COMMISSIONER'S DIRECTIVE 226	In Effect: 2013-08-19 Last Review: 2013-08-19 Due for Review: 2015-08-01

Use of Electronic Resources

PROGRAM ALIGNMENT	Internal Services
OFFICE(S) OF PRIMARY INTEREST	Senior Deputy Commissioner
ONLINE @	• http://infonet/cds/cds/226-cd-eng.pdf • http://infonet/cds/cds/226-cd-fra.pdf • http://www.csc-scc.gc.ca/text/plcy/cdshtm/226-cd-eng.shtml • http://www.csc-scc.gc.ca/text/plcy/cdshtm/226-cd-fra.shtml
AUTHORITIES	• Treasury Board Policy on Government Security (2012) • Treasury Board Policy on the Use of Electronic Networks (1998)
PURPOSE	• To ensure the appropriate use of the Correctional Service of Canada's (CSC) electronic resources
APPLICATION	Applies to CSC employees as well as any other individuals who have been authorized to use CSC's electronic resources (referred hereafter as authorized individuals)

CONTENTS

RESPONSIBILITIES

1. The Chief Information Officer will:

   a. establish procedures for authorizing individuals to access CSC's electronic resources

   b. establish a process for ensuring that authorized individuals receive appropriate training and information on the proper use of these resources

   c. establish monitoring procedures and designate individuals who will monitor the use of electronic resources.

2. The Director, Information Technology Security, will:

   a. provide direction and information on the interpretation of lawful and acceptable use of CSC's electronic resources

   b. ensure that reports of suspected unlawful or unacceptable activity pertaining to the use of CSC's electronic resources are investigated, pursuant to section 6.1.7 of the Treasury Board Policy on Government Security.

3. Managers will report all instances of suspected unlawful or unacceptable activities pertaining to the use of CSC's electronic resources to the Director, Information Technology Security, or the Regional Manager, Information Technology Security, at the regional level. The national Departmental Security Officer and designated personnel having responsibilities for the departmental security activities at the regional level will be advised.

4. On the recommendation of the Director, Information Technology Security, and the Departmental Security Officer, managers will seek legal advice in cases of suspected unlawful or unacceptable uses of CSC's electronic resources.

5. Individuals authorized to use CSC's electronic resources (authorized individuals) will:

    a. abide by the laws, government policies, directives and any other instructions published by CSC, on the use of electronic resources

    b. take reasonable measures to control the use of their password, user identification or computer accounts. This includes assuming responsibility for any actions or costs arising from the unauthorized use of electronic resources

    c. use information technology security features (e.g. encryption, virus and data protection) provided by the CSC

    d. ensure that their communications using CSC's electronic resources do not reflect badly on CSC or the Government of Canada and comply with any policies pertaining to professional conduct and the use of social media

    e. report suspected unlawful or unacceptable activities to their manager(s)

    f. seek clarification from the Director, Information Technology Security, when in doubt as to whether a planned use is acceptable and lawful.

AUTHORIZED USES OF ELECTRONIC RESOURCES

Use for Official Business

6. Electronic resources must be used for official business. This includes, but is not limited to, creating, accessing, manipulating, storing and transmitting:

    a. electronic mail messages (email)

    b. electronic records or information on CSC-managed electronic resources

    c. information on the CSC Intranet

    d. information on the Internet.

Personal Use

7. Limited personal use of CSC's electronic resources 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 unauthorized additional cost to the CSC

c. observes rules governing professional conduct and prohibitions related to unlawful and unacceptable conduct as outlined in this policy and elsewhere

d. employs only those information technology products authorized and installed by CSC-authorized Information Management/Information Technology personnel

e. does not require CSC to provide additional privacy protection for personal information stored, transmitted or processed beyond that which is already provided

f. allows CSC to read the contents of communications and files and access personal information pursuant to the section entitled "Monitoring" in this directive.

PROHIBITED USES OF ELECTRONIC RESOURCES

8. Authorized individuals are prohibited from using government electronic resources to:

   a. operate, transmit or store games or other entertainment software

   b. maintain or support a personal private business or to assist relatives, friends, or other persons in such activities, or

   c. conduct any unlawful or unacceptable activity or to store or transmit information relating thereto, except where specifically authorized as part of an official investigation.

9. Offender access to CSC's electronic resources is prohibited except where specifically authorized by CSC policy for approved purposes such as an educational or work program, in compliance with applicable rules related to the protection of personal information (see Commissioner's Directive 730 – Inmate Program Assignment and Payments).

MONITORING

Routine Monitoring

10. Routine monitoring of electronic resources will be performed by staff designated by the Chief Information Officer to assess performance, to protect the availability, integrity, confidentiality, value and intent of use of government assets and to ensure compliance with government policy. Routine 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 email messages

    d. testing for viruses

e. keyword searches on networks, computer systems and electronic storage devices.

11. CSC's electronic resources automatically log the identity of individuals and their activities while on the resource(s).

12. Copies of files and email records (including "draft" records) are automatically backed up and retained on a daily basis.

Incidental Monitoring

13. To the greatest extent possible, the CSC seeks to preserve individual privacy; however, users should be aware that their use of CSC's electronic resources is not private. While CSC does not routinely read email or file content, under certain circumstances, CSC may monitor the activity and accounts of individual users including, but not limited to, individual login sessions, communications, email and file content.

14. All cases of individual monitoring must be authorized in advance by either the Director, Information Technology Security, the Director General, Security, or the Assistant Commissioner, Human Resource Management, except:

    a. for the cases specified in paragraph 15a

    b. for the cases required by law, or

    c. when this type of monitoring is necessary to respond to legitimate emergency situations.

Monitoring for Unlawful Activity and Unacceptable Conduct

15. If there are reasonable grounds to suspect that an authorized individual is misusing electronic resources, including during personal use, monitoring without notice, including viewing the content of individual email records or files, may occur under the following circumstances:

    a. the authorized individual has voluntarily made electronic files or email accessible to CSC or to the public

    b. it is necessary to do so to protect the integrity, ensure the security and/or the liability exposure of CSC

    c. there are reasonable grounds to suspect that the authorized individual has utilized CSC's electronic resources in the commission of a violation of CSC or other government policy

    d. there are reasonable grounds to suspect that the authorized individual is using electronic resources for an unlawful or unacceptable activity

e. an account appears to be engaged in unusual or unusually excessive activity, as indicated by the routine monitoring of general activity and usage patterns, or

f. upon the receipt of a warrant or other legal instrument from a law enforcement agency.

16. Individuals who are obliged to read the content of electronic communications as part of an investigation must keep the information confidential and use it only for the purposes authorized.

DISCIPLINARY MEASURES AND SANCTIONS

17. CSC may pursue disciplinary measures or sanctions in cases of unlawful and/or unacceptable activity related to the use of its electronic resources. Disciplinary measures will be commensurate with the seriousness and circumstances of the unlawful and/or unacceptable activity. In cases where disciplinary measures are required, Labour Relations must be consulted to ensure that the application of disciplinary measures is consistent across CSC.

18. Disciplinary measures may include:

a. a verbal or written reprimand

b. restrictions on access to the electronic resources

c. review of an individual's reliability status or security clearance

d. suspension or termination of employment.

19. Following consultation with Legal Services, CSC will report suspected unlawful activities related to the use of its electronic resources to law enforcement authorities.

ENQUIRIES

20. Strategic Policy Division
National Headquarters
Email: Gen-NHQPolicy-Politi@csc-scc.gc.ca

Commissioner,

Original Signed by:
Don Head

ANNEX A

CROSS-REFERENCES AND DEFINITIONS

CROSS-REFERENCES

Related Legislation

Access to Information Act
Copyright Act
Corrections and Conditional Release Act
Corrections and Conditional Release Regulations
Criminal Code
Crown Liability and Proceedings Act
Library and Archives of Canada Act
Privacy Act
Security of Information Act

Treasury Board Policies and Publications

Communications Policy of the Government of Canada
Directive on Losses of Money or Property
Guide to the Review of Management of Government Information Holdings
Policy on Access to Information
Policy on Government Security
Policy on Harassment Prevention and Resolution
Policy on Privacy Protection
Policy on the Use of Electronic Networks
Telework Policy
Values and Ethics Code for the Public Service

CSC Policies and Guides

CD 041 – Incident Investigations
CD 060 – Code of Discipline
CD 225 – Information Technology Security
CD 568 – Management of Security Information and Intelligence
CD 568-1 – Recording and Reporting of Security Incidents
CD 730 – Inmate Program Assignment and Payments

Guide to Information Security
Laptop Computers – Safeguards to Remember
Departmental Security Procedures Manual – Security of Information and Assets
Standards of Professional Conduct in the Correctional Service of Canada

DEFINITIONS

Authorized individuals: CSC employees as well as contractors and any other individuals who have been authorized by a CSC authority to access CSC's electronic resources.

Electronic resource: any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Within the context of this document, electronic resources refer to all electronic resources owned and operated by CSC.

Personal use: an activity that is conducted for purposes other than accomplishing official or otherwise authorized activity.

Social media: interactive web-based platforms that allow for participants with distinct social/user profiles to create, share and interact with user generated content, which can include text, images, video and audio (e.g. Facebook, Twitter, YouTube and collaborative technologies, such as Wikis, Google Docs).

Unacceptable activity: any activity that violates CSC, Treasury Board or other government policy (for examples, see Appendix B of the Treasury Board Policy on the Use of Electronic Networks), or that violates the limitations on personal use as set out in this policy and in Appendix C of the above-mentioned Treasury Board policy.

Unlawful activity: criminal offences, contraventions of non-criminal regulatory federal and provincial statutes, and actions that make an authorized individual or an institution liable to a civil lawsuit. For examples, refer to Appendix A of the Treasury Board Policy on the Use of Electronic Networks.