Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada
Canada

Print version

Print Close

DP 104 (Amended)
2012-08-06
POLICY ON INFORMATION TECHNOLOGY SECURITY

TABLE OF CONTENTS

1. EFFECTIVE DATE

This departmental policy (DP) takes effect on: 2012-08-06

2. CONTEXT

In response to the Treasury Board (TB) *Policy on Government Security*, Public Works and Government Services Canada (PWGSC) has adopted a distributed security structure to implement the Departmental Security Program. Within this context, the Information Technology Services Branch (ITSB) has been assigned overall responsibility for the Departmental Information Technology (IT) Security Program. The management of the Program has been delegated to the IT Security Coordinator. This *Policy on Information Technology Security* has been developed in support of the Departmental IT Security Program.

This DP is to be read in conjunction with the *Federal Accountability Act, Departmental Security Program (051)* and the following TB policy instruments: *Policy on Management of Information Technology, Policy on*

Government Security, Operational Security Standard: Management of Information Technology Security (MITS), Policy Framework for Information and Technology, and any related supporting directives and standards.

The purpose of this DP is to ensure the security of departmental electronic information, IT assets and related services. It establishes the safeguards required to ensure the confidentiality of information while stored, processed or transmitted; the integrity of information and processes, as well as the availability of the information and related systems and services. As well, safeguards applied to the assets used to gather, process, receive, display, transmit, reconfigure, scan, store or destroy information electronically are established and are considered under the realm of IT security.

This DP ensures a common understanding on the part of all key stakeholders of their roles, responsibilities and obligations with respect to IT security.

This DP complies with related departmental and TB policies including the *Policy on Government Security* and other applicable laws and regulations.

3. POLICY STATEMENT

Public Works and Government Services Canada must:

1. maintain and adequately fund an IT Security Program to safeguard electronic information, IT assets and related services based on PWGSC Information Technology Security Principles (ref: Annex B);
2. effectively manage IT security through continuous risk assessment and the implementation, monitoring and maintenance of controls including prevention, detection, response and recovery;
3. monitor, assess and report on IT security activities;
4. ensure that IT security is an integral part of PWGSC programs, services and activities;
5. communicate to all stakeholders their role, responsibilities and accountability with respect to IT security. Refer to the following:
    - Information Technology Security Management (Annex C);
    - Application Security (Annex D);
    - Information Technology Operations Security (Annex E);
    - Information Technology Security Incident Management (Annex F).

4. SCOPE

This DP applies to users of IT in PWGSC branches, special operating agencies (SOA) and regions. Users include employees, volunteers, temporary help agency staff, students, contractors, consultants, and business partners who have been officially authorized to use PWGSC IT.

As well, it applies to the private sector, other levels of government and companies processing sensitive government information and/or using sensitive IT assets for initiatives or contracts issued or administered by

PWGSC, on or off-site, as included in the terms of the contract, and to all providers of IT services to PWGSC.

5. DEFINITIONS

Refer to Annex A.

6. RESPONSIBILITIES AND ACCOUNTABILITIES

1. The Deputy Minister (DM) is accountable for ensuring, under the realm of the Departmental Security Program, that an adequately funded and effective IT security program and supporting management and governance structures are established to safeguard sensitive electronic information and sensitive IT assets and related services under the ownership or control of PWGSC. The DM is also responsible for ensuring the Departmental IT Security Program is monitored and assessed as to its effectiveness, and if it remains appropriate to the needs of the Department. The DM will periodically report to TB on the status of the Departmental IT Security Program as part of the overall reporting on the *Departmental Security Program (051)*.

   Additionally, the DM is responsible for supporting continuous communication initiatives to IT users with respect to their role, responsibilities and accountability.

   The DM shall also appoint the departmental IT Security Coordinator and the Communication Security (COMSEC) Authority.

   N.B. In PWGSC both the responsibilities of the IT Security Coordinator and the COMSEC Authority are vested in the Director, IT Security Directorate.

2. The Director, Corporate Security Directorate, is the Departmental Security Officer (DSO) and is responsible for the Departmental Security Program (ref: *Departmental Security Program [051]*, Section 5).

3. The Chief Information Officer, of Information Technology Services Branch (ITSB) is responsible for:

   1. establishing and maintaining IT infrastructure and application security frameworks;
   2. ensuring that IT systems are certified and accredited prior to approving the systems for operation;
   3. developing and publishing IT security guidelines, procedures and standards related to IT infrastructure, application and operations;
   4. monitoring and reporting on the effectiveness of the IT infrastructure and application security and certification program to the appropriate certifying authority;
   5. providing IT security training and awareness related to applications, operations and infrastructure;
   6. monitoring of cyber threats and of unacceptable use of government IT and electronic networks and reporting incidents / violations to the IT Security Coordinator and Public Safety Canada;
   7. determining action to be taken whenever a safeguard is bypassed;
   8. establishing and maintaining a process to capture and handle digital data in support of

investigations and post-incident analysis;

9. ensuring that IT security incidents and deficiencies are addressed in a timely manner.

4. The IT Security Coordinator is responsible for:

    1. establishing and managing the Departmental IT Security Program as part of the coordinated *Departmental Security Program (051)*;
    2. endorsing all DPs that have IT security implications;
    3. ensuring review of the IT security related portions of Request for Proposals (RFPs) and other contracting documentation issued by PWGSC for PWGSC, including Security Requirements Checklists (SRCL);
    4. endorsing all contracts for external providers of IT security services and/or IT assets issued for PWGSC;
    5. working closely with program and service delivery managers to:
        - ensure IT security needs are met,
        - provide advice on safeguards,
        - advise of the potential impact of new and existing threats,
        - advise on the residual risk of a program or service;
    6. monitoring and reporting, to departmental senior management, compliance with the IT Security Program and this DP;
    7. designing, implementing and promoting an IT security awareness program;
    8. establishing and monitoring an effective process to manage IT security incidents;
    9. serving as the Department's principal IT security contact;
    10. alerting the DSO (Director, Corporate Security Directorate) of potential and actual security problems;
    11. ensuring the development and approval, through the IM/IT governance process, of an architecture of safeguards to protect government information under departmental control;
    12. serving on the Departmental Security Committee and representing the Department with lead agencies for IT security matters;
    13. leading the certification and accreditation program for all departmental IT systems and applications;
    14. providing functional direction and training to departmental Information Systems Security Officers (ISSO);

15. periodically reviewing this DP and its effectiveness;

16. periodically monitoring and assessing the IT Security Program as to its effectiveness and whether it remains appropriate to the needs of the Department;

17. reviewing and reporting to departmental senior management and the DSO on the results of internal audits.

5. Branch / Agency Heads, Regional Directors General, and Directors General are responsible for:

    1. ensuring that the ISSOs, Local Registration Authorities (LRA) and COMSEC custodians are appointed;

    2. establishing and coordinating IT security measures within their organization in support of, and in accordance with, the IT Security Program;

    3. monitoring compliance with this DP by users in their organization and managing the outcome associated with any breaches in a quick, fair and decisive manner;

    4. providing and ensuring adequate funding for regular and frequent review of IT security requirements, including the prompt reporting of any IT security anomalies and violations to their ISSO;

    5. reporting on non-compliance to this DP to the IT Security Coordinator.

6. The Deputy Chief Oversight Officer, Office of Audit and Evaluation, is responsible for conducting periodic audits of departmental compliance with this DP and providing the results to the IT Security Coordinator.

7. The Departmental COMSEC Authority is responsible for:

    1. ensuring custody of cryptographic materiel and records;

    2. developing COMSEC procedures;

    3. checking COMSEC practices and correcting deficiencies;

    4. reporting to the DSO potential and actual COMSEC problems and ensuring that corrective measures are taken;

    5. instructing personnel in the proper handling of COMSEC equipment and related security measures;

    6. reviewing contracts issued by PWGSC for PWGSC for inclusion and adequacy of COMSEC security clauses;

    7. addressing COMSEC security incidents and ensuring the timely application of corrective measures to prevent possible re-occurrence;

    8. ensuring the disposal and destruction of superseded COMSEC materiel as stipulated in current doctrine and procedures;

9. appointing COMSEC custodians and alternate custodians for the stewardship of departmental COMSEC materiel;
10. providing functional direction and training to departmental COMSEC custodians;
11. monitoring COMSEC equipment and procedures of COMSEC custodians in PWGSC;
12. monitoring COMSEC equipment in private sector and industry, as delegated by *the Industrial Security Program (054)*.

8. The Information System Security Officers (ISSO) are responsible for:
    1. acting as points of contact and promoting the IT Security Program within their line of business;
    2. assisting in the interpretation of IT security policies and best practices within their line of business;
    3. assisting in the implementation of an IT security awareness program;
    4. participating in the risk management process for IT applications, systems and services;
    5. working with the Unit Security Officer (USO), the Client Authority and the Regional Security Office or other security groups to ensure that all personnel in the IT environment have appropriate security clearance;
    6. ensuring that IT security aspects are taken into consideration prior to purchasing IT equipment;
    7. ensuring that IT security aspects are included in the process for users leaving the organization;
    8. ensuring appropriate access control to information systems and technology;
    9. ensuring that IT security aspects of IT assets are maintained for IT assets under their purview;
    10. participating in the certification and accreditation of systems owned and developed for their line of business;
    11. monitoring access to information systems and reporting on IT security incidents, security breaches and potential security problems to the IT Service Desk at 1-866-995-6030 and to the Regional Security Office, and ensuring the timely application of corrective measures to prevent possible re-occurrence.

9. Local Registration Authorities (LRA) are responsible for performing Public Key Infrastructure (PKI) credential issuance duties on behalf of PWGSC for services not available through the automated system, or as required, based on operational requirements.

10. Directors, Managers and Supervisors are responsible for:
    1. ensuring that the IT Security Program is implemented within their organizational units;
    2. ensuring that IT security practices and procedures are respected;
    3. ensuring that users under their purview receive IT security awareness training;

4. ensuring that this DP is disseminated and properly observed throughout areas under their control;
5. planning for required IT security activities;
6. establishing local procedures and safeguards for their organization's IT systems and the information stored in them;
7. ensuring that statements of sensitivity, threat and risk assessments, and contingency plans are developed and kept up-to-date for application systems or facilities under their control;
8. ensuring that all violations and breaches of IT security policies and standards are immediately reported to their ISSO;
9. ensuring that appropriate security requirements and clauses are included in IT related contracts, that suppliers meet these requirements and that these requirements are maintained for the entire duration of the contract;
10. responding to recommendations resulting from IT security reviews and confirming to the IT Security Coordinator that the issues have been resolved;
11. authorizing all changes to IT equipment and software through the formalized change control process;
12. monitoring compliance to this DP and reporting non-compliance or security incidents to their branch / agency heads, regional directors general, directors general or regional directors.

11. Users are responsible for:

1. their actions or inactions with respect to IT security;
2. reading, understanding and complying with this DP and the Departmental IT Security Program to safeguard electronic information, IT assets and related services to which they have access, against unauthorized access, interruption or modification, and against theft or damage;
3. maintaining IT security measures, in accordance with the Departmental IT Security Program, at their work environment;
4. reporting all, actual or suspected, IT security anomalies and violations to their manager and ISSO or Regional Security Office. The ISSO or the user must also contact the IT Service Desk at 1-866-995-6030 as soon as possible.

7. COMPLIANCE AND REPORTING

Monitoring on the effectiveness of this DP will be carried out in a variety of ways including, but not limited to, assessments under the Management Accountability Framework and the review of results of audits e.g. security audits.

Consequences of non-compliance with this DP can include any measure allowed by the *Financial Administration Act*.

8. REFERENCES

Acts and Regulations:

- *Access to Information Act;*
- *Canadian Charter of Rights and Freedoms;*
- *Canadian Human Rights Act;*
- *Copyright Act;*
- *Criminal Code;*
- *Crown Liability and Proceedings Act;*
- *Department of Public Works and Government Services Act;*
- *Export and Import Permits Act;*
- *Federal Accountability Act;*
- *Financial Administration Act;*
- *Library and Archives of Canada Act;*
- *Patent Act;*
- *Privacy Act;*
- *Security of Information Act;*
- *Trade-marks Act.*

Treasury Board Publications:

- *Access to Information - Policies and Publications;*
- *Integrated Risk Management Framework;*
- *Management Accountability Framework;*
- *Operational Security Standard: Management of Information Technology Security (MITS);*
- *Policy Framework for Information and Technology;*
- *Policy on Government Security;*
- *Policy on Information Management;*
- *Policy on Management of Information Technology;*
- *Policy on the Use of Electronic Networks;*
- *Privacy and Data Protection - Policies and Publications;*
- *Risk Management Policy;*
- *Telework Policy;*
- *Values and Ethics Code for the Public Service.*

PWGSC Publications:

- *Corporate Security Program (052);*
- *Departmental Security Program (051);*
- *Directive on Discipline (111-1);*.
- *Policy on Emergency Management in Public Works and Government Services Canada (001);*
- *Industrial Security Program (054);*
- *Infoguide - Departmental Consolidated Information and Assets Classification and Designation Guide*;
- *Integrated Risk Management Policy (082);*
- *Management of Electronic Mail (067);*
- *Policy on Access to Information and Privacy Acts (002);*
- *Policy on the Allocation and Usage of Information Technology (103);*
- *Protection of Personal and Private Information in the Workplace (014);*
- *PWGSC Management Framework for Communications on the Internet and Intranet (062);*
- *PWGSC Statement of Values and Ethics for the Public Service*;
- *Records Management and Information Holdings (044);*

- *Reporting of Actual and Suspected Breaches and Violations of Security (053);*
- *Risk Management Guide / Handbook*.

Other Publications:

- *COMSEC Material Control Manual*;
- *CSEC ITSG-06 Clearing and Declassifying Electronic Data Storage Devices*;
- *Directives for the Application of Communications Security in the Government of Canada*;
- *Security Requirements Checklists (SRCL)*.

10. CANCELLATION

This DP supersedes the version dated 2010-07-26.

As this DP has been written within the context of the current ITSB organizational structure, and is based on the Policy on Government Security, it may need to be reviewed if any of these change.

11. ENQUIRIES

Director, Policy, Governance, Knowledge and Information Management
Strategic Planning and Enterprise Architecture, ITSB
Portage III 5C2-105
11 Laurier Street
Gatineau, PQ K1A 0S5

E-mail: TICPolitique.ICTPolicy@tpsgc-pwgsc.gc.ca
Telephone: 819-934-2733
Facsimile: 819-956-3669

Original Signed by
Renée Jolicoeur

François Guimont
Deputy Minister and
Deputy Receiver General for Canada

Annex A - DEFINITIONS

Accreditation *(accréditation)* signifies that management has authorized the system or service to operate and has accepted the residual risk of operating the system or service, based on the certification evidence.

Authentication (*authentification*) is the procedure of identifying or verifying the eligibility of a computer, originator or individual to access specific categories of information; also refers to processes that provide protection against fraudulent transmissions by establishing the validity of a transmission, message, computer or originator.

Availability (*disponibilité*) is the degree to which a system or resource, such as data, is ready when

needed.

Backups (*copies de sauvegarde*) are copies of data and software files which allow for the recovery of information technology (IT) services if the active data or software is lost or corrupted.

Breach (***of security***) (*infraction [à la sécurité]*) occurs when any sensitive information and assets have been compromised. Without restricting its scope, a breach may include compromise in circumstances that make it probable that a breach has occurred.

Certification (*certification*) is the verification that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended.

Client Authority (*représentant de clients*) is a member of a branch who is designated as a single point of contact with whom Information Technology Services Branch interacts with for change requests.

Classified information (*renseignements classifiés*) is 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. Classification categories include Confidential, Secret, or Top Secret (See designated information).

COMSEC, Communications-Electronic Security (*SECOM, sécurité des communications électroniques*) is the part of IT security protection resulting from applying cryptographic, emission, emanation, and transmission security measures to telecommunications, computers, and other related information-handling equipment.

Confidentiality (*confidentialité*) is the sensitivity of information or assets to unauthorized disclosure, recorded as classification or designation, each of which implies a degree of injury should unauthorized disclosure occur.

Configuration chart (*tableau de configuration*) is a chart of the current hardware, software, architecture and network configuration, identifying all hardware units, their software and interconnections.

Contingency plans (*plans de secours*) are comprehensive statements of all the actions to be taken before, during and after a disaster (emergency condition causing an interruption), which, if followed, will ensure the required availability of the computers and data resources to maintain the continuity of operations.

Critical information (*information essentielle*) is information, the compromise of which, regardless of its sensitivity, would cause harm to an individual or to the Department's ability to effectively carry out an operation or activity.

Cryptography (*cryptographie*) is the discipline that treats the principles, means, and methods for safeguarding plain information by making it unintelligible. It also means reconverting the unintelligible information into intelligible form. (see encryption)

Custodians (*responsables*) are the persons responsible for the administration of the system, service or facility's functions, design, operations and data.

Department (*Ministère*) means Public Works and Government Services Canada (PWGSC).

Departmental COMSEC Authority, DCA (*responsable de la SECOM du Ministère*) is responsible for developing, implementing, maintaining, coordinating and monitoring a departmental COMSEC program that is consistent with the *Policy on Government Security* and its operational standards. (The specific responsibilities of the DCA are detailed in the COMSEC Material Control Manual [ITSG-10]).

Designated information (*renseignements désignés*) is information related to other than the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or *Privacy Act*. Categories include: 'Protected A' for sensitive, 'Protected B' for particularly sensitive, or 'Protected C' for extremely sensitive. (See classified information)

Electronic authorization and authentication (*autorisation et authentification électroniques*) is an electronic means of identifying and verifying the rights or authorities of a legitimate user of an IT system or service (authorization), and of identifying and verifying legitimate system/service users and devices (authentication).

Encryption (*cryptage*) is the transformation of readable data into an unreadable stream of characters using a reversible coding process. (see cryptography)

Information holdings (*renseignements détenus*) means all information under the control of a department, regardless of physical mode or medium in which the information is stored. Materials held by federal libraries that were not prepared or produced by or for the government are excluded.

Information Technology, IT (*technologies de l'information, TI*) means the scientific, technological and engineering disciplines and the management practices used in electronic information handling, communication and processing; the fields of electronic data processing, telecommunications, electronic networks, and their convergence in systems; their applications and associated software and equipment together with their interaction with humans and machines.

IT facilities (*installations associées à la TI*) are physical settings used to contain IT equipment and services. The facility could be part of a building or a whole building such as: a data centre, a LAN (local area network) server room, a communications centre, a communication wiring closet, a workspace, etc.

Information Technology Security, ITS (*sécurité des technologies de l'information, STI*) means the protection resulting from an integrated set of safeguards designed to ensure the confidentiality of IT assets and information electronically stored, processed or transmitted; the integrity of the information and related processes and the availability of systems and services.

IT Security incident (*incident de sécurité relié aux TI*) includes breaches and violations of IT security. Breaches occur when sensitive electronic information has been compromised, or when the availability or integrity of information or IT services has been negatively impacted. Violations are acts or omissions that contravene any provision of departmental security policies and standards.

IT Security Program *(programme de sécurité des TI)* is a program established, implemented and maintained to assure that adequate IT security is provided for all organizational information collected, processed, transmitted, stored or disseminated in its IT systems.

IT services *(services de TI)* is the access to data networks and telecommunications services and software used on IT equipment. Examples include: PWGSC electronic networks and related services, such as access to peripheral devices (e.g. printers, facsimile machines, scanners, etc.), purchased or PWGSC developed / customized software programs running on PWGSC networks or computers; electronic information management and messaging services (e.g. e-mail and voice mail systems), the Internet; the government intranet, and any other electronic service provided to PWGSC users through the PWGSC networks or via PWGSC computers or wireless devices.

Integrity (*intégrité*) is the accuracy and completeness of information and assets and the authenticity of transactions.

Interoperability (*interopérabilité*) is the ability of federal government departments to operate synergistically through consistent security and identity management practices.

Local Registration Authorities, LRA (*autorité locale d'enregistrement, ALE*) mean cleared and trusted individuals who register persons using the Public Key Infrastructure.

Malicious code (*code malveillant*) is a program created for mischievous or malicious purposes; it may cause changes to information, or software, or overload networks, or destroy information, or breach the security of systems; includes viruses, worms, Trojan horses, logic bombs, time bombs, and are usually triggered by a predetermined event or date. Some may spread copies of themselves through networks, diskettes or hardware.

Mode of operation (*mode de fonctionnement*) is a way of categorizing IT systems with respect to the controls that are needed to enforce the security policy requirements for appropriate security clearance / screening and need-to-know. The user profile, system characteristics and confidentiality considerations determine the most suitable mode of operation. There are three modes of operation:

1. Dedicated: All users have appropriate security clearance to access all information on the system, and need to know all information on the system;
2. System high: All users have appropriate security clearance to access all information on the system, but some users do not need to know all information on the system;
3. Multi-level: Some users do not have appropriate security clearance to access all information on the system, and some users do not need to know all information on the system.

Modems (*modems*) are functional units that modulate and demodulate signals in order to enable digital data to be transmitted over analog transmission facilities.

Owners (*propriétaires*) are persons responsible for the decisions concerning the system or service's functions and for the decisions concerning what information is collected and for what purpose; usually the senior manager responsible for the business function that the system or service is serving.

Private communication (*communication privée*) means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it; includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

Public Key Infrastructure, PKI (*infrastructure des clés publiques, ICP*) means a cryptographic key and certificate delivery system which makes possible secure electronic transactions and exchanges of sensitive information using a system of trusted third parties called 'certificate authority'. A PKI provides privacy, access control, integrity, authentication and non-repudiation support to IT applications and electronic commerce transactions.

PWGSC principal network (*réseau principal de TPSGC*) is the standard environment for routine PWGSC operations. It is the primary environment in which end-user systems and workgroup servers are installed. This environment can be used to process, store and transmit information up to and including 'Protected A'. 'Protected B' information can only be processed, stored and transmitted on PWGSG's principal network, if it is encrypted in accordance with an approved encryption standard (PKI/MYKEY). 'Protected C' and 'Classified' information cannot be processed, stored or transmitted on the PWGSC principal network.

Regional Security Office (*bureau régional de sécurité*) is the office responsible for co-ordination of all physical security aspects, security investigations, user screening, issuing of user ID cards, completion of threat and risk assessments, and provision of advice on security measures.

Remote access (*accès à distance*) means any required connection to departmental IT systems from outside the existing PWGSC infrastructure. This would cover the ISDN (Integrated Services Digital Network) as well as dial-up connections.

Removable media (*support d'information amovible*) includes memory cards, DVDs, CD ROMs, diskettes, magnetic tapes, hard drives, memory sticks.

Security standard (*norme de sécurité*) means the level of attainment regarded as a measure of adequacy; security requirements and guidelines approved for government-wide use. (Operational standards are contained in the Treasury Board Manual; technical standards are produced by the lead security agencies.)

Sensitive information (*renseignements de nature délicate*) means classified or designated information.

Stand-alone computers (*ordinateurs autonomes*) are computers that are not connected to any other computers or networks.

Statement of sensitivity (*énoncé de la nature délicate*) is a description of the confidentiality, integrity or availability requirements associated with the information or assets stored or processed in or transmitted by an IT system.

System Development Life Cycle (*cycle de vie du développement de système*) refers to procedures documented and implemented to guide and control the design, development, approval, test, documentation, implementation, maintenance and protection of production software and data items.

Threat and Risk Assessment (*évaluation de la menace et des risques*) means the evaluation of the nature, likelihood and consequence of acts or events that could place sensitive information and assets at risk.

Unit Security Officer, USO (*agent de sécurité de l'unité, ASU*) is a person responsible for the co-ordination of all physical security aspects, security investigations, user screening, issuing of user ID cards, completion of threat and risk assessments, and provision of advice on security measures.

Users (*utilisateurs*) include employees, volunteers, temporary help agency staff, students, contractors, consultants, and business partners who have authorized use of the departmental corporate network, telecommunications systems, computer applications, or those who use PWGSC-owned IT equipment and services in federal government facilities, and off-site (e.g. at home, on the road, etc.) for the processing, storage or transmission of information.

Violation (of security) *(manquement [à la sécurité]*) means any act or omission that contravenes any provision of the Policy on Government Security. Such acts may include failure to classify or designate information in accordance with this DP; classification or designation, or continuation of same, in violation of this DP; unauthorized modification, retention, destruction or removal of sensitive information; and unauthorized interruption of the flow of sensitive information.

Annex B - PWGSC INFORMATION TECHNOLOGY SECURITY PRINCIPLES

1. Principles

The selection and application of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of PWGSC. Security controls are the management, operational and technical safeguards or countermeasures required to protect the confidentiality, integrity, and availability of a system and its information. The following principles must guide all departmental practices in the absence of any specific departmental policies, directives or standards:

1. Individual accountability
   All users, regardless of their role, are fully accountable for their actions or inactions with respect to information technology (IT) security.

2. Awareness
   Users must be provided with appropriate knowledge of, and be informed about, the existence and general extent of measures, practices and procedures for the security of information.

3. Information classification / designation
   Information must be classified or designated according to the Departmental Consolidated Information and Assets Classification and Designation Guide.

4. System Life Cycle
   IT security must be an integral part of all systems application life cycle.

5. Proportionality
   Security measures, costs, practices and procedures must be appropriate and proportionate to the confidentiality, integrity and availability requirements of the assets.

6. Multi-disciplinary
   Measures, practices and procedures for the security of information systems should address all aspects of IT security including organizational, administrative, physical, environmental, personnel, hardware, software, communications and operational elements.

7. Proven environment
   The assumption that an environment is secure can pose a greater risk than the absence of security. Until certified by an IT security authority, no environment should be considered secure.

8. Interoperability and information exchange
   Interoperability and information exchange are enabled through effective and consistent security and identity management practices.

9. Assurance of protection
   All security measures, practices and procedures whether automated or manual must be tested and used regularly to ensure proper operation.

10. Access
    Information and other assets shall be accessed only by users having a need-to-know, the proper personnel security clearance or reliability status, and the proper authorization.

11. Segregation of responsibilities
    Responsibilities must be segregated when possible so that no one person has complete control over a particular resource or process. In some cases dual responsibility must be implemented so manipulation of a resource cannot be accomplished without the knowledge of another person.

12. Least privilege

IT system users must be provided with the least amount and types of system privileges that still provides them with an unimpeded ability to perform their jobs.

13. Ethics
    IT systems security must be applied in such a manner that the rights and legitimate interests of others are respected.

14. Integration
    To create a coherent and comprehensive system of security, measures, practices and procedures for the security of individual IT systems must be coordinated and integrated with each other and with other measures, practices and procedures of the organization.

15. Violations and breaches
    All users must act in a timely and coordinated manner to prevent, report and respond to suspected violations and breaches of IT security.

16. Reassessment
    Because security requirements may change over time, the security of IT systems must be reassessed periodically.

17. Monitoring
    Monitoring practices and procedures must be coordinated to ensure a coherent and comprehensive verification system.

18. Risk management
    This is the process by which managers inform themselves about security vulnerabilities, certify safeguards and assume residual risk. Risk management must begin with an evaluation of the sensitivity of the information followed by an assessment of threats and risks performed in an iterative process that involves steps to select, implement, certify, accredit, maintain, monitor and adjust safeguards. Risks must be managed by identifying, analyzing and assessing them, selecting risk-avoidance options, and designing and implementing cost-effective prevention and control measures.

19. Electronic privacy
    The level of individual privacy is limited by the right of the Department to monitor electronic assets for effective and efficient operations including proper usage by users. The Department must strive to ensure privacy between employees, and between employees and other entities.

20. Governance
    IT security measures and safeguards are subject to the IM/IT governance process.

21. Mode of operation
    The mode of operation of PWGSC's networks is system high, 'Protected A' mode. This means that all personnel with access to the networks must have at least a reliability status screening. Information more sensitive than 'Protected A' may not be stored or transmitted over PWGSC networks without additional safeguards.

Annex C - INFORMATION TECHNOLOGY SECURITY MANAGEMENT

1. Delegation of Authority
   The Information Technology (IT) Security Coordinator must have a formal relationship with other departmental security groups. The IT Security Coordinator may delegate to employees and contractors

certain security responsibilities. Delegated responsibilities must be officially documented.

2. Planning
   Plans for the development of systems, services and facilities in PWGSC must contain activities for the implementation of required IT security measures.

3. Risk Management
   The application of a risk management process is a key element in the Treasury Board Secretariat (TBS) *Policy on Government Security*.

   Unless specifically exempted by the IM/IT governance process, all departmental systems, applications, servers, Web sites, and IT facilities must be accredited before going into production.

   Owners and custodians must complete all of the following steps in order to acquire and maintain accreditation:

   1. Statement of sensitivity
      Owners and custodians must prepare and periodically update statements of sensitivity documenting the confidentiality, integrity and availability requirements for IT systems, applications, services and facilities that process, store or transmit sensitive or critical information.

   2. Threat and risk assessments
      Owners and custodians must prepare and periodically update threat and risk assessments, analyzing the security vulnerabilities and recommending counter measures where required for IT systems, applications, services and facilities that process, store or transmit sensitive or critical information.

   3. Certification
      Owners and custodians must ensure that the appropriate certifying authority certifies the security aspects for all IT systems, applications, services and facilities that process, store or transmit sensitive or critical information to verify that IT security safeguards are present and operate as intended and that functional security requirements are met.

4. IT Security Reviews
   Owners and custodians must review their statements of sensitivity and threat and risk assessments periodically or whenever the security environment changes in a manner which significantly alters the security requirements. The results of these reviews are to be transmitted to the appropriate certifying authority for review for compliance with policy and standards and for further action as deemed necessary through the IM/IT governance process. Should this process result in significant changes in configuration, the statement of sensitivity, the threat and risk assessment, or the certification testing (which may require changes to the security safeguards), owners and custodians must renew their accreditation.

5. Awareness and Training

   All managers will ensure that users under their purview are informed of all applicable IT security policies, standards and procedures in accordance with their role and responsibilities.

   The IT Security Coordinator is responsible for developing a departmental IT Security Awareness Program.

6. Royal Canadian Mounted Police (RCMP) and Communications Security Establishment Canada (CSEC) Advice and Training

   The IT Security Coordinator is responsible for coordinating all IT security-related consultations and training from the RCMP and CSEC.

7. Contracting for IT Services or Products
   Managers must ensure that appropriate IT security clauses are included in contracts and Memoranda of Understanding.

   Managers must ensure that their suppliers meet contractual IT security requirements.

   As the contracting authority, PWGSC must ensure that appropriate IT security clauses are included in industrial contracts awarded through PWGSC.

8. IT Security Audits
   Internal auditors conduct periodic audits of PWGSC IT that may result in recommendations to improve IT security measures.

   The IT Security Coordinator must receive copies of all IT security audits. All plans to mitigate vulnerabilities are subject to the IM/IT governance process.

9. IT Security Report to Senior Management
   The IT Security Coordinator is responsible for reporting on the status of IT security within PWGSC to the Departmental Security Officer (DSO).

10. Safeguarding of Information
    Computer media and IT systems, applications, services or facilities must be safeguarded to protect information from unauthorized access.

11. Security Labelling of Information
    Sensitive information stored or using IT resources must be labeled with the proper classification or designation level.

12. Disposal of Classified and Designated Information
    Owners and custodians are responsible for ensuring that classified and designated electronic information and IT assets (including waste) are disposed of according to standards found in the CSEC ITSG-06 Clearing and Declassifying Electronic Data Storage Devices. This includes printouts and information held on hard disks, removable media (e.g. USB sticks, removable hard drives, diskettes, cassettes, CD-ROMs, tapes) and other information technology media.

13. Controlling Logical Access to Systems, Services and Information
    Access to sensitive information must be strictly limited by physical, procedural and computer logical access controls and must be limited to users who have an operational requirement, have the proper security screening, and have the necessary authorization.

    1. Access privileges
       Owners and custodians will authorize and pre-establish access privileges prior to use of stand-alone computers, multi-user computers and networks.

    2. User identifiers
       Owners and custodians will assign a unique user identifier to each user before access to IT

systems and information is granted. User identifiers shall only be active for the duration of the employment or specific task.

3. Passwords
   Users must keep their passwords and pass codes private. Passwords shall be constructed and changed according to the IT security standards.

4. Access management
   Owners and custodians shall ensure that users' privileges do not exceed their needs and authorization.

14. Banner
    Owners and custodians must ensure that the approved IT security banner is displayed to inform the user of the rules and regulations related to its use. The banner shall be presented to users, on a monthly basis, at the sign-on process before an IT connection is granted.

Annex D - APPLICATION SECURITY

1. Development of Information Technology (IT) Systems and Services

   Project managers shall ensure that an approved PWGSC system development life cycle and accompanying IT security processes are used to develop, maintain and dispose of departmental IT systems and services.

2. Installation of Software and Applications

   Users must obtain written authorization before any software and/or applications are installed onto IT equipment owned by PWGSC. Contact IT Service Desk: 1-866-995-6030.

3. Maintenance

   Owners and custodians must authorize all maintenance of IT software.

   Maintenance staff members must be security screened as required by the level of the information to which they may have access.

   During maintenance, sensitive information must be protected to prevent copying or misuse of the data.

4. Viruses and Other Malicious Codes

   PWGSC shall provide anti-virus software to protect departmental computers.

   Users must follow anti-virus software procedures for the detection of malicious codes. Users must immediately contact the IT Service Desk at 1-866-995-6030 if they suspect their IT equipment has become infected with a virus and/or malicious code.

Annex E - INFORMATION TECHNOLOGY OPERATIONS SECURITY

1. Operational Monitoring

   Owners and custodians must monitor information technology (IT) resources for operational efficiency.

2. Threats and Vulnerabilities Monitoring

   Owners and custodians must monitor IT resources to identify vulnerabilities and detect cyber threats, and must ensure that appropriate mitigation measures are taken.

3. Backups

   Owners and custodians will ensure that regular backups are made and tested for electronic information and software under their control. Backups must be stored in a secure place away from active files. Backups of electronic information or software, critical to operations or difficult to replace, must be stored off-site and in accordance with its level of sensitivity.

4. Physical and Environmental Security

   Physical access to IT media, computers, LAN (local area networks) and telecommunications must be restricted to those with a 'need to know', a security screening and the required authorization.

   Computer, LAN and telecommunications rooms must be protected by environmental safeguards, in accordance with the Government of Canada standards.

   1. Construction of IT facilities

      Project managers have the responsibilities of custodians during all phases of the construction of an IT facility and they must ensure that IT security is addressed.

   2. Restricted zones

      Security zones must be established as per standards for areas processing and storing sensitive information including areas such as: main-frames, mini-computers, LAN servers, communications equipment, IT media storage, telecommunications rooms, or when required by threat and risk assessments.

   3. Protection of IT assets

      Users must safeguard government assets (including information) in their custody either at the departmental workplace, at home or when travelling.

   4. Positioning of equipment

      Users must position workstation monitors, printers and facsimiles equipment in such a way that unauthorized persons cannot have access to, or view, the information.

5. Configuration Chart

   Owners and custodians will maintain configuration charts for main-frame computers, mid-range computers and departmental IT networks installations. The charts must be labelled according to their sensitivity.

6. Maintenance

   Information Technology Services Branch (ITSB) will authorize all maintenance of IT equipment and provide adequate activity supervision.

   Maintenance staff members must be security cleared to the level of the information to which they may have access.

7. Telecommunication connectivity shall be formally approved, controlled and monitored by the Information Technology Services Branch in accordance with the departmental IT security policies and standards.

   Unauthorized installation, disablement and unapproved removal of telecommunication equipment shall be reported to the manager and to the IT Security Coordinator.

8. Use of Modems

   Modems shall not be connected to networked workstations.

   The approval for the installation or use of modems on PWGSC owned stand-alone computers, laptops and communication servers is subject to the IM/IT governance process. 'Classified' systems must use the Communication-Electronics Security (COMSEC) approved modem connections.

9. Remote access to Departmental Networks

   A PWGSC-approved remote access solution shall be required for all remote access to PWGSC networks.

10. Transmission of Information

    Users must use encryption products and procedures that have been approved by the IT Security Coordinator. All 'Protected B', 'Protected C' and 'Classified' information must be encrypted for transmission, regardless of the medium by which the information is being communicated, including the following:

    1. Electronic information - PWGSC's principal network

       PWGSC's principal network can be used to transmit information up to and including the security level of Protected A. Protected B information can only be transmitted on PWGSC's principal network, if it is encrypted in accordance with a PWGSC approved encryption standard. Protected C and Classified information cannot be transmitted on PWGSC's principal network.

2. Telephone
   In PWGSC, Secure Communication Interoperability Protocol (SCIP) is the authorized means by which voice communications are secured.

   Users must abide by the Communications Security Establishment Canada (CSEC) Directives for the Application of Communications Security in the Government of Canada (ITSD-01) and the guidance from the COMSEC Material Control Manual for the custody and use of SCIP.

3. Fax
   In PWGSC, secure fax transmission requires the use of SCIP.
   Users must not program facsimile machines with non-governmental speed dial numbers, regardless of the level of sensitivity of the information being transmitted.

11. Interconnection of Computer Systems
    Owners and custodians shall perform a threat and risk assessment to determine the impact of interconnection of systems.

12. Internet / Intranet
    Owners and custodians must protect Internet and intranet access with a strong access device such as an approved firewall.

13. Electronic Authorization and Authentication
    All equipment and processes for electronic authorization, authentication and digital signatures are subject to approval through the appropriate IM/IT governance process.

14. Voice Messaging Systems
    Users shall not leave voice messages that contain sensitive information.

    Owners and custodians must ensure that logical access controls are included into such system to prevent unauthorized access.

    Owners and custodians must regularly monitor the voice messaging systems for irregularities and to detect inactive accounts.

    Users must use a password to protect their mailbox.

15. Operation Procedures
    Owners and custodians shall ensure that IT security procedures for computer operations are developed, documented and made available to users.

16. Processing of Information
    PWGSC's principal network can be used to process, store and transmit information up to and including the security level of Protected A. Protected B information can only be processed, stored and transmitted on PWGSC's principal network, if it is encrypted in accordance with a PWGSC approved encryption standard. Protected C and Classified information cannot be processed, stored or transmitted on PWGSC's principal network.

17. Use of 'Privileged and Powerful Software'

    1. Definition
       The term 'privileged and powerful software' includes the following:

1. all software intended to intercept, scan, quarantine, inspect, or otherwise handle third party data for purposes other than that intended by the original parties; or

2. software designed to by-pass security measures deployed on the PWGSC infrastructure.

Examples of such software include: intrusion detection scanners, port scanners, anti-virus scanners, network 'sniffers', and protocol analyzers. This is not an exhaustive list; in case of doubt, the potential user should clarify the nature of the tool with the IT Security Coordinator.

2. Personal Liability
The use of 'privileged and powerful software' may place the user in possible violation of a number of Canadian acts and statutes, namely: the *Criminal Code*, the *Privacy Act*, the *Competition Act* and the *Canadian Charter of Rights and Freedoms*. This policy statement addresses actions that may trigger the application of some or all of this legislation. All users having access to 'powerful and privileged software' in the care and control of PWGSC should note that PWGSC can only authorize activities that are not in contravention of the law. Users who take it upon themselves to act in a manner contrary to the *Criminal Code* or other acts and statutes can be held personally responsible for these actions in a court of law.

3. Unauthorized Uses
For example, the types of actions that may trigger legal action under the *Criminal Code* include the:

1. unauthorized use of port scanning software against PWGSC or outside targets;

2. unauthorized use of intrusion detection software;

3. unauthorized alteration or destruction of data (e.g. 'hacking');

4. unauthorized use of specialized IT and telecommunications equipment designed to access private communications;

5. tampering of data that is considered 'evidence' in a potential criminal case; this would apply to modification of data dealing with a hacking incident;

6. intentional and unauthorized viewing of third party information stored on electronic media.

4. Authority to Use

1. Prior to any use, written approval from the IT Security Coordinator must be obtained by a user of 'privileged and powerful software'. The granting of any approval will take into account operational requirements and the availability of clear and effective control procedures that will ensure that legal and policy requirements are adhered to. Authorization will be granted for a specific event or period, and will only be granted to the individual(s) named in the authorization.

2. For example, without approval as specified in 4(1), users are not authorized to:

- use any software or IT systems which are designed to by-pass security measures, or to interfere with the corporate IT infrastructure or data in any manner; or

- use any software or hardware whose purpose is to intercept, scan, inspect, quarantine, store, or modify third party data that is a 'private communication'.

Annex F - INFORMATION TECHNOLOGY SECURITY INCIDENT MANAGEMENT

1. IT Security Incidents, Breaches and Violations
   All actual or suspected IT security anomalies and violations must be reported by the user to his/her manager and the Information System Security Officer (ISSO) or the Regional Security Office. The ISSO or the user must also contact the IT Service Desk at 1-866-995-6030, as soon as possible.

2. IT Security Investigations
   The IT Security Coordinator shall provide IT technical assistance to investigative units.