COMMISSIONER'S DIRECTIVE 564-2	In Effect: 2015-02-09 Last Review: 2015-02-09 Due for Review: 2017-02-09

Departmental Physical Security

PROGRAM ALIGNMENT	Internal Services
OFFICE(S) OF PRIMARY INTEREST	Correctional Operations and Programs Sector
ONLINE @	• http://infonet/cds/cds/564-2-cd-eng.pdf • http://infonet/cds/cds/564-2-cd-fra.pdf • http://www.csc-scc.gc.ca/text/plcy/cdshtm/564-2-cd-eng.shtml • http://www.csc-scc.gc.ca/text/plcy/cdshtm/564-2-cd-fra.shtml
AUTHORITIES	• *Canada Labour Code* • Treasury Board Directive on Departmental Security Management • Treasury Board Policy on Government Security • Treasury Board Policy on Management of Real Property • Treasury Board Policy on Occupational Safety and Health
PURPOSE	• The objective of this policy is to develop and define Correctional Service of Canada (CSC) standards in compliance with the Policy on Government Security (PGS) and related directives and standards
APPLICATION	Applies to all CSC employees and individuals who have access to government information, property and assets under CSC's jurisdiction

CONTENTS

22 – 23	Standards for the Transport and Transmittal of Information
24 – 28	Standards for the Destruction of Material and Information
29	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 Director General, Security, will act as a liaison between the members of the Executive Committee and members of the Security Advisory Committee. He/she will also chair the Committee, which oversees departmental security directions within CSC.

3. The Departmental Security Officer (DSO) will:

   a. ensure a standardized approach to departmental security within the organization

   b. serve as a subject matter expert on the Treasury Board physical security standards applicable to all CSC facilities.

4. The Director General, Technical Services and Facilities, will:

   a. serve as the subject matter expert on the CSC technical security requirements in institutions, Community Correctional Centres (CCCs) and parole offices

   b. liaise closely with the Departmental Security Division on departmental security matters

   c. approve and oversee construction, renovations and refits in CSC facilities.

5. The Regional Deputy Commissioners will ensure that this directive is implemented at all CSC facilities.

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

   a. ensure that a Threat and Risk Assessment (TRA) is completed and security measures are in place for the safety and security of individuals, information and CSC assets

   b. ensure that identified deficiencies are addressed and corrective measures are applied

   c. investigate all security incidents and breaches

d. collaborate with the Regional Manager, Information Technology Security (RMITS), to identify and validate information technology security risks pursuant to CD 225 – Information Technology Security.

7. Managers at all levels will comply with the Treasury Board Operational Security Standard on Physical Security and with the RCMP Policy Instruments, Guidelines and Tools in the following areas:

   a. physical security

   b. safeguarding of information and assets

   c. protection of facilities

   d. protection of all individuals.

8. Individuals will apply the physical security requirements and protection measures in accordance with the Treasury Board Operational Security Standard on Physical Security.

PHYSICAL SECURITY PROCEDURES

9. Threats and residual risks identified in a TRA will be addressed by implementing appropriate safeguards to mitigate the risks to an acceptable level. These safeguards must be pursuant to the Treasury Board Operational Security Standard on Physical Security and the CSC Technical Criteria for Correctional Institutions.

10. All security incidents/breaches and any security deficiencies will be reported in accordance with CD 568-1 – Recording and Reporting of Security Incidents.

Facilities Standards

11. The standards for CSC office/administrative facilities (e.g. National and Regional Headquarters, including administrative facilities within the institutions), warehouses or other unspecified facilities are governed by CSC's obligations under the Policy on Government Security and its related standards and the CSC Technical Criteria for Correctional Institutions.

12. Where CSC is the tenant of a facility, CSC must inform the custodian department of its security requirements for the location and make arrangements to fulfil these requirements.

13. Where CSC is the custodian of a facility and shares the facility with other organizations, CSC must apply the appropriate measures identified in a TRA in order to preserve the safety and security of the building and its occupants, based on the risks generated by all tenants.

14. Where a CSC office is located in a multi-tenant facility, the demising walls will be built in accordance with the RCMP Guide G13-02 Secure Demising Wall.

15. CSC must ensure that access to, and safeguards for, protected or classified information and assets are based on a clearly discernible hierarchy of zones. There are five zones that should be applied based on the TRA, as defined in the RCMP Guide G1-026 Guide to the Application of Physical Security Zones: (*Note: The Inmate/Offender Access Zone was added to the Treasury Board Hierarchy of Zones to meet CSC's operational requirements.*)

    a. Public Zone

    b. Reception Zone

    c. Inmate/Offender Access Zone (protected and classified information must not be stored in this zone and should not be processed unless necessary and only when inmates/offenders are under direct supervision)

    d. Operations Zone (at a minimum, Protected A and B and confidential information must be processed and stored in this zone)

    e. Security Zone (at a minimum, Protected C, Secret and Top Secret information must be processed and stored in this zone)

    f. High Security Zone.

    The definition of each zone and examples of assets found in each one based on their sensitivity level are defined in Annex A, and the minimum measures are defined in Appendix B of the Treasury Board Operational Security Standard on Physical Security.

Access Control

16. For all CSC facilities other than a designated institution (e.g. National and Regional Headquarters, CORCAN, local training depots, etc.), access control is defined in the Treasury Board Operational Security Standard on Physical Security and in the RCMP Guide G1-024 Control of Access.

17. All institutional access controls are defined in CD 566-1 – Control of Entry to and Exit from Institutions.

Storage Standards

18. Appendix B of the Treasury Board Operational Security Standard on Physical Security defines the minimum standards and security equipment required for asset storage, based on the level of sensitivity, protection and classification of information and assets.

19. According to the Treasury Board Operational Security Standard on Physical Security, all employees who work outside of the department must protect information in a manner consistent with the

minimum standards set out in Appendix B. The Treasury Board Telework Policy also provides related clarification.

20. Contractors must comply with the security requirements identified in the contract and in the Security Requirements Check List (SRCL).

21. Open shelve storage of protected and/or classified information must be in accordance with the Treasury Board Operational Security Standard on Physical Security, section 7.6.7 Secure rooms and with the RCMP Guide G13-01 Secure Storage Rooms.

Standards for the Transport and Transmittal of Information

22. Standards for the transport and transmittal of protected and classified assets have been established and are set out in Appendix C of the Treasury Board Operational Security Standard on Physical Security.

23. RCMP Guide G1-009 Transport and Transmittal of Protected and Classified Information is applicable in these circumstances.

Standards for the Destruction of Material and Information

24. Every unit must follow the CSC approved procedures for the destruction of valuable, protected and classified assets. Contact the National Headquarters Information Management Division, the Central Registry or Main Records Office for further direction and guidance.

25. Various destruction standards and mechanisms must be in place for protected and classified assets:

    a. Protected A and B information on paper must be destroyed to the maximum shred sizes, in accordance with the RCMP Guide G1-001 Security Equipment Guide, Destruction Equipment Selection Guide

    b. Protected C and all levels of classified information on paper must be destroyed in a shredder approved for the classification level, in accordance with the RCMP Guide G1-001 Security Equipment Guide, Destruction Equipment Selection Guide.

26. The person assigned to destroy protected or classified waste must hold a valid reliability status or security clearance consistent with the classification level of information and/or asset being destroyed.

27. Suppliers of destruction services approved by the Canadian Industrial Security Directorate of Public Works and Government Services Canada through a contract or standing offer have the ability to destroy Protected A and B information only without the presence of a CSC employee, provided all other secure destruction requirements pursuant to section 4 of the RCMP Guide G1-001 Security Equipment Guide, Destruction Equipment Selection Guide are met. For classified and Protected C information, all aspects of the destruction process, from pick-up, to transport, to final destruction,

must be under the continuous supervision of an appropriately security-screened departmental employee.

28. The information contained on electronic media must be destroyed in accordance with the information technology security guides and reports contained in the Communications Security Establishment Canada Clearing and Declassifying Electronic Data Storage Devices – ITSG-06.

ENQUIRIES

29. 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 564 – Departmental Security
CD 566-1 – Control of Entry to and Exit from Institutions
CD 568-1 – Recording and Reporting of Security Incidents

Communications Security Establishment Canada Clearing and Declassifying Electronic Data Storage Devices – ITSG-06
RCMP Guide G1-001 Security Equipment Guide *(Access is **restricted** to Government of Canada departments and agencies)*
RCMP Guide G1-009 Transport and Transmittal of Protected and Classified Information *(Access is **restricted** to Government of Canada departments and agencies)*
RCMP Guide G1-024 Control of Access
RCMP Guide G1-025 Protection, Detection and Response
RCMP Guide G1-026 Guide to the Application of Physical Security Zones
RCMP Guide G13-01 Secure Storage Rooms
RCMP Guide G13-02 Secure Demising Wall
RCMP Guidelines and Reports on IT Security
Treasury Board Telework Policy
Treasury Board Operational Security Standard on Physical Security

DEFINITIONS

The following definitions were established for the purpose of developing this directive (as defined in Treasury Board policy):

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

Classified assets: assets whose compromise would reasonably be expected to cause injury to the national interest.

Classified information: information related to the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or *Privacy Act*, and the compromise of which would reasonably be expected to cause injury to the national interest.

Custodian department: a department having administration of federal real property.

Facility: a physical setting used to serve a specific purpose. A facility may be part of a building, a whole building, or a building plus its site; or it may be a construction that is not a building. The term encompasses both the physical object and its use (e.g. weapons ranges, agriculture fields).

***High Security Zone**: an area to which access is limited to authorized, appropriately-screened personnel and authorized and properly-escorted visitors; it must be indicated by a perimeter built to the specifications recommended in the TRA, monitored continuously (e.g. 24 hours a day and 7 days a week) and be an area to which details of access are recorded and audited. Example: an area where high-value assets are handled by selected personnel.

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.

Inmate/Offender Access Zone: areas where offenders have unescorted access inside and outside correctional facilities. Examples: the grounds inside the fence surrounding a federal correctional facility, areas inside federal correctional institutions, Community Correctional Centres and Parole Offices.

Material: any tangible object with the exclusion of those embodying information.

***Operations Zone**: an area where access is limited to personnel who work there and to properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored periodically. Examples: typical open office space, areas where Protected A and B information is processed and/or safeguarded, or typical electrical, telecom and LAN rooms.

Physical security: the use of physical safeguards to prevent or delay unauthorized access to assets, to detect attempted and actual unauthorized access and to activate appropriate responses.

Protected asset or information: an asset or information that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act* because its disclosure would reasonably be expected to compromise the non-national interest.

Protection: for physical security, protection means the use of physical, procedural and psychological barriers to delay or deter unauthorized access, including visual and acoustic barriers.

Public Zone: where the public has unimpeded access and generally surrounds or forms part of a government facility. Examples: the grounds surrounding a building, or public corridors and elevator lobbies in multiple occupancy buildings. At CSC medium and maximum security facilities, the Public Zone is outside the fence surrounding the facility.

Reception Zone: where the transition from a Public Zone to a restricted-access area is demarcated and controlled. It is typically located at the entry to the facility where initial contact between visitors and the department occurs; this can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons.

Restricted-access area: work areas where unescorted access is limited to authorized and security screened individuals only, includes Operations, Security and High Security Zones.

Risk: the chance of a vulnerability being exploited.

***Security Zone**: an area to which access is limited to authorized personnel and to authorized and properly-escorted visitors; it must be indicated by a recognizable perimeter and monitored continuously (e.g. 24 hours a day and 7 days a week). Example: an area where Protected C and Secret information is processed and/or stored.

Threat: any potential event or act, deliberate or accidental, that could cause injury to employees or assets.

Zones: a series of clearly discernible spaces to progressively control access.

*The following three zones are restricted-access areas to authorized and security screened individuals only and to properly escorted visitors: Operations Zone, Security Zone and High Security Zone.