Treasury Board of Canada
Conseil du Trésor du Canada

Ottawa Canada
K1A 0R5

Security Policy of the Government of Canada

Canada

Treasury Board of Canada

Security Policy of the Government of Canada

Table of contents

.1 Introduction

.1.1 Purpose and scope

It is the purpose of this policy to prescribe a security system for the Government of Canada that will effectively protect classified information and other assets sensitive to the national interest from unauthorized disclosure, destruction, removal, modification or interruption. The policy is also intended to prescribe safeguards for other sensitive information and sensitive and valuable assets, to prevent improper classification, and to avoid unnecessary security clearances.

An equally important objective of this policy is a job-related screening system which will protect employer and national interest information by providing assurance that all persons engaged by the government meet the standards of reliability, trustworthiness and loyalty required by the nature of their duties or tasks.

To accomplish these objectives, this policy:

(a) establishes a system for the classification and protection of information and other assets which are sensitive to the national interest, and for declassification or downgrading when sensitivity disappears or diminishes;

(b) provides an enhanced level of protection for sensitive information and sensitive and valuable assets lying outside the national interest;

(c) reaffirms a base level of protection reflecting good management practices for all other government information and assets;

(d) establishes a security screening system to protect the national interest by requiring a current security clearance at the appropriate level for persons whose work requires them to have access to classified information or other assets sensitive to the national interest, or 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;

(e) safeguards the employer's interest by making a basic reliability check mandatory, with specified exceptions, for all persons engaged to perform duties or tasks for or within the government, and by requiring an enhanced check where duties or tasks have been identified as requiring a greater degree of trust;

(f) makes institutions responsible for detecting breaches and violations of security in relation to information and other assets under their control, and for applying appropriate countermeasures and sanctions; and

(g) directs institutions to develop their own security policy within the provisions of this policy and to assign internal accountability for implementation.

For the purpose of this policy, the national interest is considered to concern the defence and maintenance of the social, political and economic stability of Canada and thereby the security of the nation. Injury to the national interest is defined by the specific sections of the Access to Information and Privacy Acts as described in section .2 below.

.1.2 Application

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

In addition, the national interest requirements of the policy may apply to certain other institutions which require access to classified information and other assets sensitive to the national interest and to security screening services which have been the subject of agreements between the President of the Treasury Board and the Ministers responsible for these institutions. Agreements shall include a statement of the measures taken to implement the national interest provisions within the institutions concerned. Effective January 1, 1987, only institutions which are the subject of such agreements shall have the access to information, other assets and services described above. Except as otherwise noted, all appointments, assignments and contracts for goods and services are subject to the provisions of this policy.

.1.3 Authorities and cancellations

This policy is issued under the authority of the Financial Administration Act, by which the Treasury Board may act on all matters relating to administrative and personnel policy in the Public Service of Canada, and of Cabinet Decision 3-042485 RD. Treasury Board minute 802143 applies.

The policy replaces the 1956 Privy Council Office document entitled "Security of Information in the Public Service of Canada" and Cabinet Directive 35 of 1963, relating to security screening.

.1.4 Roles and responsibilities

.1.4.1 Individual government institutions Deputy heads of departments and heads of agencies (henceforth referred to in this policy as deputy heads) have full authority, within the provisions of this policy, for the administration of all aspects of security in their institutions.

Deputy heads are accountable for implementing this policy. Each shall designate a senior official to coordinate and direct the implementation of the policy within the institution.

In particular, in regard to personnel reliability and security screening, this means that deputy heads must:

(a) determine the screening requirements, based on the need for access to information or assets classified in the national interest or access to other sensitive information or sensitive or valuable assets;

(b) decide, after examining the information obtained about an individual, whether any risk attached to his or her appointment or assignment is justifiable and accept responsibility for the decision; and

(c) provide notice to individuals as required by the Canadian Security Intelligence Service Act and this policy.

.1.4.2 The Privy Council Office is responsible for advising deputy heads on decisions to order a formal investigation of suspected breaches of security, and on decisions to deny security clearances. The Privy Council Office also provides general guidance and advice on substantive decisions relating to security matters to deputy heads, and to senior officials designated by them to coordinate and direct the implementation of this policy in institutions. The Privy Council Office also performs certain functions assigned by this policy as they relate to specified Governor-in-Council appointments.

.1.4.3 The Department of the Solicitor General is responsible for providing advice and assistance to the Treasury Board in the development of government-wide policy and procedures pursuant to this policy.

.1.4.4 The Treasury Board Secretariat is responsible for developing and interpreting this policy, for coordinating the development of government-wide security policies and procedures and advising the Treasury Board on their adoption, for monitoring compliance with and evaluating the effectiveness of this security policy, and for reporting on its implementation.

.1.4.5 Government-wide and other roles A number of committees and institutions have roles which affect other departments and agencies with respect to the implementation of this policy. Roles relating to government-wide policy direction and management of implementation are set forth in Appendix A.

.2 Classified information and other assets

Information shall be classified, protected and declassified or downgraded in classification in accordance with this section. Other assets sensitive to the national interest shall be protected in accordance with article .2.8.

.2.1 Information to be classified

Government institutions shall classify information when its unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause injury to the national interest.

Institutions shall therefore classify that information which is exempt from access or excluded from the application of the Access to Information Act (ATIA) or the Privacy Act under the following provisions:

(a) where compromise of the information would 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 (s.18(a) and (d), ATIA);

(b) where the information is obtained or prepared by an investigative body in the course of lawful investigations pertaining to activities suspected of constituting threats to the security of Canada within the meaning of the Canadian Security Intelligence Service Act (s.16(1)(a)(iii) and 16(1)(c), ATIA; s.22(1)(a)(iii) and 22(1)(b), Privacy Act);

(c) where the information relates to investigative techniques or plans for specific lawful investigations in relation to (b) above (s.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 s.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 is prohibited from disclosure by certain statutory provisions (s.24 and Schedule II, ATIA); or

(g) where the information constitutes a confidence of the Queen's Privy Council for Canada (as described in s.69, ATIA or s.70, Privacy Act).

The basis for determining whether information is exempt or excluded under the above provisions and therefore classifiable in the national interest is set forth in the Treasury Board Interim Policy Guide: Access to Information Act and the Privacy Act, Parts II and III (TB Circular Letter 1983-35).

No information other than that which is exempt or excluded in accordance with the provisions of the Guide shall be classified in the national interest. In particular, in no case is information to be classified in the national interest in order to conceal violations of law, inefficiency or administrative error, to avoid embarrassment, or to restrain competition.

Classified information received from provincial, municipal or regional governments, from governments of other nations or from international organizations of nations or institutions thereof shall be protected at the level of TOP SECRET, SECRET or CONFIDENTIAL, as applicable, in accordance with agreements or understandings between the parties concerned.

.2.2 Levels of classification in the national interest

Information shall be classified as:

- TOP SECRET when unauthorized disclosure, destruction, removal, modification or interruption could reasonably be expected to cause exceptionally grave injury to the national interest;

- SECRET when any of these events could reasonably be expected to cause serious injury to the national interest; or

- CONFIDENTIAL when any such event could reasonably be expected to cause injury to the national interest.

These designations shall not be used for any other purpose than to classify information in the national interest.

Government institutions shall classify information at the level necessary for the protection of the national interest. Institutions shall develop their own guidelines indicating the necessary level for each kind of information to be classified. In preparing these guidelines, institutions should carefully balance the injury posed by

unauthorized disclosure, destruction, removal, modification or interruption of the information and the injury that would result, against the cost of safeguarding it at higher levels of classification. Guidelines shall be incorporated in departmental information classification guides prescribed in article .2.3.

While the RESTRICTED designation is not part of the Canadian classification scheme, information so designated, received from NATO countries or OECD sources, must be protected. Such information is to be safeguarded in accordance with agreements or understandings between the parties concerned. The designation RESTRICTED may be assigned to information originating in the Government of Canada only in relation to RESTRICTED information received from NATO countries or OECD sources.

.2.3 Authority to classify information in the national interest

Information shall be classified in the national interest only by:

- employees of a government institution when classification of the information is governed by an information classification guide, approved by the deputy head; or

- designated officials of the institution when particular information is not covered by such a guide.

Information classification guides must reflect the classification provisions of this policy, describe the kinds of information to be classified, and indicate the levels of classification to be applied.

The designation of officials must be in writing from the deputy head.

Both information classification guides and lists of designated officials are to be reviewed annually to ensure that guides are current, explicit and as comprehensive as possible, and that classification authority is still required for designated officials.

Where an employee requires a classification decision in the absence of a designated official, the employee may mark the information at the level he or she deems appropriate, provided the decision is confirmed within thirty days by the designated official concerned.

Classification authority is not required for the classification of information which derives from other information which has already been classified in accordance with this policy. Examples include extracts and summaries.

Institutions must ensure that all employees and designated officials engaged in the classification of information have a current security clearance at the highest level at which they will be required to classify information.

Appendix G
Conditions relating to Security Clearances

(a) Where a reliability check has been conducted before a security clearance request, information gathered as result of this check shall be forwarded through the Departmental Security Officer (DSO) to the investigative body. Security clearance investigations will be carried out by the Canadian Security Intelligence Service, with the exceptions noted in the roles of the Royal Canadian Mounted Police, Department of National Defence and the Department of External Affairs (see Appendix A). Requests for security clearances will be made through Departmental Security Officers on TB form, "Security Clearance Request and Authorization".

(b) In order to be considered for an assignment involving a reliability check or security clearance individuals will be requested to sign TB Form ___ "Consent to Disclosure of Personal Information". Such disclosures are governed by the provisions of the Privacy Act.

(c) Persons should be denied a security clearance if there are reasonable grounds to believe:

- they are engaged in, or may engage in activities that constitute a "threat to the security of Canada" as that term is defined in the Canadian Security Intelligence Service Act (definition is attached to this Appendix);

- because of personal beliefs, features of character, association with persons or groups considered a security threat, or family or other close ties of affection to persons living in oppressive or hostile countries:

  . they may act or may be induced to act in such a way as to constitute a "threat to the security of Canada", as defined; or

  . they may disclose, may be induced to disclose or may cause to be disclosed in an unauthorized way, government information classified in the national interest.

(d) A decision to grant or deny a security clearance must be based on adequate information. Where such information does not exist or cannot be obtained, then a security clearance cannot be given. An assessment which indicates that no information is available concerning an individual or which may cover only a very short period of his or her life, does not provide adequate grounds on which to base a security clearance.

(e) When a deputy head has denied or revoked a security clearance, the individual must be informed according to sub-section 42(1) and (2) of the CSIS Act.

(f) Individuals who have been granted a security clearance shall be briefed on their security responsibilities and sign TB Form ___ "Security Briefing and Declaration".

Definition of "Threat to the Security of Canada"

(a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage;

(b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person;

(c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political objective within Canada or a foreign state; and

(d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of the constitutionally established system of government in Canada,

but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (a) to (d).