raison licite – la *Loi sur le droit d'auteur* prévoit des poursuites au pénal et au civil en pareils cas (voir également la section sur les droits d'auteur à la rubrique portant sur les infractions aux lois fédérales et provinciales).



- c. **Defamation:** causing a statement to be read by others that is likely to injure the reputation of any person by exposing that person to hatred, contempt or ridicule, or that is designed to insult the person (see ss. 296-317 of the *Criminal Code*). There are a number of defences for this offence. For instance, the maker of the statement may believe, on reasonable grounds, that the statement is true and that the statement is relevant to a subject of public interest whose public discussion benefits the public.
- d. **Hacking and other crimes related to computer security – Gaining unauthorized access to a computer system:** using someone else’s password or encryption keys to engage in fraud or obtaining money, goods or services through false representations made on a computer system. See the following *Criminal Code* provisions: s. 122 (breach of trust by public officer); s. 380 (fraud); s. 361 (false pretences); s. 403 (fraudulent personation); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
- e. **Trying to defeat the security features of the electronic networks.** See the following *Criminal Code* provisions: s. 342.1 (unauthorized use of computer systems and obtaining computer services); s. 342.1(d) (using, possessing or trafficking in stolen computer passwords or stolen credit card information); s. 342.2 (making, possessing or distributing computer programs that are designed to assist in obtaining unlawful access to computer systems); ss. 429 and 430 (mischief in relation to data).
- f. **Spreading viruses with intent to cause harm.** See the following *Criminal Code* provisions: ss. 429 and 430 (mischief in relation to data); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
- c. **Diffamation :** Faire lire par d'autres un énoncé susceptible de nuire à la réputation de quelqu'un en l'exposant à la haine, au mépris ou au ridicule, ou conçu pour l'insulter (voir les articles 296 à 317 du *Code criminel*). On peut invoquer plusieurs défenses contre une accusation de diffamation. Par exemple, l'auteur de l'énoncé peut avoir des raisons valables de croire que celui-ci est véridique et qu'il est pertinent dans le contexte d'une question d'intérêt public dont la discussion publique est avantageuse pour le public.
- d. **Piratage et autres crimes contre la sécurité informatique – Accès non autorisé à un système informatique :** Utilisation du mot de passe ou des codes de cryptage d'autrui pour commettre une fraude ou obtenir de l'argent, des biens ou des services en faisant de fausses représentations sur un système informatique. Voir les articles suivants du *Code criminel* : 122 (abus de confiance par un fonctionnaire public); 380 (fraude); 361 (escroquerie); 403 (supposition frauduleuse de personne); 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).
- e. **Tentative de percer les dispositifs de sécurité des réseaux électroniques.** Voir les dispositions suivantes du *Code criminel* : article 342.1 (utilisation non autorisée d'ordinateur et de services informatiques); alinéa 342.1d) (utilisation, possession ou trafic de mots de passe d'ordinateur volés ou de renseignements relatifs à des cartes de crédit volées); article 342.2 (fabrication, possession ou distribution de programmes informatiques conçus pour faciliter l'accès illégal à des systèmes informatiques); articles 429 et 430 (méfait concernant des données).
- f. **Introduction de virus dans l'intention de causer du tort.** Voir les articles suivants du *Code criminel* : 429 et 430 (méfait concernant des données) ainsi que 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).



- g. **Destroying, altering or encrypting data without authorization and with the intent of making it inaccessible to others with a lawful need to access it.** See the following *Criminal Code* provisions: ss. 429 and 430 (mischief in relation to data); s. 342.1 (unauthorized use of computer systems and obtaining computer services); ss. 129 and 139(2) (destroying or falsifying evidence to obstruct a criminal investigation).
- g. **Destruction, modification ou cryptage de données sans autorisation, dans l'intention d'en interdire l'accès à d'autres en ayant licitement besoin.** Voir les dispositions suivantes du *Code criminel* : articles 429 et 430 (méfait concernant des données); article 342.1 (utilisation non autorisée d'ordinateur et de services informatiques); article 129 et paragraphe 139(2) (destruction ou falsification de preuves pour faire obstacle à une enquête criminelle).
- h. **Interfering with others' lawful use of data and computers.** See the following *Criminal Code* provisions: ss. 429 and 430 (mischief in relation to data); s. 326 (theft of telecommunication services); s. 322 (theft of computer equipment); s. 342.1 (unauthorized use of computer systems and obtaining computer services).
- h. **Entrave à l'utilisation licite par d'autres de données et d'ordinateurs.** Voir les articles suivants du *Code criminel* : 429 et 430 (méfait concernant des données); 326 (vol de service de télécommunication); 322 (vol de matériel informatique); 342.1 (utilisation non autorisée d'ordinateur et de services informatiques).
- i. **Harassment:** sending electronic messages, without lawful authority, that cause people to fear for their safety or the safety of anyone known to them (see s. 264 of the *Criminal Code*). Section 264.1 of the *Criminal Code* makes it an offence to send threats to cause serious bodily harm, damage personal property or injure a person's animal.
- i. **Harcèlement :** Envoyer, sans en avoir l'autorité légale, des messages électroniques incitant quelqu'un à craindre pour sa sécurité ou pour celle de gens qu'il connaît (voir l'article 264 du *Code criminel*). L'article 264.1 du *Code criminel* dispose que commet une infraction quiconque fait parvenir à autrui des menaces de lui causer des lésions corporelles, d'endommager ses biens ou de blesser un animal qui lui appartient.
- j. **Hate propaganda:** disseminating messages that promote hatred or incite violence against identifiable groups in statements outside of private conversations (see s. 319 of the *Criminal Code*).
- j. **Propagande haineuse :** Diffuser ou distribuer des messages fomentant la haine ou incitant à la violence contre des groupes identifiables autrement que dans une conversation privée (voir l'article 319 du *Code criminel*).
- k. **Interception of private communications or electronic mail (in transit):** unlawfully intercepting someone's private communications or unlawfully intercepting someone's electronic mail (see s. 184 and s. 342.1 of the *Criminal Code*, respectively).
- k. **Interception de communications privées ou de courrier électronique (en transit) :** Intercepter illégalement les communications privées de quelqu'un ou intercepter illégalement le courrier électronique de quelqu'un (voir respectivement les articles 184 et 342.1 du *Code criminel*).



- i. **Obscenity:** distributing, publishing or possessing for the purpose of distributing or publicly displaying any obscene material (e.g. material showing explicit sex where there is undue exploitation of sex, where violence or children are present, or where the sex is degrading or dehumanizing and there is a substantial risk that the material could lead others to engage in anti-social acts). See s. 163 of the *Criminal Code*.

- m. **Various other offences:** the *Criminal Code* (and a few other statutes) provide for a range of other offences that can take place in whole or in part using electronic networks. For example, fraud, extortion, blackmail, bribery, illegal gambling, and dealing in illegal drugs can all occur, at least in part, over electronic networks and are criminal acts.

- i. **Obscénité :** Distribuer, publier ou avoir en sa possession en vue de le distribuer ou de l'exposer publiquement tout document obscène (p. ex. représentant des actes sexuels explicites exploitant indûment la sexualité, où il y a violence ou des enfants sont présents, ou encore où les actes sexuels sont dégradants ou déshumanisants et où il y a risque substantiel que le document pourrait inciter d'autres personnes à se livrer à des actes antisociaux). Voir l'article 163 du *Code criminel*.

- m. **Divers autres crimes :** Le *Code criminel* et quelques autres lois prévoient toute une gamme d'autres actes criminels susceptibles d'être entièrement ou partiellement commis grâce à l'utilisation des réseaux électroniques. Par exemple, la fraude, l'extorsion, le chantage, la corruption, les paris illégaux et le trafic de drogues illégales sont tous des actes criminels qui peuvent être commis, du moins en partie, sur les réseaux électroniques.

Violations of Federal and Provincial Statutes

- 8. The following are examples of unlawful (though not criminal) activity that can take place on electronic networks.
 - a. **Copyright and intellectual property:** violating another person's copyright (the *Copyright Act* provides for criminal prosecutions and civil actions in such cases). Unauthorized use of trade-marks and patents can also occur on electronic networks and these acts are proscribed in the *Trade-Marks Act*.

 - b. **Defamation:** spreading false allegations or rumours that would harm a person's reputation. In addition to criminal libel, defamation is contrary to provincial statutes dealing with this subject.

Infractions aux lois fédérales et provinciales

- 8. Voici des exemples d'activités illégales (mais non criminelles) susceptibles d'avoir lieu sur les réseaux électroniques.
 - a. **Atteintes au droit d'auteur et à la propriété intellectuelle :** Violation du droit d'auteur d'autrui (la *Loi sur le droit d'auteur* prévoit des poursuites au pénal et au civil en pareils cas). Il est possible aussi d'utiliser sans autorisation des marques de commerce et des brevets sur les réseaux électroniques, alors que ces actes sont interdits par la *Loi sur les marques de commerce*.

 - b. **Diffamation :** Fait de répandre des allégations ou des rumeurs mensongères nuisant à la réputation d'autrui. En plus d'être un acte criminel, la diffamation est interdite par les lois provinciales.



c. **Destroying or altering data without authorization:** unlawfully destroying, altering or falsifying electronic records. See the following provisions: s. 5 of the *National Archives of Canada Act*; ss. 6 and 12 of the *Privacy Act*; s. 4 of the *Access to Information Act*; s. 5 of the *Official Secrets Act*.

d. **Disclosing sensitive information without authorization – Disclosing personal information:** failing to respect the privacy and dignity of every person. The obligation to respect a person's privacy is expressed in a number of statutory provisions, such as ss. 4, 5, 7 and 8 of the *Privacy Act* and s. 19(1) of the *Access to Information Act*. Many federal statutes have non-disclosure provisions, often designed to protect the privacy of citizens who provide information to the government (see list of provisions in Schedule II of the *Access to Information Act*). In addition, Quebec has a number of privacy provisions in its *Civil Code* (see articles 3, 35-41) and in its *Human Rights Charter* (see articles 4, 5 and 49). British Columbia, Saskatchewan, Manitoba and Newfoundland also have statutes that provide for civil actions where there is an undue invasion of privacy.

e. **Disclosing business trade secrets:** revealing business trade secrets without authorization or in response to a formal request under the *Access to Information Act*, business trade secrets or confidential commercial information supplied in confidence by a third party and consistently treated as confidential by the third party. See s. 20(1)(a) and (b) of the *Access to Information Act*.

c. **Destruction ou modification de données sans autorisation :** Destruction, modification ou falsification illégales de documents électroniques. Voir l'article 5 de la *Loi sur les Archives nationales du Canada*, les articles 6 et 12 de la *Loi sur la protection des renseignements personnels*, l'article 4 de la *Loi sur l'accès à l'information* et l'article 5 de la *Loi sur les secrets officiels*.

d. **Communication non autorisée de données délicates – Communication de renseignements personnels :** Le fait de ne pas respecter la vie privée et la dignité d'un individu. L'obligation de respecter la vie privée d'une personne est exprimée dans plusieurs dispositions législatives, comme les articles 4, 5, 7 et 8 de la *Loi sur la protection des renseignements personnels* et le paragraphe 19(1) de la *Loi sur l'accès à l'information*. De nombreuses lois fédérales contiennent des dispositions interdisant la communication de renseignements de ce genre, souvent conçues pour protéger la vie privée des citoyens qui fournissent des renseignements au gouvernement (voir la liste de ces dispositions à l'annexe II de la *Loi sur l'accès à l'information*). Il y a plusieurs dispositions analogues dans le *Code civil* et dans la *Charte des droits de la personne* du Québec (respectivement les articles 3 et 35 à 41, ainsi que les articles 4, 5 et 49). La Colombie-Britannique, la Saskatchewan, le Manitoba et Terre-Neuve ont aussi des lois qui prévoient des poursuites au civil en cas d'atteintes à la vie privée.

e. **Divulgence de secrets industriels :** Révélation non autorisée de secrets industriels ou, en réponse à une demande officielle présentée en vertu de la *Loi sur l'accès à l'information*, de secrets industriels ou de renseignements commerciaux confidentiels communiqués à titre confidentiel par un tiers et traités comme tels de façon constante par celui-ci. Voir les alinéas 20(1)a) et b) de la *Loi sur l'accès à l'information*.



f. **Disclosing sensitive government information:** revealing sensitive government information without authorization. See ss. 3 and 4 of the *Official Secrets Act*. As well, when responding to formal requests under the *Access to Information Act*, institutions must not disclose information obtained in confidence from other governments (see s. 13 of the *Access to Information Act*). The other exemptions in the Act relating to government information are discretionary.

Note that employees and other authorized individuals and the government are immune from legal actions with respect to disclosures made in good faith under either the *Privacy Act* or *Access to Information Act*.

g. **Harassment:** It is a discriminatory practice "(a) in the provision of [...] services [...] available to the general public [...] or (c) in matters related to employment to harass an individual on a prohibited ground of discrimination". The prohibited grounds are race, national or ethnic origin, colour, religion, age, sexual orientation, marital status, family status, disability and conviction for which a pardon has been granted. Thus, in some circumstances, displaying unwelcome sexist, pornographic, racist or homophobic images or text on a screen at work can be unlawful harassment. See s. 14 of the *Canadian Human Rights Act*.

f. **Divulgateion de renseignements gouvernementaux de nature délicate :** Communication non autorisée de renseignements gouvernementaux de nature délicate (voir les articles 3 et 4 de la *Loi sur les secrets officiels*). Dans ce contexte, lorsqu'elles répondent à des demandes officielles présentées en vertu de la *Loi sur l'accès à l'information*, les institutions fédérales ne doivent pas communiquer de renseignements obtenus à titre confidentiel d'autres gouvernements (voir l'article 13 de la *Loi sur l'accès à l'information*). Les autres exceptions à cet égard prévues dans la Loi sont de nature discrétionnaire.

Il convient de souligner que les fonctionnaires et autres personnes autorisées ainsi que le gouvernement ne sont pas passibles de poursuites en justice à l'égard des communications qu'ils ont faites de bonne foi en vertu soit de la *Loi sur la protection des renseignements personnels*, soit de la *Loi sur l'accès à l'information*.

g. **Harcèlement :** Constitue un acte discriminatoire, « s'il est fondé sur un motif de distinction illicite, le fait de harceler un individu : a) lors de la fourniture [...] de services [...] destinés au public; c) en matière d'emploi ». Les motifs de distinction illicite sont ceux qui sont fondés sur la race, l'origine nationale ou ethnique, la couleur, la religion, l'âge, l'orientation sexuelle, l'état matrimonial, la situation de famille, la déficience ou l'état de personne graciée. Ainsi, dans certaines circonstances, afficher des images sexistes, pornographiques, racistes ou homophobes indésirables au travail, sur un écran d'ordinateur, peut constituer du harcèlement illégal. Voir l'article 14 de la *Loi canadienne sur les droits de la personne*.



| | |
|------------------|------------------|
| Number - Numéro: | 2000-05-01 |
| Date | Annex/e "A" |
| 226 | Page: 8 of/de 10 |

- h. **Privacy infractions:** reading someone else's electronic mail or other personal information without authorization, listening in on someone's private conversations or intercepting electronic mail while it is in transit, for example.

When an employee or other person has a reasonable expectation of privacy in his or her electronic mail or other personal documents, an institution may be guilty of an unreasonable search or seizure under s. 8 of the *Charter of Rights and Freedoms* if it infringes on that reasonable expectation without a lawful authority. This is true whether the institution is acting as employer or otherwise.

The institution may also be deemed to have collected or used data unlawfully, contrary to ss. 4, 5, 7 and 8 of the *Privacy Act*. The government may be liable for damages when private communications are intercepted unlawfully. See ss. 16-20 of the *Crown Liability and Proceedings Act* concerning electronic surveillance activities carried out by Crown servants in the course of their employment; s. 20 specifically provides that the Crown servant will be accountable to the Crown for the amount of the damages awarded by a court. The government may also be liable for damages when an unlawful disclosure of personal information occurs contrary to provisions in various statutes (see the list of such provisions in Schedule II of the *Access to Information Act*). For more information on these issues, refer to Appendix E of the Treasury Board Policy on the Use of Electronic Networks, which discusses reasonable expectations of privacy.

- h. **Atteintes à la vie privée :** Lecture du courrier électronique ou d'autres renseignements personnels d'autrui sans autorisation, écoute des conversations privées ou interception du courrier électronique en transit, par exemple.

Quand un fonctionnaire ou une autre personne a le droit d'avoir des attentes raisonnables quant à la protection des renseignements personnels qui le concerne dans son courrier électronique ou dans d'autres documents personnels, l'institution – qu'elle les ait à son service ou pas – peut être coupable d'une infraction en vertu de l'article 8 de la *Charte canadienne des droits et libertés* (perquisitions et saisies abusives), si en l'absence d'une autorité légale, elle ne respecte pas ces attentes raisonnables.

L'institution peut aussi être réputée avoir recueilli ou utilisé illégalement des données contrairement aux articles 4, 5, 7 et 8 de la *Loi sur la protection des renseignements personnels*. Le gouvernement peut être passible de poursuites en dommages-intérêts quand des communications privées sont interceptées illégalement (voir les articles 16 à 20 de la *Loi sur la responsabilité civile de l'État et le contentieux administratif*, concernant les activités de surveillance électronique exécutées par des fonctionnaires dans le cadre de leurs fonctions; en fait, l'article 20 dispose expressément que le fonctionnaire est redevable envers l'État du montant des dommages-intérêts accordé par un tribunal. Le gouvernement peut aussi être passible de poursuites en dommages-intérêts quand une communication illégale de renseignements personnels a lieu contrairement aux dispositions de diverses lois (voir la liste de ces dispositions à l'annexe II de la *Loi sur l'accès à l'information*). Pour un complément d'information sur ces questions, voir l'annexe E de la « Politique d'utilisation des réseaux électroniques » du Conseil du Trésor, qui contient un exposé sur les attentes raisonnables quant à la protection des renseignements personnels.



| | |
|------------------|------------------|
| Number - Numéro: | 2000-05-01 |
| Date | Annex/e "A" |
| 226 | Page: 9 of/de 10 |

- i. **Use of public money without proper authority.** See the following provisions of the *Financial Administration Act*: s. 33 (making a requisition without authority); s. 34 (certifying receipt of goods or services without authority); s. 78 (liability for losses caused by malfeasance or negligence); and s. 80 (taking bribes or participating in corrupt practices).

- i. **Utilisation des fonds publics sans autorisation.** Voir les articles suivants de la *Loi sur la gestion des finances publiques*: 33 (demande de paiement non autorisée); 34 (attestation non autorisée de livraison de fournitures ou de prestations de services); 78 (responsabilité des pertes résultant d'une malversation ou d'une négligence); 80 (acceptation de pots-de-vin ou participation à des activités de corruption).

Activity That Can Expose Authorized Individuals or the Employer to Civil Liability

- 9. Various kinds of conduct can expose a person or an employer to civil liability. The employer's liability will be triggered when a Public Service employee performs the unlawful activity in the course of his or her employment. The Public Service employee remains personally liable for these actions, even when the federal government is also liable. (The government's policy on indemnifying authorized individuals – Policy on the Indemnification of and Legal Assistance for Crown Servants – is relevant to such actions.) The following are examples of civil wrongs that can take place on electronic networks.

- a. **Disclosing or collection of sensitive data:** revealing or obtaining such information without authorization. In addition to the statutory provisions mentioned above, an unauthorized disclosure or collection of personal information can result, in some circumstances, in a civil action for invasion of privacy, nuisance or trespass under common law, and similar actions under the Civil Code of Quebec (articles 3, 15-41); for breach of contract and for breach of trust or breach of confidence (e.g. if confidential commercial information is disclosed).

Activités pouvant exposer des personnes autorisées ou l'employeur à des poursuites en responsabilité civile

- 9. Divers comportements peuvent exposer une personne autorisée ou un employeur à des poursuites en responsabilité civile. L'employeur est réputé responsable lorsqu'un employé de la fonction publique commet une activité illégale dans le cadre de ses fonctions. L'employé de la fonction publique demeure personnellement responsable de ses actions, même si le gouvernement fédéral en est lui aussi responsable. (La politique gouvernementale d'indemnisation des personnes autorisées, qui s'intitule « Politique sur l'indemnisation des fonctionnaires de l'État et la prestation de services juridiques à ces derniers », est pertinente dans ce contexte.) Voici des exemples de quasi-délits civils susceptibles de se produire sur les réseaux électroniques.

- a. **Communication ou collecte de données de nature délicate :** Révéler ou obtenir des renseignements de ce genre sans autorisation. En plus des dispositions législatives déjà mentionnées, la communication ou la collecte non autorisées de renseignements personnels peut provoquer, dans certaines circonstances, des poursuites au civil pour atteinte à la vie privée, nuisance ou intrusion en vertu de la *common law* et des poursuites analogues fondées sur le *Code civil du Québec* (articles 3 et 15 à 41), pour rupture de contrat ainsi que pour abus de confiance (p. ex. si des renseignements commerciaux confidentiels sont communiqués).



| | |
|------------------|-------------------|
| Number - Numéro: | 2000-05-01 |
| Date | Annex/e "A" |
| 226 | Page: 10 of/de 10 |

- b. **Defamation:** spreading false allegations or rumours that would harm a person's reputation. In addition to criminal libel, publishing defamatory statements without a lawful defence can result in a civil action.

- c. **Inaccurate information:** posting inaccurate information, whether negligently or intentionally. This can lead to civil lawsuits for negligent misrepresentation if it can be shown that (a) the posting caused harm and resulted in damages to the person who (b) reasonably relied on the information, that (c) the person or institution that made the posting owed a duty of care to the person who was harmed by inaccurate information; and (d) the inaccuracy was due to negligence (conduct that falls below what is reasonable in the circumstances).

- b. **Diffamation :** Répandre des allégations ou des rumeurs mensongères susceptibles de porter atteinte à la réputation de quelqu'un. En plus d'être un acte criminel, la publication de déclarations diffamatoires sans défense légale peut exposer son auteur à des poursuites au civil.

- c. **Communication de renseignements erronés :** Afficher des renseignements erronés, que ce soit par négligence ou à dessein. Ce genre de comportement peut provoquer des poursuites au civil pour fausse représentation faite avec négligence si l'on peut démontrer : a) que l'affichage a lésé des personnes et porté préjudice à des personnes qui b) s'étaient raisonnablement fondées sur les renseignements, c) que la personne ou l'institution qui a affiché les renseignements avait le devoir de s'occuper raisonnablement de la personne lésée par la fausse déclaration et d) que les erreurs étaient attribuables à une négligence (un comportement ne répondant pas aux critères de diligence raisonnable dans les circonstances).



| | |
|------------------|-----------------|
| Number - Numéro: | 2000-05-01 |
| Date | Annex/e "B" |
| 226 | Page: 1 of/de 3 |

UNACCEPTABLE ACTIVITY THAT IS NOT NECESSARILY UNLAWFUL BUT WHICH VIOLATES TREASURY BOARD POLICIES (Non-Exhaustive List of Examples)

1. A number of Treasury Board policies are not media-specific – that is, they apply whether the unacceptable activity occurs on paper, by telephone, through computer networks, in oral conversation or through any other medium. It is unacceptable to violate Treasury Board policies including institutional policies. The following policies are important in the context of the use of electronic networks: the Government Security Policy (in relation to standards including the Technical Security Standards for Information Technology); the Harassment in the Workplace Policy; the Privacy and Data Protection Policy, including the Employee Privacy Code; the Government Communications Policy; and the Conflict of Interest and Post-Employment Code for the Public Service. These policies relate to various activities, as described below.
 - a. **Sending classified or designated information on unsecured networks, unless it is sent in encrypted form.** (Government Security Policy)
 - b. **Accessing, without authorization, sensitive information held by the government.** (Government Security Policy)

ACTIVITÉS INACCEPTABLES QUI, SANS ÊTRE NÉCESSAIREMENT ILLÉGALES, SONT INCOMPATIBLES AVEC LES POLITIQUES DU CONSEIL DU TRÉSOR (Liste d'exemples non exhaustive)

1. Pour la plupart, les politiques du Conseil du Trésor ne s'appliquent pas à un moyen de communication plutôt qu'à un autre, puisque les politiques sont aussi valables si l'activité inacceptable se fait par écrit, au téléphone, sur les réseaux électroniques, dans une conversation ou à l'aide d'un autre moyen de communication quelconque. Il est inacceptable pour un fonctionnaire de violer les politiques du Conseil du Trésor, y compris les politiques institutionnelles. Les politiques suivantes sont importantes dans le contexte de l'utilisation des réseaux électroniques : la Politique du gouvernement concernant la sécurité (en ce qui concerne les normes, y compris les Normes de sécurité techniques de la technologie de l'information); la Politique sur le harcèlement en milieu de travail; la Politique sur la protection des renseignements personnels, y compris le Code de la protection des renseignements personnels concernant les employés; la Politique du gouvernement en matière de communications; le Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique. Ces textes s'appliquent aux activités décrites ci-après.
 - a. **Communiquer des renseignements protégés ou désignés sur des réseaux non protégés, sauf s'ils sont cryptés.** (Politique du gouvernement concernant la sécurité)
 - b. **Consulter sans autorisation des renseignements délicats détenus par le gouvernement.** (Politique du gouvernement concernant la sécurité)



| | |
|------------------|-----------------|
| Number - Numéro: | 2000-05-01 |
| Date | Annex/e "B" |
| 226 | Page: 2 of/de 3 |

- c. **Attempting to defeat information technology security features**, through such means as using anti-security programs; using someone else's password, user identification or computer account; disclosing one's password, network configuration information or access codes to others; or disabling anti-virus programs. (Government Security Policy)
- d. **Causing congestion and disruption of networks and systems**, through such means as sending chain letters and receiving list server electronic mail unrelated to a work purpose. These are examples of excessive use of resources for non-work related purposes. (Government Security Policy)
- e. **Sending abusive, sexist or racist messages to employees and other individuals.** (Harassment in the Workplace Policy)
- f. **Using the government's electronic networks for private business, personal gain or profit or political activity.** (Conflict of Interest and Post-Employment Code for the Public Service)
- g. **Making excessive public criticisms of governmental policy.** (Conflict of Interest and Post-Employment Code for the Public Service)
- h. **Representing personal opinions as those of the institution, or otherwise failing to comply with institutional procedures concerning public statements about the government's positions.** (Conflict of Interest and Post-Employment Code for the Public Service)
- c. **Tenter de percer les dispositifs de sécurité des systèmes informatiques**, notamment en utilisant des programmes antisécurité, en se servant du mot de passe, du code d'utilisateur ou du compte informatique de quelqu'un d'autre, en donnant son mot de passe, des renseignements sur la configuration du réseau ou des codes d'accès à quelqu'un d'autre ou en désactivant des programmes antivirus. (Politique du gouvernement concernant la sécurité)
- d. **Congestionner et perturber les réseaux et les systèmes**, notamment en envoyant des chaînes de lettres et en recevant du courrier électronique de serveurs de listes pour d'autres fins que le travail. Ce ne sont là que deux exemples d'utilisation abusive des ressources à des fins personnelles. (Politique du gouvernement concernant la sécurité)
- e. **Envoyer des messages abusifs, sexistes ou racistes à des fonctionnaires ainsi qu'à d'autres personnes.** (Politique sur le harcèlement en milieu de travail)
- f. **Utiliser les réseaux électroniques du gouvernement pour des affaires commerciales personnelles, pour gain ou profit personnel, ou pour des activités politiques.** (Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique)
- g. **Faire publiquement des critiques excessives de la politique gouvernementale.** (Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique)
- h. **Présenter ses opinions personnelles comme celles de l'institution ou manquer autrement à son devoir de se conformer aux procédures institutionnelles sur les déclarations publiques au sujet des positions du gouvernement.** (Code régissant les conflits d'intérêts et l'après-mandat s'appliquant à la fonction publique)



- i. **Failing to provide employees and other authorized individuals with notice of electronic monitoring and auditing practices.** (Government Security Policy and the Employee Privacy Code)

- j. **Providing personnel with access to systems, networks, or applications used to process sensitive information before such personnel are properly security screened.** (Government Security Policy)

- k. **Failing to revoke system access rights of personnel, when they leave the institution, due to the end of employment or the termination of a contract, or when they lose their reliability status or security clearance.** (Government Security Policy)

- l. **Unauthorized removal or installation of hardware or software on government owned informatics devices or electronic networks.** (Government Security Policy)

- i. **Manquer à son devoir d'informer les fonctionnaires et d'autres personnes autorisées des pratiques de contrôle et de vérification électroniques.** (Politique du gouvernement concernant la sécurité et Code de la protection des renseignements personnels concernant les employés)

- j. **Fournir au personnel l'accès aux systèmes, aux réseaux ou aux applications utilisées pour le traitement de renseignements de nature délicate avant qu'il ait fait l'objet d'une enquête de sécurité adéquate.** (Politique du gouvernement concernant la sécurité)

- k. **Négliger d'annuler les droits d'accès aux systèmes d'un employé qui quitte l'institution en raison d'une mise en disponibilité ou de l'expiration d'un contrat, ou qui perd son statut de fiabilité ou son attestation de sécurité.** (Politique du gouvernement concernant la sécurité)

- l. **Installer ou retirer sans autorisation du matériel ou des logiciels sur des ordinateurs ou des réseaux électroniques de l'État.** (Politique du gouvernement concernant la sécurité)



| | |
|-----------------------------|--|
| Number - Numéro: 226 | Date 2000-05-01 Annex/e "C" Page: 1 of/de 1 |
|-----------------------------|--|

UNACCEPTABLE ACTIVITIES RELATING TO ACCESS TO ELECTRONIC NETWORKS PROVIDED BY THE GOVERNMENT

1. Authorized individuals shall not use CSC's network to access or download Web sites or files, or send or receive electronic mail messages or other types of communication, that fall into the following categories:
 - a. documents that incite hatred against identifiable groups contained in personal messages (the *Criminal Code* prohibits incitement of hatred against identifiable groups in public conversations);
 - b. documents whose main focus is pornography, nudity and sexual acts (however, authorized individuals may access such information for valid work-related purposes, and may visit sites whose main focus is serious discussions of sexual education and sexual orientation issues).

ACTIVITÉS INACCEPTABLES QUANT À L'ACCÈS AUX RÉSEAUX ÉLECTRONIQUES DE L'ÉTAT

1. Il est interdit aux personnes autorisées d'utiliser le réseau électronique du SCC pour visiter des sites Web, pour consulter ou télécharger des fichiers du WWW, ou encore pour envoyer ou recevoir du courrier électronique ou d'autres types de communications s'inscrivant dans les catégories suivantes :
 - a. communications incitant à la haine contre des groupes identifiables et contenues dans des messages personnels (le *Code criminel* interdit l'incitation à la haine contre des groupes identifiables dans des conversations publiques);
 - b. communications essentiellement axées sur la pornographie, la nudité et les actes sexuels (les personnes autorisées peuvent néanmoins avoir accès à des renseignements de cet ordre pour des raisons valides liées à leur travail, et peuvent aussi visiter des sites essentiellement axés sur des discussions sérieuses de questions relatives à l'éducation et à l'orientation sexuelle).