PROTECTED
DRAFT

SECURITY POLICY OF

THE GOVERNMENT OF CANADA

Table of Contents

POLICY OBJECTIVE .....

POLICY STATEMENT .....

APPLICATION .....

POLICY REQUIREMENTS .....

MONITORING .....

REFERENCES .....

ENQUIRIES .....

APPENDIX A - AGENCIES AND CROWN CORPORATIONS SUBJECT TO THE POLICY .....

APPENDIX B - ROLES AND RESPONSIBILITIES .....

APPENDIX C - DEFINITIONS .....

APPENDIX D - CLASSIFYING AND DESIGNATING INFORMATION .....

POLICY OBJECTIVE

To ensure that all sensitive information and sensitive and valuable assets of the federal government are safeguarded in an appropriate manner.

POLICY STATEMENT

It is the policy of the government to:

- assign accountability to deputy heads for the safeguarding of information and other assets under their control;

- classify information when its unauthorized disclosure or other compromise could reasonably be expected to cause injury to the national interest, with reference to specified provisions of the Access to Information Act or the Privacy Act;

- limit access to Classified information to those whose duties require it, whether by appointment, assignment or contract, and who have a valid security clearance at the appropriate level;

- designate sensitive information lying outside the national interest if that information is reasonably likely to be exempt or is excluded from access under specified provisions of the Access to Information Act or the Privacy Act;

- limit access to Designated information and other sensitive or valuable assets to those whose duties require it whether by appointment, assignment or contract, and who have a valid reliability status;

- ensure that all persons subject to personnel screening are treated in a fair and unbiased manner; and

- safeguard Classified and Designated information and assets in accordance with government-wide standards and threat and risk assessments.

The legal basis for the requirement to determine whether information may be classified or designated is set forth by provisions of the Access to Information Act and the Privacy Act as specified in sections 1.2 and 1.3 of Guidelines. In no case may information be classified in the national interest or designated in order to conceal violations of law, inefficiency or administrative error, to avoid embarrassment, or to restrain competition.

APPLICATION

This policy applies to all government institutions and portions of the Public Service of Canada listed in Schedule I, Parts I and II of the Public Service Staff Relations Act, and to the Canadian Armed Forces, the Royal Canadian Mounted Police and the Canadian Security Intelligence Service.

The national interest requirements of this policy apply to certain other institutions that are party to agreements between the President of the Treasury Board and the Ministers responsible for those institutions. See Appendix A.

POLICY REQUIREMENTS

1. Corporate management

Government institutions are required to:

- name a senior official to coordinate and direct the on-going implementation of this policy;
- conduct threat and risk assessments in relation to Classified and Designated information and assets; and
- develop, maintain and apply written policies and procedures pursuant to the Security Policy and Operational Security Standards.

2. Classification and designation of information

Within the framework of the Security Policy, institutions are required to maintain and apply written guidelines that provide for:

- the identification, classification or designation, and marking of information under their control;
- the declassification of information when it no longer needs safeguarding in the national interest; and
- the downgrading of the classification/designation of information.

Institutions must also name in writing officials to classify or designate information not covered by the departmental guide.

No authority is needed to classify or designate information derived from other information already classified or designated in accordance with this policy. This also applies to contractors, who may mark information derived from Classified or Designated information provided by a government institution.

3. Personnel screening

Government institutions are required to:

- inform all individuals who will be subject to screening of the nature of the verifications;

- conduct an enhanced reliability check for all individuals whose duties or tasks involve, TO A SIGNIFICANT DEGREE, the care and custody of, or access to, Designated information or assets;

- grant or deny reliability status;

- arrange for security clearance at the appropriate level of all individuals whose duties or tasks REQUIRE access to Classified information or assets OR of those who have access to essential persons or installations critical to the national interest that, in the opinion of the deputy head, affords regular and consistent access to such information or assets;

- grant or deny security clearances with the advice of the related investigative body;

- grant the required reliability status or clearance before individuals start performing their duties or tasks or, in case of appointments from competition, before a person's name is placed on an eligibility list;

- ensure that only the deputy head denies, revokes or suspends a security clearance and that this authority is not delegated; and

- advise individuals who have been denied a reliability status or a security clearance of their rights of review and redress.

4. Safeguards

Government institutions must:

- apply administrative, physical, and information technology security measures on the basis of threat and risk assessments and Operational and Technical Security Standards;

- treat sensitive information received from provincial, municipal or regional governments, from governments of other nations, or from international organizations of nations or their institutions, in accordance with agreements or understandings between the parties concerned; and

- establish written agreements for the protection of Classified and Designated information provided to other governments or organizations.

5. Security breaches and violations

Government institutions must:

- report possible breaches of security immediately to the deputy head;
- report to the appropriate law enforcement authority suspected breaches constituting criminal offences;
- report immediately to the Canadian Security Intelligence Service probable unauthorized disclosure of, or unauthorized access to Classified information;
- inform the institution that originated the information or other assets involved that a breach of security has occurred, if this applies;
- conduct an injury assessment within 10 working days whenever it is probable that a breach of security has occurred and report on this to the deputy head;
- inform other institutions that have information or other assets involved in a breach of security of the circumstances and findings that affect them;
- determine whether or not a breach of security should be formally investigated; and
- ensure that violations of security are reported to the senior official responsible for the operational area concerned.

6. Sanctions

Government institutions are required to apply sanctions in response to breaches and violations of security when, in the opinion of the deputy head, there has been misconduct or negligence. Redress for disciplinary sanctions, except the removal of security clearances, is available through the relevant provisions of Sections 90 and 91 of the Public Service Staff Relations Act or equivalent procedures for employees not subject to that Act. A person whose security clearance has been removed may have recourse to the formal review process of the Security Intelligence Review Committee, as specified in the Canadian Security Intelligence Service Act.

7. Audit and Review

Government institutions must:

- conduct an internal audit of their compliance with the policy and the efficiency with which they are implementing it at least once every five years, the first to be completed by 1993; and

- arrange through the Security Branch of the Department of Supply and Services the inspection of private sector EDP facilities that require, through contract, access to Classified or Designated information.

Government institutions, other than DND, must:

- request an inspection of their EDP systems by the Security Evaluation and Inspection Team (SEIT) of the RCMP, according to the Operational Security Standards. They must also consult SEIT when major changes are planned in their information processing systems; and

- advise the SEIT within six months of receipt of the SEIT report of their plan to deal with identified problems and thereafter provide annual progress reports.

RESPONSIBILITIES

The roles of central agencies, lead agencies and common service organizations with responsibilities for implementation of the Security Policy government-wide are described in Appendix B.

MONITORING

The Treasury Board Secretariat will monitor compliance with all aspects of this policy through internal audit reports as well as through the annual report by the National Archives to the Secretary of the Treasury Board on the state of the management of information holdings relevant to their classification, designation, and safeguarding throughout their life cycle; an annual report by the RCMP on EDP security; and periodic reports by the RCMP on the state of physical security and by the Communications Security Establishment on the state of communications - electronic security.

REFERENCES

This policy is issued under the authority of Section 5 of the Financial Administration Act and of a decision of Cabinet in January, 1986.

The policy replaces the 1956 Privy Council Office document entitled, "Security of Information in the Public Service of Canada"; Cabinet Directive 35 of 1963, relating to security screening; Chapter 440.8, EDP: Security; and section .6 of Chapter 435, Telecommunications Administration, of the Treasury Board Administrative Policy Manual. It also replaces the policies published in Treasury Board Circulars 1986-26, 1987-10, 1987-31 and 1987-40.

This policy should be read in conjunction with relevant legislation and other administrative and personnel policies issued by the Treasury Board including:

. Access to Information Act

- Canadian Security Intelligence Service Act
- Financial Administration Act
- Operational Security Standards
- Interim Policy Guide: Access To Information Act and the Privacy Act, Parts II and III
- Official Secrets Act
- Privacy Act
- Public Service Employment Act
- Public Service Staff Relations Act

DEFINITIONS

See Appendix C for a list of definitions of selected security terms.

ENQUIRIES

For interpretation of aspects of the policy concerning administration, contact the Information Management Division, Administrative Policy Branch, Treasury Board Secretariat.

Interpretation of personnel screening aspects of the policy is available from the Policies and Procedures Group, Personnel Policy Branch, Treasury Board Secretariat.

PROTECTED
DRAFT

APPENDIX A

Agencies and Crown Corporations Subject to the Policy

Air Canada
Atlantic Pilotage Authority
Atomic Energy of Canada Limited
Bank of Canada
Canada Deposit Insurance Corporation
Canada Development and Investment Corp.
Canada Harbour Place Corporation (EXPO 86)
Canada Mortgage and Housing Corporation
Canada Ports Corporation
Canada Post Corporation
Canadian Broadcasting Corporation
Canadian Centre for Occupational Health and Safety
Canadian Commercial Corporation
Canadian Film Development Corporation (Telefilm Canada)
Canadian National Railway Company
Canadian Patents and Development Ltd.
Canadian Saltfish Corporation
Canadian Wheat Board
Defence Construction (1951) Limited
Export Development Corporation
Farm Credit Corporation
Farm Debt Review Board
Federal Business Development Bank
Fraser River Harbour Commission
Freshwater Fish Marketing Corporation
Great Lakes Pilotage Authority
Halifax Port Corporation
Hamilton Harbour Commissioners
International Development Research Centre
Laurentian Pilotage Authority
Marine Atlantic Inc. (formerly CN Marine Inc.)
Montreal Port Corporation
Nanaimo Harbour Commission
National Arts Centre
North Fraser Harbour Commission
Oshawa Harbour Commission
Pacific Pilotage Authority
Port Alberni Harbour Commission
Port of Belledune
Port of Chicoutimi
Port of Churchill
Port of Quebec Corporation
Port of Prince Rupert Corporation
Port of Sept-Iles
Port of Trois-Rivières

Royal Canadian Mint
Saint John Port Corporation
St. John's Port Corporation
St. Lawrence Seaway Authority
Standards Council of Canada
Teleglobe Canada
Thunder Bay Harbour Commission
Toronto Harbour Commissioners
Vancouver Port Corporation
Via Rail Canada Inc.
Western Grain Transportation Agency
Windsor Harbour Commission

PROTECTED
DRAFT

APPENDIX B

Roles in implementing the security policy government wide

Committees

The Cabinet Committee on Security and Intelligence (CCSI), chaired by the Prime Minister, provides general policy direction on security matters. It receives advice from the Interdepartmental Committee on Security and Intelligence (ICSI), chaired by the Clerk of the Privy Council. The Treasury Board approves administrative and personnel security policies and operational security standards.

Institutions

The Canadian Security Intelligence Service is responsible for:

(a) investigating individuals, when requested, for the purpose of security clearances;

(b) conducting subject interviews as part of the security clearance process, other than for DND and the RCMP;

(c) providing security assessments, as requested by deputy heads;

(d) maintaining a central index of security clearances;

(e) establishing guidelines for the declassification or downgrading of classified information pertaining to intelligence activities, as defined in sections 12 to 16 and subsection 19(a) of the Canadian Security Intelligence Service Act, as well as that relating to intelligence sources or methods; and

(f) providing, when requested, advice to institutions on threat and risk assessments.

The Communications Security Establishment is responsible for:

(a) formulating operational directives and guidelines on communications-electronic security (COMSEC) for the approval of Treasury Board and advising on their application;

(b) issuing technical directives and guidelines on COMSEC and for the protection of signals intelligence and cryptographic information and material, and advising on their application;

(c) providing cryptographic material and documentation to appropriate government institutions;

(d) approving release of classified/controlled COMSEC information and assets to government and non-government entities;

(e) providing advice and guidance on the planning, acquisition, installation and procedures for using COMSEC systems;

(f) reporting to Treasury Board, when requested, on the state of COMSEC across the government;

(g) inspecting, testing and evaluating COMSEC systems and procedures, other than for DND, and, on request, reviewing government telecommunications to assess adherence to prescribed COMSEC practices;

(h) classifying signals intelligence and cryptographic information and material, and establishing procedures for the systematic review of such Classified information and material for declassification or downgrading;

(i) approving the allocation of positions requiring special access (SA) to signals intelligence information and material, and maintaining the inventory of personnel cleared for access to such information and material; and

(j) providing a research and development and evaluation capability on security aspects of computer hardware, software and communications systems to ensure that information is available to the government on the security of computer systems and their use in government.

External Affairs Canada is responsible for:

(a) performing or arranging the inspection of measures used by other government institutions to protect classified information and other assets handled by its Canadian Diplomatic Communications Service (which includes diplomatic couriers) to ensure continuity and uniformity of protection; and

(b) ensuring that adequate safeguards are accorded by all government institutions to North Atlantic Treaty Organization (NATO) documents under their control, and inspecting the custodial arrangements for such documents. The Department of National Defence, however, does its own inspections.

The National Archives of Canada is responsible for:

(a) safeguarding at the applicable level Classified or Designated information transferred to Archives;

(b) declassification and downgrading of information transferred to their control for historical or archival purposes, according to agreements; and

(c) auditing of the security classifications/designation of records.

National Defence. The Deputy Minister and the Chief of the Defence Staff are jointly or separately responsible, as appropriate, for:

(a) verifying that government institutions holding documents containing atomic information exchanged in accordance with bilateral and multilateral agreements are safeguarding those documents as required by the agreements;

(b) developing security measures that meet the intent of the government-wide standards for military and related field operations or national emergencies; and

(c) conducting the security clearance of members and prospective members of the Canadian Forces and other individuals employed or about to be employed by, in or on behalf of DND, excluding the Communications Security Establishment and Defence Construction (1951) Limited. Where a search of security intelligence records is required, CSIS shall carry out this activity.

The Public Service Commission is responsible for:

(a) establishing the staffing policies and procedures necessary to fulfill the requirements of this policy and to expedite appointments to Public Service positions, consistent with the statutory obligations and limitations of the Public Service Commission;

(b) establishing and maintaining a Central Index of employees released, rejected, dismissed or discharged for cause from the Public Service; and

(c) establishing security training programs, as required.

The Privy Council Office is responsible for:

(a) advising deputy heads on decisions to order a formal investigation of suspected breaches of security;

(b) advising deputy heads on decisions to deny security clearances; and

(c) establishing procedures for declassifying confidences of the Queen's Privy Council for Canada and records administered under the Cabinet Paper System.

Public Works Canada is responsible for the following aspects of physical security at the facilities in its custody:

(a) providing a basic level of physical security with regard to buildings, their sites and the spaces within them;

(b) providing an enhanced level of physical security with regard to buildings, their sites and the spaces within them, when justified by a tenant-prepared Security Site Brief or Security Design Brief, as appropriate.

(c) requesting the advice of the RCMP in case of unresolved disputes between a tenant department and PWC concerning requirements for or the provision of physical security;

(d) resolving disputes between a tenant department and PWC concerning requirements for or provision of physical security;

(e) providing, where required, security guard services for the general security of the building perimeter and common areas; and

(f) providing, on a cost recoverable basis, additional security guard services within the tenant premises, where requested.

The Royal Canadian Mounted Police is responsible for:

(a) developing government-wide physical, and EDP security standards;

(b) inspecting, testing, evaluating and, where required, designing physical security equipment, and developing related specifications;

(c) maintaining, where required, physical security equipment uniquely designed or modified for the protection of Classified information;

(d) providing on request, advice on threat and risk assessments;

(e) when requested, reviewing and advising on physical security and counter-technical intrusion measures in government institutions;

(f) providing, on request, a security consulting service for the design of new or renovated government buildings or the application of physical security equipment or systems to help institutions satisfy their protection responsibilities;

(g) when requested, reviewing and advising on EDP security in government institutions, other than for DND, and in the private sector where it is engaged in processing sensitive government information under contract through the EDP Security Evaluation and Inspection Team (SEIT);

(h) reporting to the Secretary of the Treasury Board, when requested, on the state of physical security across the government and, annually, on the security status of all EDP facilities in government institutions (SEIT Report);

(i) helping to determine the suitability of persons for reliability or security clearance, by checking criminal records and providing details of any adverse information to the CSIS, in the case of security clearances, to DND in respect of its own security clearances, and to departments in the case of reliability checks;

(j) conducting the security clearance of members and prospective members of the RCMP, other individuals employed or to be employed by or in the RCMP, and persons employed under contracts awarded or

administered by the RCMP. Where a search of security intelligence records is required, the CSIS shall carry out this activity; and

(k) carrying out specialized training on physical and EDP security, either directly or with the assistance of other government institutions, as required and mutually agreed upon.

Supply and Services Canada (SSC) is responsible for:

(a) ensuring that adequate safeguards are applied at off-government premises by non-government personnel or private sector organizations with access to or custody of Classified assets during a pre-contractual process, or under a contract or agreement to provide goods or services through SSC to the government;

(b) establishing the necessary policies and procedures to conform to the national interest provisions of the policy, including security clearances where required, of contractors providing goods or services through SSC to government departments and agencies; and

(c) arranging for the SEIT inspection of private sector EDP facilities that are involved in the processing of Classified or Designated information on contract with the federal government; reporting on the inspection to the chief officer of the private sector organization; and, on request, providing information on authorized private sector EDP facilities to government institutions.

The Treasury Board Secretariat is responsible for:

(a) identifying requirements for policy direction at a government-wide level; and

(b) developing a government-wide security policy and issuing such policy as approved by the Treasury Board; and

(c) providing coordination and leadership, including the tasking of lead agencies and interdepartmental committees, as required, in the process for the development of operational and technical security standards.*

---

* To be terminated effective June, 1990. Reassignment of this responsibility to be determined.

PROTECTED
DRAFT

APPENDIX C

Definitions

Breach of security: when any Classified or Designated information or assets have been the subject of unauthorized disclosure or unauthorized access. Without restricting its scope, a breach may include unauthorized disclosure by any person, theft, and loss or exposure in circumstances that make it probable that a breach has occurred.

Classified information: information that may cause injury, serious injury or exceptionally grave injury to the national interest and may qualify for a related ATIP exemption or is excluded from ATIP.

Confidential: level of classification that applies when compromise would reasonably be expected to cause injury to the national interest.

Designated information: information that may cause injury or serious injury to other than the national interest if compromised and may qualify for a related ATIP exemption or is excluded from ATIP.

Enhanced Reliability check: an assessment assuring an individual's trustworthiness. An enhanced reliability check comprises:

- a declaration, that is included in an individual's consent to screening, concerning any conviction for a criminal offence;
- verification of personal data, educational or professional qualifications, employment data and references;
- check of PSC's Separation for Cause Inventory System (SCIS);
- a fingerprint check, except for current federal government employees where the deputy head may decide that a criminal records name check will suffice;
- a credit check, when the duties or tasks to be performed, in the opinion of the manager require it;
- other checks, according to the duties or tasks to be performed and with the prior consent of the Treasury Board.

The completion of this verification to the satisfaction of the manager will result in the granting of reliability status.

National interest: concerns the defense and maintenance of the social, political and economic stability of Canada and thereby the security of the nation.

Secret: level of classification that applies when compromise could reasonably be expected to cause serious injury to the national interest.

Security clearance: and assessment of loyalty to Canada and, so far as it is related thereto, the reliability of an individual. It may comprise a check of:

- CSIS indices;
- character references;
- credit history;
- personal background normally covering a period of 10 years;
- subject interview.

An individual granted a security clearance may access, on a need to know basis, Classified information and assets.

Security standards: criteria set for usages or practices, that is operational and technical standards for government-wide use in the safeguarding of Classified and Designated information and assets, as approved by Treasury Board and designated lead agencies, respectively.

Significant degree: where the frequency of care and custody of, or access to, Designated information; or the sensitivity of Designated information; or the volume of Designated information is such that, in the opinion of the authorizing manager, personnel screening is warranted.

Top Secret: level of classification that applies when compromise could reasonably be expected to cause exceptionally grave injury to the national interest.

Threat and Risk Assessment (TRA): process of determining who might pose a threat to Classified or Designated information or assets, how the threat might be carried out, and vulnerabilities relative to threats, for the purpose of determining an appropriate course of action.

Violation of security: any action that contravenes any provision of the Security Policy. Such actions may include failure to classify or designate information in accordance with the policy; classification or designation, or continuation of same, in violation of the policy; unauthorized modification, retention, destruction or removal of Classified or Designated information; and unauthorized interruption of the flow of Classified or Designated information.

PROTECTED
DRAFT

APPENDIX D

Classifying and Designating Information

Institutions are responsible for classifying as Confidential, Secret or Top Secret information that is reasonably likely to be exempted or excluded from access under the following provisions of the Access to Information Act or the Privacy Act:

(a) where compromise could reasonably be expected to be injurious to

- the conduct by the Government of Canada of federal-provincial affairs (s.14, ATIA; s.20, Privacy Act),

- international affairs and defence, including the detection, prevention or suppression of subversive and hostile activities (s.15, ATIA; s.21, Privacy Act), or

- the economic interests of Canada (para. 18(a) and 18(d), ATIA);

(b) where the information is obtained or prepared by an investigative body during lawful investigations into activities suspected of being threats to the security of Canada within the meaning of the Canadian Security Intelligence Service Act (sub-para. 16(1)(a)(iii) and p. 16(1)(c), ATIA: sub-para. 22(1)(a)(iii) and para. 22(1)(b), Privacy Act);

(c) where the information relates to investigative techniques or plans for specific lawful investigations in relation to (b) above (para. 16(1)(b), ATIA);

(d) where the information would reveal the identity of a source in relation to the security clearance process (s.23 and para. 22(1)(b), Privacy Act, re: the granting, and review and updating of clearances);

(e) where the information contains advice, etc. relating to (a) to (c) above (s.21, ATIA);

(f) where the information relates to (a) to (c) above and its disclosure is prohibited by certain statutory provisions (s.24 and Schedule II, ATIA);

(g) where the records and drafts thereof that contain information relating to (a-c) above constitute confidences of the Queen's Privy Council for Canada (as described in s.69, ATIA or s.70, Privacy Act) including Treasury Board Papers;

(h) where records and drafts thereof are created and administered under the Cabinet Papers System, including:

- Memoranda to Cabinet
- Records of Cabinet Decisions
- Committee Reports
- Cabinet Minutes
- Cabinet Committee Minutes
- Briefing Notes for Committee Chairpersons and Members
- Agendas of Cabinet and Cabinet Committees
- Draft Orders in Council and Schedules thereto
- Draft Ministerial Orders

When requests are received under the Access to Information Act or the Privacy Act for records that have been classified, institutions should carefully review such records in order to determine whether or not exemptions should be invoked. A decision to deny access to a record, or any part of it, is based solely on the exemption provisions of the Acts as they apply at the time the request is made, and not on a security classification or other designation, however recently it may have been assigned.

In preparing guidelines for the classification of information, care should be taken to balance the risk of injury to the national interest against the cost of safeguarding information at high levels of classification.

Institutions are responsible for designating information that is reasonably likely to be exempted or excluded from access under the following provisions of the Access to Information Act or the Privacy Act:

(a) Law enforcement and investigations, where these do not relate to the national interest (s.16, ATIA; s.22 and s.24, Privacy Act);

(b) Safety of individuals (s.17, ATIA; s.25, Privacy Act);

(c) (i) Competitive position of government (para.18(b), ATIA)

(ii) Government Research (para.18(c), ATIA)

(iii) Undue benefit to a person (para.18(d), ATIA);

(d) Third-party (business) information (s.20, ATIA);

(e) Testing procedures, tests and audits (s.22, ATIA);

(f) Solicitor-client privilege (s.23, ATIA; s.27, Privacy Act);

(g) Information obtained in confidence from other governments (s.13, ATIA; s.19, Privacy Act);

(h) Medical records (s.28, Privacy Act);

(i) Advice etc. relating to non-national interest sensitive matters (s.21, ATIA);

(j) Certain statutory provisions prohibiting the disclosure of information which does not relate to the national interest (s.24 and Schedule II, ATIA);

(k) Personal information, as defined in section 3 of the Privacy Act; and

(l) Cabinet confidences, as defined in s.69(1) of the ATIA and ss.70(1) of the Privacy Act, which are not part of the Cabinet Papers System and do not otherwise qualify for classification in the national interest.