COMMISSIONER'S DIRECTIVE 564	In Effect: 2015-02-09 Last Review: 2015-02-09 Due for Review: 2017-02-09

Departmental Security

PROGRAM ALIGNMENT	Internal Services
OFFICE(S) OF PRIMARY INTEREST	Correctional Operations and Programs Sector
ONLINE @	• http://infonet/cds/cds/564-cd-eng.pdf • http://infonet/cds/cds/564-cd-fra.pdf • http://www.csc-scc.gc.ca/text/plcy/cdshtm/564-cd-eng.shtml • http://www.csc-scc.gc.ca/text/plcy/cdshtm/564-cd-fra.shtml
AUTHORITIES	• *Corrections and Conditional Release Act* (CCRA), sections 3, 3.1, and 4 • Treasury Board Policy on Government Security • *Financial Administration Act*, section 7
PURPOSE	• To provide direction to Correctional Service of Canada (CSC) staff to ensure compliance with the Treasury Board Policy on Government Security • To ensure that those who have access to government information, assets and services are deemed trustworthy, reliable and loyal through an appropriate security screening program • To ensure that security threats, risks and incidents are assessed and managed to help protect individuals, and CSC's critical assets and information, as well as to ensure the continued delivery of services • To ensure that all CSC employees effectively manage departmental security activities within their areas of responsibility and contribute to an effective CSC-wide security management program
APPLICATION	Applies to all CSC employees and individuals who have access to government information, property and assets under CSC's jurisdiction

CONTENTS

SECTIONS	
1 – 9	Responsibilities

10	Procedures
11	Enquiries
Annex A	Cross-References and Definitions

RESPONSIBILITIES

1. The Assistant Commissioner, Correctional Operations and Programs, is responsible for the development and approval of guidelines to support all departmental security directives.

2. The Chief Information Officer will:

   a. consult with the Departmental Security Officer prior to issuing any Information Technology (IT) security policies and procedures

   b. appoint an Information Technology Security Coordinator with a functional reporting relationship to both the Departmental Security Officer and Departmental Chief Information Officer.

3. The Director General, Security, will:

   a. ensure that departmental security activities are carried out under the overall coordination of the Departmental Security Officer

   b. ensure that the Policy on Government Security responsibilities are integrated into CSC's Corporate Business Plan to assist Executive Committee decision-making

   c. ensure that departmental security policies are developed and maintained in accordance with legislation and the Treasury Board policy

   d. act as the Chairperson of the Security Advisory Committee (SAC)

   e. act as a liaison between members of EXCOM and members of the SAC.

4. The Departmental Security Officer (DSO) designated by the Commissioner will:

   a. coordinate policy-related activities such as directives, procedures and guidelines that comply with the Treasury Board policy requirements

   b. ensure consistency among local, regional and national practices by providing advice and guidance on security matters related to the Policy on Government Security and its associated standards

c. ensure departmental security breaches and incidents are reported

d. ensure the execution of the mandate set out in the Treasury Board policy by representing the Commissioner at the Treasury Board Secretariat for all departmental activities related to security and identity management and the Policy on Government Security.

5. The Regional Deputy Commissioners will:

a. designate individuals having responsibilities for departmental security activities to ensure that trained individuals implement the Departmental Security Program in their respective regions.

6. The regional designated individuals having responsibilities for departmental security activities will:

a. coordinate departmental security activities at the regional level

b. implement the program objectives

c. conduct departmental security threat and risk assessments

d. ensure that corrective measures are taken

e. maintain a functional reporting relationship with the Departmental Security Officer and liaise with the National Headquarters Departmental Security Division.

7. Each facility under Regional Headquarters' jurisdiction will designate a Unit Security Officer who will:

a. maintain a functional relationship with the regional designated individuals having responsibilities for the departmental security activities

b. support the regional designated individuals having responsibilities for departmental security activities in the coordination or the delivery of security awareness sessions to all CSC employees and persons having access to government information, property and assets under CSC's jurisdiction

c. ensure the completion of a Threat and Risk Assessment (TRA) when necessary, and contribute to the effective maintenance of the departmental security plan, as required

d. report all Government Security Policy breaches in accordance with the established reporting structure in CD 568-1 – Recording and Reporting of Security Incidents.

8. Managers at all levels will:

    a. ensure the safety of individuals, the security of information and the protection of property and valuable assets for which they are responsible

    b. ensure that security requirements are integrated into the business planning, programs, services and other management activities

    c. assess security risks, formally accept or recommend acceptance of residual risks, reassess risks in light of changes to programs, activities or services, and take corrective action to address identified deficiencies

    d. monitor the implementation and effectiveness of security controls and report accordingly to the Departmental Security Officer or regional designated individuals having responsibilities for departmental security activities, as appropriate

    e. ensure all individuals apply effective security practices in day-to-day operations

    f. identify contract security requirements and other safeguards for the protection of information and assets

    g. confirm that all authorized individuals have the required reliability status or security clearance prior to accessing CSC's facilities, protected information and valuable assets

    h. ensure that all individuals having access to government information, property and assets under CSC's jurisdiction participate in a security awareness session and/or receive appropriate training pursuant to departmental security policies

    i. ensure that departmental security practitioners and other individuals with specific departmental security responsibilities receive appropriate and up-to-date training to ensure they have the necessary knowledge and competencies to effectively perform their security responsibilities and do not inadvertently compromise security.

9. All employees will:

    a. safeguard CSC information and assets under their control, whether working on or off-site

    b. ensure that situations likely to compromise site security are reported immediately

    c. on an ongoing basis, apply security controls related to their areas of responsibility (this includes, but is not limited to, administrative and corporate practices)

    d. refer to and apply the guidelines attached to the Commissioner's Directives on departmental security, as needed.

PROCEDURES

10. The departmental security program and activities will adhere to the Treasury Board Policy on Government Security and the following Commissioner's Directives:

    a. CD 564-1 – Individual Security Screening: to ensure that individuals undergo a screening process when their duties or tasks necessitate access to classified/protected information and assets

    b. CD 564-2 – Departmental Physical Security: to establish baseline physical security requirements to counter threats to CSC employees, assets and service delivery and to provide consistent safeguarding for the Government of Canada.

ENQUIRIES

11. 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

CD 225 – Information Technology Security
CD 226 – Use of Electronic Resources
CD 564-1 – Individual Security Screening
CD 564-2 – Departmental Physical Security
CD 568-1 – Recording and Reporting of Security Incidents
CD 600 – Management of Emergencies
GL 600-1 – Business Continuity and Emergency Preparedness Planning

Access to Information Act
Privacy Act
Treasury Board Operational Security Standard: Management of Information Technology (MITS)

DEFINITIONS

Assets: tangible or intangible resources of the Government of Canada. Assets include but are not limited to: information in all forms and media, networks, systems, material, real property, financial resources, employee trust, public confidence and international reputation.

Information: any data, published material or records in any form, which is collected, created or received, and which is maintained as evidence in pursuance of legal obligations or in the transaction of business.

Reliability status: the minimum standard of security screening for positions requiring unsupervised access to Government of Canada protected information, assets, facilities or information technology systems. Security screening for reliability status appraises an individual's honesty and whether he/she can be trusted to protect CSC's interests. Security screening for reliability status can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions.

Security Advisory Committee (SAC): the governance body for the effective implementation and maintenance of a security program, management of security controls and the achievement of control objectives.

Security clearance: the standard of security screening for all positions requiring access to Government of Canada classified information, assets, facilities or information technology systems. Security screening for a security clearance appraises an individual's loyalty to Canada and his/her reliability as it relates to that loyalty. Security screening for security clearance can include enhanced inquiries, verifications and assessments when duties involve or directly support security and intelligence functions.