



Print version



DP 051

2007-01-29

DEPARTMENTAL SECURITY PROGRAM

Table of Contents

1. [Background](#)
 2. [Policy](#)
 3. [Scope](#)
 4. [Definitions](#)
 5. [Roles and Responsibilities](#)
 6. [Guidelines and Procedures](#)
 7. [Compliance](#)
 8. [References](#)
 9. [Cancellation](#)
 10. [Inquiries](#)
- [Annex A - Distributed Departmental Security Structure](#)
 - [Annex B - PWGSC Departmental Security Committee - Terms of Reference](#)

1. BACKGROUND

The stated objective of the Treasury Board's [Government Security Policy](#) (GSP) is to support the national interest and the Government of Canada's business objectives by safeguarding employees and assets and assuring the continued delivery of services. According to the GSPGSP, government departments must establish and direct a security program to ensure both the coordination of all GSPGSP functions and the implementation of GSPGSP requirements.

To apply the GSP, Public Works and Government Services Canada (PWGSC) has adopted a distributed governance structure for security, which is illustrated in [Annex A](#). This departmental policy (DP) establishes the framework for the Departmental Security Program in connection with the distributed governance structure. It also serves as the common reference for all other DPs that concern security.

Note: Wherever "protected information" is mentioned, this term includes personal information.



2. POLICY

Public Works and Government Services Canada shall:

- a. Fulfill the following responsibilities in line with its role as a lead security department under the GSP:
 1. Develop and deliver the Industrial Security Program on behalf of the federal government to ensure that classified and protected information in the care of Canadian and international private sector organizations is properly safeguarded and to prevent unauthorized access to controlled goods in Canada. This responsibility entails the following activities:
 - a. Developing operational standards and technical documentation on security in contracting, in consultation

- with the Treasury Board of Canada Secretariat and other departments;
 - b. Conducting the security screening of private industry contractor personnel;
 - c. Ensuring adequate security provisions in contract clauses;
 - d. Ensuring the security compliance and inspection of companies that have access to protected and classified information and assets (both Canadian and foreign);
 - e. Making administrative arrangements for international visitors;
 - f. Ensuring that security requirements for the transportation of documents are met;
 - g. Ensuring that appropriate measures for the examination, possession, transfer and disposition of controlled goods within Canada are taken to prevent the goods from being accessed by unauthorized individuals;
 - h. Developing and providing training on the subject of security in contracting;
 - i. Maintaining a database of private sector organizations and individuals that are security screened for access to government assets;
 - j. Negotiating international industrial security agreements, arrangements and memoranda of understanding on behalf of the Government of Canada, in consultation with Foreign Affairs and International Trade Canada.
2. Control all government communications security ([COMSEC](#)) assets in the private sector;
 3. Ensure that contractors meet the security requirements of contracts that involve information technology security assets;
 4. Ensure the provision of base building security, when it is the custodian department;
 5. Ensure the confidentiality, integrity and availability of common information technology services that PWGSC provides to other departments;
 6. Provide for the continued delivery of its services in accordance with the [GSP](#) (including the GSP's [operational standards](#)) by means of baseline security measures, business continuity planning and continuous risk management.
- b. Safeguard protected and classified information and other assets under its control in accordance with the [GSP](#), including the [GSP's operational standards](#).
 - c. Ensure the safety and security of its employees in accordance with [Part II of the Canada Labour Code](#) and the [GSP](#), including the GSP's [operational standards](#).
 - d. Incorporate security requirements into all departmental planning, operations and accommodations, including, but not limited to:
 1. Construction and modification projects undertaken by PWGSC as an occupant, as a custodian department, and as the federal lead agency for providing base building security to support general purpose office accommodation;
 2. Contracts let by PWGSC as a contracting authority as well as pre-contractual documents under its responsibility;
 3. Information technology projects undertaken by PWGSC as a common service provider.
 - e. Report and investigate actual or suspected breaches and violations of security and privacy, take the necessary corrective action, and maintain a record of all investigations and related recommendations
 - f. Report on and conduct special investigations into evidence, allegations or suspicion of employee involvement in the following activities:
 1. Fraud;
 2. Misappropriation;

3. Defalcation;
4. Violation of laws, regulations and departmental guidelines for conduct in the workplace;
5. Other activities that are not in the interest of PWGSC.



3. SCOPE

This DP applies to all employees of PWGSC, including its Special Operating Agencies; to other persons having authorized access to protected and classified information and other assets (as defined by the [GSP](#)) that are associated with government programs, contracts and other arrangements administered by PWGSC; and to other persons who are authorized under the Industrial Security Program to examine, possess or transfer controlled goods for which PWGSC is responsible.


Separate DPs have been issued to describe individual elements of the Departmental Security Program, including corporate security, information technology security, industrial security and business continuity planning as well as investigations into fraud, conflict of interest, and wrongdoing revealed by internal disclosure. These policies are listed in section 9, "References."



4. DEFINITIONS

Breach of security (*infraction à la sécurité*) means an action that results in the compromise of protected or classified assets (including information) or controlled goods.

Classified assets (*biens classifiés*) means assets whose unauthorized disclosure would reasonably be expected to cause injury to the national interest.

Classified information (*renseignements classifiés*) means information related to the national interest that may qualify for an exemption or exclusion under the [Access to Information Act](#) or the [Privacy Act](#), and the compromise of which would reasonably be expected to cause injury to the national interest. Such information is categorized as Confidential (when the potential injury is just above the threshold of the national interest), Secret (when the potential injury is serious) or Top Secret (when the potential injury is exceptionally grave). See also the "[Departmental Consolidated Information & Assets Classification and Designation Guide](#)." 

Compromise (*compromission*) means the unauthorized disclosure, destruction, removal, modification, interruption or use of assets (as defined by the [Government Security Policy](#)), or the unauthorized examination, possession or transfer of controlled goods.

Controlled goods (*marchandises contrôlées*) means the goods to which the [schedule for section 35 of the Defence Production Act, Part 2](#), refers.

Information technology security (*sécurité des technologies de l'information*) means the safeguards to preserve the confidentiality, integrity, availability, intended use and value of electronically stored, processed or transmitted information.


National interest (*intérêt national*) means that which concerns the defence and maintenance of the social, political and economic stability of Canada.




Personal information (*renseignements personnels*) means information recorded in any form about an identifiable individual as per the definition of "personal information" in section 3 of the [Privacy Act](#). This includes, but is not limited to, the following types of information about an individual: race, age and marital status; education; medical, criminal, financial and employment history; any identifying number assigned to the individual; fingerprints; address; personal views; and so on. It does not include certain information regarding the position and functions of a government employee (*Privacy Act*, section 3, definition of "personal information," paragraph (j)), the services performed by an individual under contract for a government institution (*ibid.*, para. (k)), a discretionary benefit of a financial nature (*ibid.*, para. (l)), or an individual who has been dead for more than twenty years (*ibid.*, para. (m)). Personal information is a subset of protected information.

Protected assets (*biens protégés*) means assets whose unauthorized disclosure would reasonably be expected to cause injury to a non-national interest.

Protected information (*renseignements protégés*) means information that is not related to the national interest but may qualify for an exemption or exclusion under the [Access to Information Act](#) or the [Privacy Act](#), and the compromise of which

would reasonably be expected to cause injury to a non-national interest.

Security incident investigations (*enquêtes sur les incidents de sécurité*) means investigations into any of the following circumstances: threats uttered against departmental employees; violence in the workplace (which is the subject of [DP 076 – Violence in the Workplace](#) ); breaches and violations of security; obstruction of the right to access information under the [Access to Information Act](#) and the [Privacy Act](#); property damage and other losses to the Crown that result from vandalism, breaking and entering, and theft; illegal or otherwise unlawful use of government equipment; and other offences and illegal acts against the Crown.





Special investigations (*enquêtes spéciales*) means investigations into activities that fall within the purview of [DP 026 – Audit and Ethics Branch Investigation](#)  and are proscribed by the [Treasury Board's Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown](#) (including fraud, misappropriation and defalcation), by the [Criminal Code](#) or by other federal legislation in cases where the Crown is a victim; into non-compliance with [DP 063 – Conflict of Interest and Post-Employment](#) ; into wrongdoing under [DP 081 – Internal Disclosure Concerning Wrongdoing in the Workplace](#) ; into complaints of conflict of interest under the [Treasury Board's Values and Ethics Code for the Public Service](#); and into wrongdoing with respect to Receiver General functions.






Threat and risk assessment (*évaluation de la menace et des risques*) means an evaluation of the possibility an asset may be compromised through exploitation of its vulnerabilities, taking into account the effectiveness of existing and proposed security measures.





Violation of security (*manquement à la sécurité*) means any act or omission that contravenes any provision of the [Government Security Policy](#) (GSP). This may include failure to categorize information as classified or protected; categorizing information in a way that conflicts with the GSP; unauthorized modification, retention, destruction or removal of classified or protected information; and unauthorized interruption of the flow of classified or protected information.



5. ROLES AND RESPONSIBILITIES

- a. The Deputy Minister is accountable for safeguarding all employees and assets (including information) under the responsibility of PWGSC and for implementing within PWGSC the legislative requirements for controlled goods.
- b. The Assistant Deputy Minister, Corporate Services, Policy and Communications Branch, is responsible for the following functions:
 1. Administering the Departmental Security Program;
 2. Representing PWGSC on the Assistant Deputy Minister Public Safety Committee;
 3. Representing PWGSC on the Senior Security Policy Advisory Committee.
- c. The Director General, Health, Safety, Security, Emergencies and Administration Sector, is the Departmental Security Officer (DSO). The DSO is responsible for the following functions:
 1. Representing PWGSC in dealings with the Treasury Board Secretariat and other government departments in respect of the [GSP](#);
 2. Representing PWGSC on the DSO Readiness Committee, which is chaired by the Privy Council Office;
 3. Directing the Departmental Security Program in accordance with the [GSP](#), including the GSP's [operational standards](#). This involves developing, implementing, maintaining and monitoring the program in close consultation with all the designated authorities who are responsible for elements of the distributed governance structure for security;
 4. Directing the Corporate Security Program, which is the subject of [DP 052 – Corporate Security Program](#) ;
 5. Directing the Special Investigations Program in connection with [DP 026](#) , [DP 063](#)  and [DP 081](#) ;
 6. Interpreting the [GSP](#), including the [GSP's operational standards](#), on behalf of PWGSC;
 7. Promulgating departmental security policies;
 8. Developing departmental standards and procedures for threat and risk assessments;

9. Chairing the Departmental Security Committee, which is composed of representatives from organizations within PWGSC's distributed governance structure for security and ad hoc representatives from other departmental organizations. This committee coordinates the delivery of the Departmental Security Program, advises the DSO, and serves as the review and approval body for all departmental policies concerning health, safety and security. (See [Annex B](#), "Departmental Security Committee Terms of Reference");
 10. Providing functional direction to the regional security authorities.
- d. The Director, Corporate Security Directorate, is the Associate Departmental Security Officer (ADSO). The ADSO is responsible for the following activities:
1. Supporting the DSO through administration of functions for which the DSO is responsible;
 2. Directing the operations of the Corporate Security Program ([DP 052](#) ) , whose objectives are the following:
 - a. The protection of personnel, information and other assets across PWGSC;
 - b. The protection of buildings for which PWGSC is responsible as the lead agency for providing base building security to support general purpose office accommodation;
 - c. The integrity of national critical infrastructure under PWGSC's responsibility;
 - d. The availability of PWGSC's critical infrastructure to the Government and to Canadians.
 3. Administering the Security Intelligence Analysis Program, which includes the following activities:
 - a. Obtaining, collating and analyzing information concerning the security of PWGSC personnel, services, information, critical infrastructure and other assets;
 - b. Providing PWGSC's senior managers with threat assessments, trend analysis, advice and other information drawn from security intelligence in advance of potentially harmful events;
 - c. Coordinating information analysis in support of PWGSC's response to changes in security readiness levels as defined by the GSP's ["Operational Security Standard – Readiness Levels for Federal Government Facilities."](#)
 4. Directing the Parliamentary Precinct Security Program and the Ministers' Regional Office Security Program.
- e. The Director, Corporate Emergency Preparedness Directorate, is responsible for coordinating the Business Continuity Planning Program.
- f. The Director, Special Investigations Directorate, is responsible for the following activities:
1. Conducting special investigations in line with [DP 026](#) , [DP 063](#)  and [DP 081](#) ;
 2. Conducting security incident investigations at the request of the Director, Corporate Security Directorate.
- g. The Assistant Deputy Minister, Consulting, Information and Shared Services Branch, is responsible for administering the Industrial Security Program, which is the subject of [DP 054 – Industrial Security Program](#) . This program comprises the service lines named Contract Security and Controlled Goods, and it includes the following elements:
1. Security in contracting;
 2. Personnel security screening;
 3. Organization security screening;
 4. International industrial security;
 5. Joint Certification Program;
 6. Analysis of foreign ownership, control and influence;
 7. Controlled goods.

- h. The Director General, Industrial Security Sector, is responsible for delivering the Industrial Security Program ([DP 054](#) ). The Director General delivers this program through the Canadian and International Industrial Security Directorate and the Controlled Goods Directorate.
- i. The Assistant Deputy Minister, Information Technology Services Branch, is responsible for administering the Information Technology Security Program, which is the subject of [DP 055 – Information Technology \(IT\) Security Program](#) .
- j. The Director, Information Technology Security Directorate, is responsible for directing the operations of the Information Technology Security Program ([DP 055](#) ). The Director is also the Departmental Information Technology Security Coordinator.
- k. The Assistant Deputy Minister, Real Property Branch, is responsible for providing base building security in line with the [GSP](#) where PWGSC administers real property as a custodian department. This responsibility includes, but is not limited to, the following functions:
 - 1. Providing and funding physical security safeguards to protect the base building assets of facilities;
 - 2. Constructing or modifying security features as needed to enhance the protection of base building assets above the minimum required level;
 - 3. Researching and developing security-related building technologies for incorporation into the design, construction and renovation of facilities;
 - 4. Verifying that base building safeguards and related activities (including work performed under contract) comply with the [GSP](#).
- l. The Director General, Professional and Technical Programs Sector, is responsible for the following functions:
 - 1. Promulgating and implementing the GSP's [operational standards](#) in connection with base building security;
 - 2. Coordinating base building threat and risk assessments;
 - 3. Applying PWGSC's security programs to the fulfillment of custodian department responsibilities under the [GSP](#);
 - 4. Directing the research and development of security-related building technologies.
- m. The Director General, Audit and Evaluation Branch, is responsible for conducting periodic audits of the Departmental Security Program.
- n. The Branch/Agency Heads are responsible for funding and applying within their organizations the security programs and measures that have been approved by PWGSC.
- o. Managers are responsible for implementing the Departmental Security Program within their organizational units.
- p. Human Resources officials are responsible for providing managers with functional advice and assistance for implementing [DP 052 – Corporate Security Program](#)  as part of the Departmental Security Program.
- q. Employees and persons engaged under contract are responsible for applying and adhering to the security procedures that have been approved by PWGSC for safeguarding protected and classified information and other assets under their control.



6. GUIDELINES AND PROCEDURES

Detailed guidelines and procedures for implementing the Departmental Security Program and its constituent elements (except controlled goods) are promulgated in the documents listed under "PWGSC Publications" in section 8. Policies and guidelines for controlled goods are posted on the [Controlled Goods Directorate](#) website.



7. COMPLIANCE

It is mandatory to comply with this DP, which is subject to the [GSP](#), GSP-related legislation, and the [Defence Production Act, Part 2](#).



8. REFERENCES

Acts and Regulations:

- [Access to Information Act](#);
- [Canada Labour Code, Part II](#);
- [Controlled Goods Regulations](#);
- [Criminal Code](#);
- [Defence Production Act, Part 2](#);
- [Financial Administration Act](#);
- [Privacy Act](#).

Treasury Board Policies:

- [Government Security Policy](#), which includes [operational security standards](#) such as the following:
 - ["Operational Security Standard: Management of Information Technology Security \(MITS\)"](#);
 - ["Operational Security Standard on Physical Security"](#);
 - ["Operational Security Standard – Readiness Levels for Federal Government Facilities"](#);
 - ["Security Organization and Administration Standard."](#)
- [Policy on Losses of Money and Offences and Other Illegal Acts Against the Crown](#);
- [Values and Ethics Code for the Public Service](#).

PWGSC Publications:

- [DP 001 – Policy for Emergency Preparedness in Public Works and Government Services Canada](#) ;
- [DP 014 – Protection of Personal and Private Information in the Workplace](#) ;
- [DP 026 – Audit and Ethics Branch Investigation](#) ;
- [DP 052 – Corporate Security Program](#) ;
- [DP 053 – Reporting of Actual and Suspected Breaches and Violations of Security](#) ;
- [DP 054 – Industrial Security Program](#) ;
- [DP 055 – Information Technology \(IT\) Security Program](#) ;
- [DP 063 – Conflict of Interest and Post-Employment](#) ;
- [DP 076 – Violence in the Workplace](#) ;
- [DP 081 – Internal Disclosure of Information Concerning Wrongdoing in the Workplace](#) ;
- [AFD Management Handbook Standard Operating Procedure: Base Building Security](#) ;
- [National Call Letter Building Management Plans](#) ;
- [Supply Manual](#).



9. CANCELLATION

This version of DP 051 supersedes the one dated 2003-02-13.



10. INQUIRIES

Departmental Security Officer and
 Director General
 Health, Safety, Security, Emergencies and Administration Sector
 Corporate Services, Policy and Communications Branch
 819-956-3121

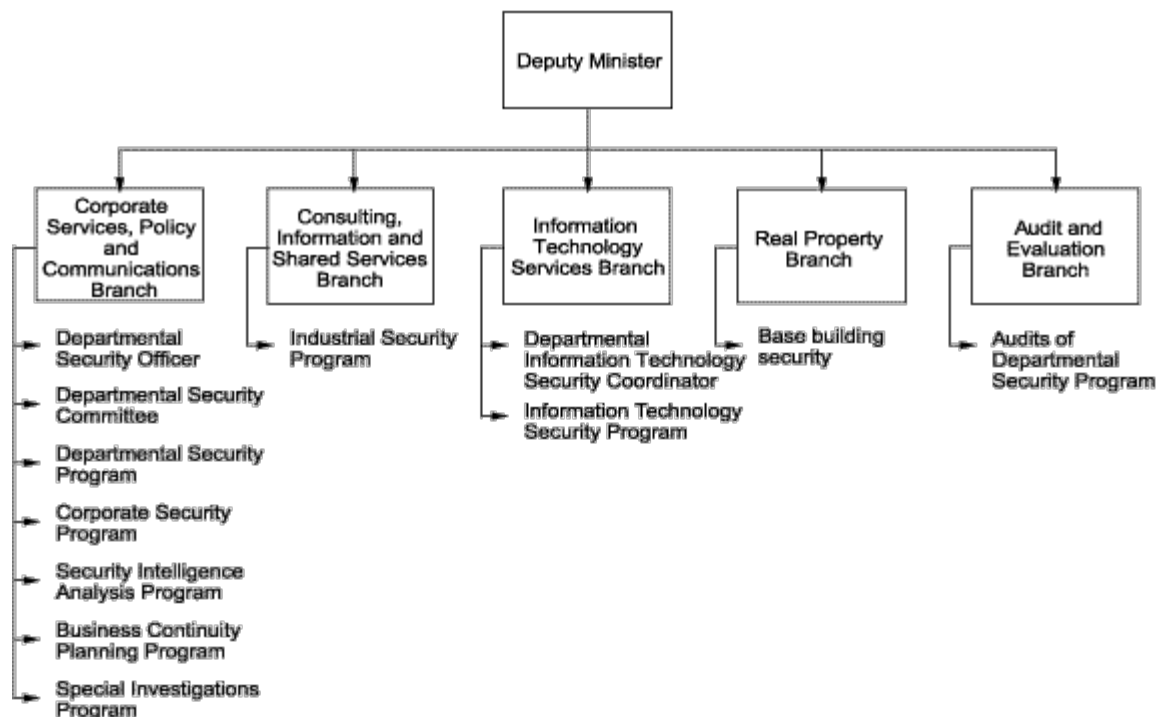
Associate Departmental Security Officer and
 Director
 Corporate Security Directorate
 Health, Safety, Security, Emergencies and Administration Sector
 Corporate Services, Policy and Communications Branch
 819-956-2826

Original Signed by
I. David Marshall

I. David Marshall
Deputy Minister and
Deputy Receiver General for Canada



Annex A - Distributed Departmental Security Structure



- Deputy Minister
 - Corporate Services, Policy and Communications Branch
 - Departmental Security Officer
 - Departmental Security Committee
 - Departmental Security Program
 - Corporate Security Program
 - Security Intelligence Analysis Program
 - Business Continuity Planning Program
 - Special Investigations Program
 - Consulting, Information and Shared Services
 - Industrial Security Program
 - Information Technology Services Branch
 - Departmental Information Technology Security Coordinator
 - Information Technology Security Program
 - Real Property Branch
 - Base building security
 - Audit and Evaluation Branch
 - Audits of Departmental Security Program



Annex B - Departmental Security Committee - Terms of Reference

1. PURPOSE

The Departmental Security Committee (DSC) coordinates the delivery of the Departmental Security Program and serves as an advisory body to the Departmental Security Officer (DSO). It also serves as the review and approval body for all departmental policies (DPs) concerning health, safety and security. However, it does not direct the operations of its members' organizations.

2. SCOPE

The DSC follows the [Government Security Policy](#)'s example in using the term "security" to cover safeguards associated with personnel, information, physical assets, information technology and contracting; safety against violence; and emergency preparedness. The DSC examines all these elements and provides strategic advice to the DSO for possible application across PWGSC. However, the DSC does not take the place of other advisory bodies, such as the National Health and Safety Committee and the Emergency Preparedness Network.

3. COMMITTEE MEMBERSHIP

Chair

The DSC is chaired by the DSO in the person of the Director General, Health, Safety, Security, Emergencies and Administration Sector, Corporate Services, Policy and Communications Branch. On account of having a formal role in providing senior management with security advice and guidance, the DSO is able to elevate the concerns of DSC members.

Members

DSC members include the following:

- a. Representatives from organizations within the distributed governance structure for security:
 1. Corporate Services, Policy and Communications Branch:
 - Health, Safety, Security, Emergencies and Administration Sector:
 - DSO and Director General, Health, Safety, Security, Emergencies and Administration Sector;
 - Associate Departmental Security Officer and Director, Corporate Security Directorate;
 - Director, Corporate Environment, Health and Safety Directorate;
 - Director, Corporate Emergency Preparedness Directorate;
 - Director, Special Investigations Directorate.
 2. Consulting, Information and Shared Services Branch:
 - Director General, Industrial Security Sector.
 3. Information Technology Services Branch:
 - Departmental Information Technology Security Coordinator and Director, Information Technology Security Directorate, PWGSC Chief Information Officer Functions Sector.
 4. Real Property Branch:
 - Director, Asset and Facilities Management Directorate, Professional and Technical Programs Sector.
 5. Human Resources Branch:
 - Director, Labour Relations Directorate, Labour Relations and Compensation Sector.
 6. A regional director general.
- b. When required, additional representatives from departmental organizations that have some responsibility for business continuity planning and other elements of security, but are not part of the distributed governance structure for security:
 1. Director, Professional Development and Change Management Directorate, Risk, Integrity and Strategic Management Sector, Acquisitions Branch;
 2. A representative from the Accounting, Banking and Compensation Branch;
 3. Director, Business Support Services, Corporate Services, Translation Bureau.

4. FUNCTIONS

- a. DSC members will advise the Chair (serving the role of DSO) of concerns, issues, opportunities, events, etc., affecting the implementation of the Departmental Security Program.
- b. The DSC shall ensure a coordinated approach to the following activities of individual organizations:
 1. Development of departmental security policies and operational and technical standards to implement the requirements of the [Government Security Policy](#) (GSP);
 2. Implementation of a certification and accreditation program for information technology systems;

3. Introduction and application of security risk management principles and practices;
 4. Development and application of security training standards;
 5. Delivery of PWGSC's security awareness programs;
 6. Delivery of the Industrial Security Program;
 7. Development and implementation of a program to investigate security incidents and advise the Deputy Minister on subsequent sanctions for misconduct and negligence;
 8. Dissemination of security intelligence that may apply to the whole of PWGSC.
- c. The DSC shall exercise approval authority for all DPs regarding security.
 - d. The DSC will coordinate the annual review of security-related operational plans in order to ensure adherence to the [GSP](#), strategic priorities and objectives in departmental security, and other departmental objectives.
 - e. The DSC shall serve as a forum for consultation and exchange of information on the following items:
 1. Individual projects and action plans developed by each organization within the distributed governance structure for security
 2. Directives and guidelines issued by lead departments and central agencies.
 - f. The DSC shall support PWGSC's Business Continuity Planning Program in line with the governance requirements of the [GSP's "Operational Security Standard – Business Continuity Planning \(BCP\) Program." section 3.1.](#)
 - g. The DSC may meet for consultation before notifying the Deputy Minister of a significant threat that could result in a change to PWGSC's level of security.
 - h. The DSC may conduct post-mortem assessments of major security incidents.
 - i. The DSC shall ensure that security directives from the Privy Council Office which apply to PWGSC are implemented.

5. ADMINISTRATION

Schedule: The DSC shall meet at least once every quarter, at the call of the Chair.

Personnel screening requirement: All members and their representatives must hold at least a Secret clearance.

Minutes: Minutes of meetings will be prepared by the Health, Safety, Security, Emergencies and Administration Sector and will be circulated to members for approval.

