Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Directive on Security Screening

Published: 2025-01-06

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-85/2025E-PDF
ISBN: 978-0-660-75242-6

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Directive sur le filtrage de sécurité

Directive on Security Screening

1. Effective date

1.1 This directive takes effect on January 6, 2025.

1.2 This directive replaces the *Standard on Security Screening* dated October 20, 2014.

1.3 Transitional consideration: The Standard on Security Screening Model and Position Analysis requires individuals who occupy positions at the Top Secret or Enhanced Top Secret level to be a Canadian citizen. All individuals in these positions will be deemed to meet this requirement when this directive comes into effect. They will continue to meet this requirement so long as they maintain a valid clearance at that level up to a maximum of five years from the effective date of this directive. This transitional consideration does not apply to individuals who are applying for a new clearance or to individuals whose existing clearance is being upgraded or downgraded at the Top Secret or Enhanced Top Secret levels.

2. Authorities

2.1 This directive is issued pursuant to the authorities indicated in section 2 of the *Policy on Government Security*.

2.2 The Treasury Board has delegated to the President of the Treasury Board the authority to amend and rescind this directive and any

supporting instruments, including standards, mandatory procedures and other appendices.

2.3 The Treasury Board has delegated to the President of the Treasury Board the authority to issue any supporting instruments, including standards, mandatory procedures and other appendices.

2.4 The Treasury Board has delegated to the President of the Treasury Board the authority to grant temporary exceptions, on a case-by-case basis, to this directive and any supporting instruments, including standards, mandatory procedures and other appendices.

3. Objectives and expected results

3.1 The objectives indicated in section 3 of the *Policy on Government Security* apply to this directive.

3.2 In addition to the expected results indicated in section 3 of the *Policy on Government Security*, the expected result of this directive is to ensure that security screening activities respect the principles of employment equity, diversity and inclusion and that these principles are applied consistently.

4. Requirements

Chief security officer

4.1 The chief security officer is to:

Security screening function

4.1.1 Lead and oversee the departmental security screening function to:

4.1.1.1 Enable the consistent and comprehensive conduct of security screening that:

4.1.1.1.1 Assesses the security screening requirements of positions, contracts or other arrangements;

4.1.1.1.2 Assesses the eligibility of an individual to hold a security or site access status, prior to a security or site access clearance;

4.1.1.1.3 Informs the decision-making process to grant, deny or revoke a security status or clearance, or site access status or clearance; and

4.1.1.1.4 Affords rights of review and redress that apply to all individuals, where a decision may be reached to deny, revoke or suspend a security status or clearance, or site access status or clearance;

4.1.1.2 Ensure that individuals:

4.1.1.2.1 Can be trusted to safeguard government information and assets, including information technology (IT) systems and facilities; and

4.1.1.2.2 Are aware of their security responsibilities;

4.1.1.3 Ensure departmental workforce awareness, capacity and capability to meet security screening function requirements, including respecting the values and principles of the Government of Canada;

4.1.1.4 Maintain a security file for all individuals for whom security screening is conducted in accordance with the *Privacy Act* and associated Government of Canada policy instruments;

4.1.1.5 Ensure that personal information for the purpose of security screening is:

4.1.1.5.1 Collected, created, used, disclosed, retained and disposed of in accordance with the *Privacy Act* and Government of Canada policy instruments;

4.1.1.6 Develop and implement processes to share information within the department and with other departments that:

4.1.1.6.1 Are defined and implemented;

4.1.1.6.2 Align with Government of Canada direction for managing security screening information;

4.1.1.6.3 Comply with the *Privacy Act* and Government of Canada policy instruments for handling personal information;

4.1.1.6.4 Facilitate the transfer and acceptance of security screening files with other departments; and

4.1.1.6.5 Enable sharing of information within the department and with other departments, where a decision is reached to deny, revoke or suspend a

security status or clearance or site access status or clearance;

4.1.2 When there is a requirement to conduct security screening of individuals external to government with whom the department has a need to share sensitive information or assets or to provide access to sensitive IT systems or facilities, ensure that:

4.1.2.1 Security screening requirements for contractors and other individuals are detailed in relevant documentation (see Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control of the *Directive on Security Management*); and

4.1.2.2 The required security status or clearance is granted before information is shared and access is provided;

Interdepartmental security screening services

4.1.3 Use security screening services where mandated or available to meet the departmental security screening requirements; and

4.1.3.1 Ensure that the services obtained meet those requirements;

4.1.4 Ensure that a written agreement is in place when the organization provides or receives security screening services from another organization pursuant to subsections 6.3 and 6.4 that:

4.1.4.1 Defines applicable security and privacy requirements, in collaboration with responsible departmental officials; and

4.1.4.2 Establishes respective security screening responsibilities;

4.1.5 Where the security screening function involves the provision of services to client departments:

4.1.5.1 Confirm that security screening requirements of client department positions are developed under the direction of the chief security officer of the client department; and

4.1.5.2 Before recommending a decision to grant, grant with conditions, deny or revoke a security status or clearance, consult the chief security officer and, as appropriate, the deputy head, of the client department;

Security risk and adverse information

4.1.6 Take measures to address any security risk that presents serious and immediate threats to the security of persons, information or assets of the department or the Government of Canada and, when appropriate:

4.1.6.1 Consult with human resources management regarding the suspension of an employee's security status or clearance;

4.1.6.2 Consult with the contracting authority regarding the suspension of a contractor's:

4.1.6.2.1 Security status or clearance; or

4.1.6.2.2 Site access status or clearance;

4.1.6.3 Suspend the security status or clearance or site access status or clearance of the individual, pending an investigation;

4.1.6.4 Revoke the security status or clearance or site access status or clearance of the individual, where they refuse to provide consent or withdraws consent 30 days after suspension; and

4.1.6.5 Report such security events to the appropriate law enforcement authority or security and intelligence agency (see Appendix I: Standard on Security Event Reporting of the *Directive on Security Management*);

Variation requests

4.1.7 Support the deputy head to obtain the approval of the President of the Treasury Board of any temporary exception to the application of this directive and any supporting instruments, including standards, mandatory procedures and other appendices, in consultation with the Treasury Board of Canada Secretariat and other stakeholders;

Life-cycle management

4.1.8 Establish and oversee the implementation and review of security screening practices for positions and individuals:

4.1.8.1 Define, document, and implement departmental practices for the life cycle of position analysis and security screening; and

4.1.8.2 Coordinate with departmental human resources management practices;

Monitoring and reporting

4.1.9 Monitor compliance with this directive:

4.1.9.1 Assess, investigate and report any significant compliance issues to the deputy head; and

4.1.9.2 Take action as directed by the deputy head;

4.1.10 Document and monitor security screening practices to meet identified security requirements for programs, services and activities; and

4.1.10.1 Ensure ongoing adherence with security screening practices;

4.1.11 Collaborate with senior officials and other stakeholders to respond to direction, advice and information requests issued by the Treasury Board of Canada Secretariat; and

4.1.12 Provide information to the Treasury Board of Canada Secretariat upon request.

Senior officials in the departmental security governance

4.2 Senior officials, designated by the deputy head in the departmental security governance, are to:

Security screening function

4.2.1 Participate in and report to the departmental security governance;

4.2.2 Collaborate with senior officials, security functional specialists, partners and other stakeholders to:

4.2.2.1 Identify security screening requirements and related resource needs for programs, services and activities;

4.2.2.2 Document and implement security screening practices to meet identified security requirements for programs, services and activities;

4.2.2.3 Ensure ongoing adherence with security screening practices;

4.2.2.4 Assign security screening responsibilities for programs, services and activities;

4.2.2.5 Document and implement departmental security rights of review and redress practices for security screening activities; and

4.2.2.6 Provide advice to the deputy head, the chief security officer and other stakeholders on departmental security screening matters in their area of responsibility;

Interdepartmental security screening services

4.2.3 Where the security screening function involves the provision of services to, or relies upon, another department, ensure that:

4.2.3.1 Support is provided to the chief security officer in meeting subsection 4.1.4 of this directive so that:

4.2.3.1.1 Requirements and responsibilities of the agreement are met; and

4.2.3.1.2 Compliance is monitored;

Security risk and adverse information

4.2.4 Address adverse information, in collaboration with the chief security officer, partners and other stakeholders; and

Monitoring and reporting

4.2.5 Monitor and report on the effectiveness of security screening practices within their area of responsibility and share the results with the chief security officer.

Security functional specialists and other designated individuals

4.3 Security functional specialists and other designated individuals in the departmental security governance are to:

4.3.1 Coordinate and provide support as appropriate in relation to the departmental security screening control to:

4.3.1.1 Implement departmental security screening practices as prescribed in the appendices of this directive;

4.3.2 Monitor and report on the effectiveness of security screening practices and share the results with the chief security officer to:

4.3.2.1 Assess the extent to which departmental security requirements are met; and

4.3.2.2 Identify necessary actions to address any deficiencies; and

4.3.3 Provide advice to the chief security officer and other stakeholders, as appropriate, on departmental security screening matters.

Managers

4.4 Individuals who have human resources responsibilities are to:

4.4.1 Integrate security screening considerations into planning and other administrative activities;

4.4.2 Collaborate with the chief security officer to determine the appropriate screening level for each position for which they are responsible:

4.4.2.1 In accordance with subsections A.2.2.4 and A.2.2.10 of Appendix A: Standard on Security Screening

Model and Position Analysis;

4.4.3 Ensure the established requirement of a security status or clearance as a condition of employment, appointment, contract or other arrangement, or assignment for positions for which they are responsible, is reflected in relevant documentation;

4.4.4 Ensure that individuals for whom they are currently responsible or may become responsible have a valid security status or clearance, as defined by the department's security screening requirements, before:

4.4.4.1 Issuing an unconditional job offer;

4.4.4.2 Awarding a contract; or

4.4.4.2.1 During the pre-contractual phase, providing a contractor access to sensitive information for the purpose of bidding;

4.4.4.3 Placing them in a position by means of other mechanisms such as an assignment, secondment, volunteer or other official capacity; and

4.4.4.4 Providing access to sensitive information and assets, including IT systems and facilities;

4.4.5 Ensure that individuals for whom they are responsible have received a security briefing prior to providing access to sensitive information and assets, including IT systems and facilities; and

4.4.6 Report to the chief security officer changes in personal circumstances and behaviour of individuals for whom they are responsible, which may affect the security status or clearance they have been granted.

Individuals

4.5 Individuals are to:

4.5.1 Provide their consent to initiate screening activities;

4.5.2 Provide the personal information and evidentiary documents required for security screening:

4.5.2.1 Accurately and truthfully; and

4.5.2.2 In accordance with the required format and established time frames and update cycles;

4.5.3 Indicate their understanding and acceptance of security responsibilities by signing the Security Screening Certificate and Briefing Form;

4.5.4 Perform their duties reliably and in compliance with:

4.5.4.1 The security status or clearance they are granted;

4.5.4.2 The security obligations detailed in the Security Screening Certificate and Briefing Form; and

4.5.4.3 Government of Canada security policy and departmental security practices, including safeguarding information and assets under their control, whether working onsite or offsite;

4.5.5 Notify their manager or chief security officer of the following:

4.5.5.1 Information related to a change in personal circumstances;

4.5.5.2 Any persistent or unusual contact, or any attempt by an individual, group, organization or other entity to solicit or obtain access to sensitive

information and assets, including IT systems and facilities, without authorization; or

4.5.5.3 Behaviour of individuals that may present a security risk to the department or the Government of Canada (as described in Appendix G: Mandatory Procedures for the Granting, Ongoing Maintenance and Assurance of the Security Screening of an Individual).

Individuals designated by deputy heads of internal enterprise service organizations to oversee their internal enterprise service activities

4.6 Individuals designated by deputy heads of internal enterprise service organizations authorized to provide enterprise security screening services to departments are to:

Security screening function

4.6.1 Support the deputy head, chief security officer and other stakeholders, as appropriate, on departmental security screening matters, including:

4.6.1.1 Ensuring that a written agreement is in place for security screening services provided to other organizations pursuant to subsections 6.3 and 6.4;

4.6.2 Make available to the deputy head or chief security officer of a client department upon request and in a timely manner:

4.6.2.1 Information that pertains to security screening activities and results, unless prohibited by law, including the *Privacy Act*, the *Criminal Records Act* or other applicable legislation; and

4.6.2.2 Advice and recommendations to support the result of security screening activities and inform

decision-making;

4.6.3 Maintain a security file for all individuals for whom security screening is conducted in accordance with the *Privacy Act* and associated Government of Canada policy instruments;

4.6.4 Ensure that personal information for the purpose of security screening is:

4.6.4.1 Collected, created, used, disclosed, retained and disposed of in accordance with the *Privacy Act* and Government of Canada policy instruments;

Security screening internal enterprise services

4.6.5 Ensure that individuals or organizations that are assigned responsibility for conducting security screening are qualified to do so, including that they:

4.6.5.1 Perform their responsibilities in accordance with legal and policy requirements, with the security interests of Canada in mind;

4.6.5.2 Monitoring compliance of security screening services against established service standards; and

4.6.5.3 Reporting any issues related to the fulfillment of security screening services to the affected departments and the Treasury Board of Canada Secretariat;

Monitoring and reporting

4.6.6 Monitor compliance with this directive:

4.6.6.1 Assess, investigate and report any significant compliance issues to the deputy head;

4.6.6.2 Take action as directed by the deputy head; and

4.6.6.3 Report findings to the Treasury Board of Canada Secretariat, including information to help inform government-wide policy direction and oversight;

4.6.7 Collaborate with senior officials and other stakeholders to respond to direction, advice and information requests issued by the Treasury Board of Canada Secretariat.

5. Roles of other government organizations

5.1 This section identifies key government organizations in relation to the *Policy on Government Security*. In and of itself, this section does not confer any authority.

5.2 This section identifies lead security agencies or internal enterprise service organizations that have a leadership and support role in relation to this directive and contribute to the achievement of government security policy objectives. The responsibilities of each organization are identified, in accordance with its mandate.

5.3 The following roles and responsibilities are supplementary to those defined in the *Policy on Government Security*.

5.4 The Canadian Security Intelligence Service is to:

5.4.1 Conduct, on behalf of departments, appraisals of the individuals' loyalty to Canada and, so far as it relates thereto their loyalty, their reliability.

5.5 The Communications Security Establishment is to:

5.5.1 Define criteria and formal control systems for access to signals intelligence (SIGINT) compartmented information to authorize government departments to perform indoctrinations and maintain the national inventory of indoctrinated personnel.

5.6 National Defence is to:

5.6.1 Process requests for visits when security-cleared military personnel must visit a government or military establishment in Canada or abroad; and

5.6.2 Define criteria and formal control systems for access to Talent-Keyhole (TK) compartmented information to authorize government departments to perform indoctrinations and maintain the national inventory of indoctrinated personnel.

5.7 Global Affairs Canada is to:

5.7.1 Conduct security screening of locally engaged staff and of other governments' officials at Canadian missions abroad.

5.8 Public Services and Procurement Canada is to:

5.8.1 Conduct security screening of contractors, other individuals and organizational entities as part of the government contracting process, including those participating in foreign contracts; and

5.8.2 Manage a visit-clearance request system for visitors accessing classified information in private sector premises and for foreign private sector individuals accessing classified information on government premises.

5.9 The Royal Canadian Mounted Police is to:

5.9.1 Conduct criminal record checks and law enforcement records checks to verify whether an individual has been convicted of a criminal offence and, when appropriate, to assess the person's involvement with criminality or with criminal organizations.

5.10 The Treasury Board of Canada Secretariat is to:

5.10.1 Determine the personal information that is to be collected, used, disclosed, retained and disposed of for the purpose of security screening, and maintain the description of the Standard Personal Information Bank PSU 917 (Security Screening) for this purpose.

6. Application

6.1 This directive applies to the organizations listed in subsection 6.1 of the *Policy on Government Security*.

6.2 The heads of the following organizations are solely responsible for monitoring and ensuring compliance with this directive within their organizations:

- Office of the Auditor General of Canada
- Office of the Chief Electoral Officer
- Office of the Commissioner of Lobbying of Canada
- Office of the Commissioner of Official Languages
- Office of the Information Commissioner of Canada
- Office of the Privacy Commissioner of Canada
- Office of the Public Sector Integrity Commissioner of Canada

6.3 Subsections 4.1.4 and 4.2.3.1 of this directive apply only to interdepartmental agreements pursuant to subsection 29.2 of the *Financial Administration Act* and to arrangements with Crown corporations, other orders of government, the private sector or other entities that are not governed by the *Policy on Government Security*, where the department has authority to enter into such agreements or arrangements.

6.4 Subsections 4.1.4 and 4.2.3.1 of this directive apply to contracts for the production or delivery of goods or services and to any other arrangement that involves the sharing of sensitive information or assets with organizations or individuals that do not fall under the application of the *Policy on Government Security*.

7. References

7.1 Legislation

- *Access to Information Act*
- *Canadian Charter of Rights and Freedoms*
- *Canadian Human Rights Act*
- *Canadian Security Intelligence Service Act*
- *Criminal Code*
- *Criminal Records Act*
- *Employment Equity Act*
- *Federal Public Sector Labour Relations and Employment Board Act*
- *Federal Public Service Labour Relations Act*
- *Financial Administration Act*
- *Inquiries Act*
- *National Security and Intelligence Review Agency Act*
- *Official Languages Act*
- *Privacy Act*
- *Public Service Employment Act*
- *Security of Canada Information Disclosure Act*
- *Foreign Interference and Security of Information Act*
- *Youth Criminal Justice Act*

7.2 Related policy instruments

- *Foundation Framework for Treasury Board Policies*
- *Policy on Government Security*
- *Policy on People Management*
- *Policy on Service and Digital*
- *Policy on Privacy Protection*
- *Policies for Ministers' Offices*
- *Values and Ethics Code for the Public Sector*
- *Directive on the Management of Procurement*
- *Directive on Identity Management*
- *Directive on Service and Digital*
- *Directive on Privacy Practices*

- *Directive on Privacy Impact Assessment*
- *Directive on Personal Information Requests and Correction of Personal Information*
- *Directive on Security Management*
- *Directive on Automated Decision-Making*
- *Directive on Employment Equity, Diversity and Inclusion*

7.3 Related guidance

- Guideline on Identity Assurance
- Guideline on Service and Digital
- Guidelines for Discipline
- Guidelines for Termination or Demotion for Unsatisfactory Performance; Termination or Demotion for Reasons Other than Breaches of Discipline or Misconduct; and Termination of Employment During Probation
- Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
- Privacy Implementation Notice 2023-03: Guidance Pertaining to the Collection, Use, Retention and Disclosure of Personal Information that Is Publicly Available Online

8. Enquiries

8.1 Members of the public may contact Treasury Board of Canada Secretariat Public Enquiries for information about this directive.

8.2 Individuals from departments should contact their departmental security management group for any questions regarding this directive.

8.3 Individuals from the departmental security group may contact the Security Policy Division at the Treasury Board of Canada Secretariat by email at SEC@tbs-sct.gc.ca for interpretation of this directive.

Appendix A: Standard on Security Screening Model and Position Analysis

A.1 Effective date

A.1.1 This standard takes effect on January 6, 2025.

A.2 Standards

A.2.1 This standard provides details on the requirements set out in subsections 4.1.1.1 and 4.6.1 of the *Directive on Security Screening*.

A.2.2 Standards are as follows:

A.2.2.1 Grant either a status or a clearance at the level required based on:

A.2.2.1.1 The position the individual occupies; or

A.2.2.1.2 The contract or other arrangement through which the individual is participating.

Security screening model for individuals

A.2.2.2 Conduct security screening for:

A.2.2.2.1 All positions or duties in the Government of Canada;

A.2.2.2.2 All contracts or other arrangement where there is a need to share or provide access to sensitive information and assets, including IT systems and facilities; and

A.2.2.2.3 In accordance with Annex A1.

A.2.2.3 Assess:

A.2.2.3.1 Reliability, honesty and trustworthiness as a function of eligibility to hold a status; and

A.2.2.3.2 Reliability, honesty, trustworthiness, loyalty to Canada, and reliability as it relates to that loyalty, as a function of eligibility to hold a clearance.

Position analysis for individuals

A.2.2.4 Determine the level of screening required for positions based on:

A.2.2.4.1 The duties to be performed;

A.2.2.4.2 The level of authority or control exercised by the position;

A.2.2.4.3 The sensitivity of information and assets, including IT systems and facilities to be accessed, including:

A.2.2.4.3.1 The degree of injury that could result from compromise; and

A.2.2.4.3.2 The need-to-know or need-to-access principle;

A.2.2.4.4 At a minimum, all positions are established at Reliability status when occupied by employees or other individuals working in departments as defined in section 2 and any other agency included in Schedules IV and V of the *Financial Administration Act* unless excluded by specific acts, regulations or orders-in-council; and

A.2.2.4.5 In accordance with the criteria identified within Annex A2.

A.2.2.5 Top Secret or Enhanced Top Secret level clearances are to be granted only to employees or other individuals who have Canadian citizenship; and

A.2.2.6 Extend security screening to an enhanced level in accordance the criteria identified within Annex A2.

Security requirements for contracts and other arrangements

A.2.2.7 In accordance with Appendix F: Mandatory Procedures for Security in Contracts and Other Arrangements Control of the *Directive on Security Management*, contracts and other arrangements that have an assessed security requirement to a Top Secret or Enhanced Top Secret level are to be granted only to contractors or other individuals who have Canadian citizenship.

Site access screening model for non-employees

A.2.2.8 Conduct site access screening for:

A.2.2.8.1 Individuals who are not employees and have a need to access protected or restricted areas or facilities; and

A.2.2.8.2 In accordance with Annex A3.

A.2.2.9 Assess:

A.2.2.9.1 Reliability, honesty and trustworthiness as a function of eligibility to hold a status; and

A.2.2.9.2 Reliability, honesty, trustworthiness, loyalty to Canada and reliability, as it relates to that loyalty, as a function of eligibility to hold a clearance.

Position analysis for non-employees

A.2.2.10 Determine the level of site access screening required for contracts or other arrangements based on:

A.2.2.10.1 The sensitivity and nature of departmental programs, services and activities;

A.2.2.10.2 The nature of the duties or services to be performed;

A.2.2.10.3 Whether the individual will be escorted or unescorted;

A.2.2.10.4 Whether the individual requires access to the exterior or interior of a facility;

A.2.2.10.5 The risk of the individual inadvertently seeing or overhearing sensitive information or conversations; and

A.2.2.10.6 In accordance with the criteria identified in Annex A4.

Annex A1: Levels of Security Screening and Associated Activities

Level	Security screening activities	Level	Security screening activities
Reliability status Validity: 10 years	• Verification of identity • Verification of 5 years of background information • Verification of educational and professional credentials • Personal and professional reference checks • Financial inquiry (credit check) • Criminal record check	**Enhanced Reliability status** Validity: 10 years	All activities for Reliability status plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview

Level	Security screening activities	Level	Security screening activities
Secret clearance Validity: 10 years	All activities for Reliability status plus: • Verification of 10 years of background information • CSIS security assessment	**Enhanced Secret clearance** Validity: 10 years	All activities for Secret clearance plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview
Top Secret clearance Validity: 5 years	All activities for Secret clearance plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview • Foreign travel, passports, assets and military service • Canadian Citizenship	**Enhanced Top Secret clearance** Validity: 5 years	All activities for Top Secret clearance plus: • Polygraph examination

Annex A2: Criteria for Determining Level of Security Screening

Level	Criteria for determining level	Access permissions
Reliability Status	• Conduct screening of individuals to the level of Reliability: ◦ When positions require: ▪ Unsupervised access to Government of Canada information and assets; ▪ Unescorted access to physical security zones in facilities, where Government of Canada protected information is processed; or ▪ User-level access to IT systems categorized as Protected A or B. ◦ As the minimum screening for all positions.	• Access to informatio assets, or I systems categorize as Protecte A or B

Level	Criteria for determining level	Access permissions

Secret clearance	• Conduct screening of individuals to the level of Secret:
	  ◦ Building on screening criteria for a Reliability status and when positions require:
	  ▪ Unsupervised access to Government of Canada information and assets categorized as Secret;
	  ▪ Unescorted access to Physical security zones in government facilities where Secret information is processed; or
	  ▪ User-level access to IT systems categorized as Secret.
		• Access to informatio assets or I systems categorize as Protecte A, B, Confidenti and Secret
		• Access to I systems categorize as Protecte A, B, Confidenti and Secret
		• Enhanced privileges (administra access) to systems

Top Secret clearance	• Conduct screening of individuals to the level of Top Secret:
	  ◦ Building on screening criteria for a Secret clearance and when positions require:
	  ▪ Unsupervised access to Government of Canada information and assets categorized as Top Secret;
	  ▪ Unescorted access to Physical security zones in government facilities, where Top Secret information is processed; or
	  ▪ User-level access to IT systems categorized as Top Secret.
		• Access to informatio assets or I systems categorize as Protecte A, B or C o classified a any level
		• Restricted access to specific To Secret networks systems

Level	Criteria for determining level	Access permissions

Enhanced Reliability status	• Conduct screening of individuals to the level of Enhanced Reliability:
	  ◦ Building on screening criteria for Reliability status and when positions require:
	  ▪ Individuals to perform security and intelligence functions, including:
	  ▪ Uncontrolled access to criminal or law enforcement intelligence information or assets, including IT systems or unescorted access to physical security zones within facilities where this information is processed or stored; or
	  ▪ Duties that support those functions.
		• Access to informatio and assets including I systems categorize as Protecte A, B or C

Level	Criteria for determining level	Access permissions

Enhanced Secret clearance	• Conduct screening of individuals to the level of Enhanced Secret:
	  ◦ Building on screening criteria for a Secret clearance and when positions require:
	  ▪ Individuals to perform security and intelligence functions, including:
	  ▪ Uncontrolled access to criminal or law enforcement intelligence information or assets classified as Secret, including IT systems or unescorted access to physical security zones within facilities where this information is processed or stored; or
	  ▪ Duties that support those functions and that:
	  ▪ Require unsupervised access to Secret law enforcement information or assets.
		• Access to informatio IT systems and assets categorize as Protecte A, B, C, Confidenti and Secret
		• Enhanced privileges (administra access) to systems

Level	Criteria for determining level	Access permissions

Enhanced Top Secret clearance	• Conduct screening of individuals to the level of Enhanced Top Secret:
	  ◦ Building on screening criteria for a Top Secret clearance and when positions require:
	  ▪ Individuals to perform defence, security and intelligence functions, including:
	  ▪ Uncontrolled access to criminal or law enforcement intelligence information or assets categorized as Top Secret, including IT systems; or
	  ▪ Unsupervised access to methods, sources, analytical processes, plans and techniques related to the collection of sensitive intelligence or counter-intelligence information; or
	  ▪ Unescorted access to physical security zones within facilities where criminal or law enforcement intelligence is processed or stored;
	  ▪ Duties that support those functions and that:
	  ▪ Require uncontrolled access to Top Secret assets; or
	  ▪ Unescorted access to physical security zones within facilities where this information
		• Access to governme information assets or I systems categorize as protecte or classifie at any leve

Level	Criteria for determining level	Access permissions
	is processed or stored.	

Annex A3: Levels of Site Access Screening and Associated Activities

Level	Activities
Site Access status Validity: 10 years	• Verification of identity • Verification of 5 years of background information • Criminal record check
Site Access clearance Validity: 10 years	All activities for Site Access status plus: • CSIS security assessment
Additional activities may be used in accordance with subsection A.2.2.10, “Position analysis for non-employees.”	All activities for Site Access clearance plus: • Personal and professional reference checks • Internet inquiry • Law enforcement records check • Security questionnaire or security interview • Polygraph examination

Annex A4: Criteria for Determining Level of Site Access Screening

Level	Criteria for determining level	Access permissions

Site Access status	• Conduct screening of individuals to the level of Site Access status:
	  ◦ As the minimum level of Site Access screening and there is a requirement to:
	  ▪ Enter areas where protected information and assets are present whether being processed or stored; or
	  ▪ As required, access areas that form part of the controlled hierarchy of physical security zones;
	  ◦ When access to sensitive government information is not required; and
	  ◦ The individual is not an employee.
		• Unescorted access to federal government facilities and restricted access areas within those facilities
		• No access to information

Level	Criteria for determining level	Access permissions
Site Access clearance	• Conduct Site Access clearance screening of individuals: ◦ Building on screening criteria for a Site Access status and there is a requirement to: ▪ Enter areas where classified information and assets are present, whether being processed or stored; ▪ Enter restricted access areas of law enforcement facilities; or ▪ As required, access areas that form part of the controlled hierarchy of physical security zones; ◦ When access to sensitive government information is not required; and ◦ The individual is not an employee.	• Unescorted access to federal government facilities and restricted access areas within those facilities • Unescorted access to law enforcement facilities • No access to information

Appendix B: Mandatory Procedures for Management of Personal Information for the Purpose of Security Screening

B.1 Effective date

B.1.1 These procedures take effect on January 6, 2025.

B.2 Procedures

B.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.1, 4.1.1.4, 4.1.1.5, 4.1.1.6, 4.6.1, 4.6.3 and 4.6.4 of the *Directive on Security Screening*.

B.2.2 Mandatory procedures are as follows:

Safeguarding of personal information

B.2.2.1 Assign a security category to personal information, commensurate with the sensitivity of the information, in accordance with Appendix E: Mandatory Procedures for Information Management Security Control of the *Directive on Security Management*; and

B.2.2.1.1 Implement measures to protect sensitive information using appropriate security controls.

Collection and creation of personal information: personal information banks

B.2.2.2 Collect, create, use, disclose, retain and dispose of personal information for the purposes of security screening in accordance with the *Privacy Act* and the *Directive on Privacy Practices*.

Security screening forms and models

B.2.2.3 Collect personal information using Treasury Board of Canada Secretariat prescribed forms and models.

Consent regarding collection, use and disclosure

B.2.2.4 In accordance with the *Directive on Privacy Practices*, before information is collected, used or disclosed, obtain informed consent:

B.2.2.4.1 Of the individual; or

B.2.2.4.2 Of the legal parent or guardian when conducting security screening for individuals under the age of 18.

Failure to provide consent or information

B.2.2.5 When an individual does not provide consent, withdraws consent or does not provide the required information for security screening, cease screening activities and:

B.2.2.5.1 When the security screening action is for an initial or upgraded security screening:

B.2.2.5.1.1 Inform the individual that:

a. Security screening cannot proceed without consent or the required information; and
b. Failure to provide consent and the required information will result in the individual no longer being considered for appointment, employment, contract, assignment or other arrangement;

B.2.2.5.1.2 Administratively cancel the screening process until consent and the required information are obtained; and

B.2.2.5.1.3 Where security screening is being conducted in support of a contract, inform the contracting authority;

B.2.2.5.2 When the security screening action is for an update:

B.2.2.5.2.1 Inform and consult with the manager of the individual;

B.2.2.5.2.2 Evaluate the risk associated with the individual remaining in their position; and

B.2.2.5.2.3 Where the individual does not provide the required information and the update:

a. Cannot proceed as a result of the missing information; or
b. Cannot be completed before the status or clearance exceeds its validity period; and
c. Presents an unacceptable security risk to the department or the Government of Canada:

B.2.2.5.2.3.1 Consult with human resources management or inform the contracting authority; and

B.2.2.5.2.3.2 Suspend the status or clearance and initiate a review for cause; or

B.2.2.5.2.4 Where an individual does not provide consent or withdraws consent:

B.2.2.5.2.4.1 Document refusal of the individual to provide

consent and notify them of the consequences of not providing consent;

B.2.2.5.2.4.2 Suspend the status or clearance of the individual; and

B.2.2.5.2.4.3 Revoke the status or clearance of the individual 30 days after suspension if consent has not been obtained within that time.

Security screening file management

B.2.2.6 Create and maintain a file (record) for each individual who undergoes security screening that contains relevant personal information, including:

B.2.2.6.1 Completed original digital or paper copies of security screening forms and questionnaires;

B.2.2.6.2 Relevant results of all security screening activities, verifications, inquiries and assessments, with each of these dated;

B.2.2.6.3 Analysis of results and any advice or recommendations to support decision-making;

B.2.2.6.4 Decisions to grant, grant with conditions, deny, revoke, suspend pending investigation, or administratively cancel a security status or clearance; and

B.2.2.6.5 Relevant information related to any conditions, temporary access, review for cause, or investigation, and any ensuing decisions.

B.2.2.7 Update security screening files when:

a. A change is reported in the personal circumstances of the individual, including at minimum any of the following:
    i. Change in criminal record status;
    ii. Involvement with law enforcement;
    iii. Association with criminals;
    iv. A significant change in financial situation; or
    v. Where an individual works in security or intelligence organizations, additional changes in their personal or legal status;
b. There is a change in a security status or clearance of the individual;
c. The security status or clearance of the individual is subject to review for cause; or
d. A decision is made with respect to the above.

B.2.2.8 Ensure that any results of department-specific inquiries conducted against departmental data sources and indices are included in the security screening file of an individual only when it is used to resolve doubt.

B.2.2.9 Remove from security screening files and dispose of information related to criminal offences for which the individual received a record suspension.

Transfer of security screening files

B.2.2.10 Make available the security screening file of the individual to facilitate the temporary or permanent movement of:

B.2.2.10.1 An individual within or between departments; or

B.2.2.10.2 A contractor between contracts;

B.2.2.11 Transfer the security screening file of an individual:

B.2.2.11.1 Upon request and in a timely manner;

B.2.2.11.2 When they move permanently to another department;

B.2.2.11.3 In accordance with requirements for reactivation and expiry;

B.2.2.11.4 Except for:

B.2.2.11.4.1 Any classified CSIS security assessment, which must be returned to CSIS:

B.2.2.11.4.1.1 Advise the chief security officer of the receiving department of the existence of the assessment; and

B.2.2.11.4.2 A record of discharge under section 730 of the *Criminal Code* must not be:

a. Transferred to another department, including acknowledgement of the existence of the record; and
b. Disclosed, including the fact that the discharge occurred, unless prior approval of the Minister of Public Safety is received if:
    i. More than one year has elapsed since

the individual was discharged absolutely; or

ii. More than three years have elapsed since the individual was discharged on the conditions prescribed in a probation order.

B.2.2.12 Upon receipt of a transferred security screening file:

B.2.2.12.1 Update security screening activities where:

a. The results exceed the validity period;
b. There is evidence to suggest that the security screening was not previously done in accordance with this directive;
c. There are conditions attached to the status or clearance;
d. Results of criminal record checks, law enforcement records checks or security assessments have been removed from the file; or
e. There is adverse information on file that may represent a security risk to the receiving department; and

B.2.2.12.2 Record the rationale for not accepting a current status or clearance within a transferred security

screening file, and redo the security screening of the individual.

B.2.2.13 Upon transfer of the security clearance of an individual, notify CSIS via form CSIS 4160 Notification of Change in Security Clearance.

Deactivation and reactivation

B.2.2.14 Deactivate a valid security status or clearance when:

B.2.2.14.1 An employee has:

a. Retired or otherwise terminated employment; or
b. Taken an authorized absence from the Government of Canada longer than:
    i. Two years for a status; or
    ii. One year for a clearance; or
c. Taken an unauthorized absence from the Government of Canada longer than 30 days; or

B.2.2.14.2 A contractor or other individual has been removed from the contract or other arrangement; or

B.2.2.14.3 The contract or other arrangement has been completed, cancelled or terminated.

B.2.2.15 Reactivate the security status or clearance:

B.2.2.15.1 Only within the original validity period; and

B.2.2.15.2 If an employee returns to active employment and is no more than:

a. Two years removed from having possessed a valid security status; or

b. One year removed from having possessed a valid security clearance; or

B.2.2.15.3 If a contractor or other individual is no more than:

a. Two years removed from having possessed a valid security status;
b. One year removed from having possessed a valid security clearance; or
c. One year removed from having possessed a valid Site Access status or clearance.

B.2.2.16 When reactivating a status or a clearance:

B.2.2.16.1 Revalidate identity information;

B.2.2.16.2 Require individuals to account for their activities during the period of absence and the circumstances surrounding their departure;

B.2.2.16.3 Do not extend the validity period; and

B.2.2.16.4 Do not reactivate a security status or clearance and repeat the security screening when:

B.2.2.16.4.1 The circumstances surrounding the departure involve:

a. Review for cause;
b. Suspension pending an investigation;
c. An outstanding resolution of doubt; or
d. Disciplinary reasons; or

B.2.2.16.4.2 There is adverse information or conditions on file; or

B.2.2.16.4.3 The status or clearance has exceeded its validity period.

B.2.2.17 Administratively cancel a security status or clearance or Site Access status or clearance once the reactivation period for the individual has elapsed and there has been no activity on the file.

File retention and disposition

B.2.2.18 Retain security screening files of individuals contained in:

B.2.2.18.1 Standard Personal Information Bank PSU 917 (Security Screening) for a minimum of two years following the departure of the individual from the federal public service:

B.2.2.18.1.1 Prevent security screening files of individuals who have left the employment of the federal public service from being transferred to the departmental Personnel Records Centre or to any Regional Service Centre of Library and Archives Canada; and

B.2.2.18.2 Standard Personal Information Bank PSU 917 (Security Screening) who have been denied or had revoked a security status or clearance for a minimum of 10 years following their departure from the federal public service.

Appendix C: Mandatory Procedures for

Security Screening Activities

C.1 Effective date

C.1.1 These procedures take effect on January 6, 2025.

C.2 Procedures

C.2.1 These procedures provide details on the requirements set out in subsections A.2.2.2.3, A.2.2.3, A.2.2.8.2 and A.2.2.9 of the Standard on Security Screening Position Analysis and Model.

C.2.2 Mandatory procedures are as follows:

C.2.2.1 Conduct security screening activities in accordance with Annex A1 and Annex A3 of Appendix A: Standard on Security Screening Position Analysis and Model as identified below:

C.2.2.1.1 Verify identity before undertaking any subsequent security screening activities; and

C.2.2.1.2 Conduct all subsequent security screening activities in relation to the individual;

Identity verification practices

C.2.2.1.3 Verify evidence of identity in accordance with the Standard on Identity and Credential Assurance; and

C.2.2.1.3.1 Apply identity and credential assurance level 3 as the minimum level required for all levels of security screening;

Background verification practices

C.2.2.1.4 Verify the accuracy of the background information provided by the individual through a risk-based approach:

C.2.2.1.4.1 Where it is not possible to verify all the required years of background information, consider:

C.2.2.1.4.1.1 Alternate sources of information, including but not limited to:

C.2.2.1.4.1.1.1 Additional references; and

C.2.2.1.4.1.1.2 Resolution of doubt in accordance with Appendix E: Mandatory Procedures for Resolution of Doubt and Review for Cause;

C.2.2.1.4.2 Account for individuals who have lived outside of Canada for longer than six months consecutively within the time period required by the security status or clearance in the following ways:

a. A letter of reference or referral from a foreign embassy or mission in Canada;
b. A letter of reference or referral from a Canadian

embassy or mission in the country or countries in which the individual resided;

c. A letter of reference from a foreign educational institution or university;
d. A letter or police clearance certificate from a law enforcement agency of jurisdiction in the country in which the individual resided;
e. A credit summary from an established foreign financial institution;
f. Employment or assignment with a Government of Canada department or agency or with the Canadian Armed Forces outside Canada;
g. Information from counterpart security screening organizations in countries with which Canada has entered into bilateral arrangements for the exchange of security screening information; or
h. Alternate sources of information that are sufficient to account for

their activities and the associated risk;

C.2.2.1.4.2.1 Assess activities accounted for in one or more of these ways in consideration of the adequacy and reliability of the source;

Educational and professional credential verification

C.2.2.1.5 Verify relevant educational and professional credentials and designations;

Personal and professional reference checks

C.2.2.1.6 Verify information about the individual from persons who know or who are in a position to take notice of the individual;

Financial inquiry

C.2.2.1.7 Obtain a full consumer credit report from a credit reporting agency that:

C.2.2.1.7.1 Includes information on the credit history, liens, judgments or bankruptcy of the individual; and

C.2.2.1.7.2 Excludes and does not negatively affect the credit score of the individual;

C.2.2.1.8 Where a reliable credit report from a credit reporting agency cannot be obtained, develop and administer a financial assessment questionnaire for individuals; and

C.2.2.1.9 Apply the results of the financial inquiry to assess whether an individual poses a security risk on the

basis of financial pressure or a history of poor financial responsibility;

Criminal records check

C.2.2.1.10 Obtain a criminal record check against the RCMP's National Repository of Criminal Records to confirm the involvement of the individual in criminal activity;

C.2.2.1.11 Require individuals who have lived outside of Canada for longer than six months consecutively within the time period required by the security status or clearance to:

C.2.2.1.11.1 Obtain a police clearance certificate or equivalent documentation that provides:

a. A summary of an individual's criminal record; or
b. A declaration of the absence of any criminal record;

C.2.2.1.11.2 Where a country of residence:

a. Does not provide police clearance certificates or equivalent documentation; or
b. Obtaining the documentation presents undue risk to the individual, consider:

C.2.2.1.11.2.1 Alternate sources of information, sufficient to:

C.2.2.1.11.2.1.1 Confirm the involvement or absence thereof, of the individual in criminal activity; and

C.2.2.1.11.2.1.2 Assess the risk associated with past criminal convictions;

C.2.2.1.12 Apply the results of criminal record checks and out-of-country documentation to assess the risk associated with past criminal convictions.

CSIS security assessment

C.2.2.1.13 Obtain a CSIS security assessment to:

C.2.2.1.13.1 Determine whether there is sufficient information available upon which to base a security screening decision; and

C.2.2.1.13.2 Assess, where sufficient information is available, whether there is reasonable cause to believe that the individual has engaged, is engaged or may engage in activities that constitute a “threat to the security of Canada,” as defined in

section 2 of the *Canadian Security Intelligence Service Act*;

Internet inquiry

C.2.2.1.14 Review publicly available personal information on the Internet to:

C.2.2.1.14.1 Verify accuracy and integrity of the background information provided by the individual; and

C.2.2.1.14.2 Identify potential adverse information based on behaviours, conduct, associations, judgment or features of character;

C.2.2.1.15 Take reasonable steps to verify the accuracy of information obtained from the Internet inquiry;

Law enforcement records check

C.2.2.1.16 Obtain additional RCMP and jurisdictional police agency records to verify:

C.2.2.1.16.1 Outstanding warrants or prohibitions; and

C.2.2.1.16.2 Whether an individual has any associations with criminality or organized crime;

Security questionnaire or security interview

C.2.2.1.17 Develop and conduct a security questionnaire or a security interview that solicits information to:

C.2.2.1.17.1 Identify and validate adverse information;

C.2.2.1.17.2 Provide the individual an opportunity to explainadverse information; and

C.2.2.1.17.3 Assess security risk on the basis of ideology, conduct, associations, judgment, features of character and vulnerability to coercion;

Polygraph examination

C.2.2.1.18 Conduct a polygraph:

C.2.2.1.18.1 For positions that require an Enhanced Top Secret security clearance; or

C.2.2.1.18.1.1 Where necessary to comply with international information-sharing agreements entered into by the Government of Canada; and

C.2.2.1.18.2 To corroborate the results of security screening activities, including the absence of results;

Canadian citizenship verification

C.2.2.1.19 Verify Canadian citizenship for a Top Secret or Enhanced Top Secret security clearance:

C.2.2.1.19.1 In accordance with documents prescribed by the Government of Canada.

Appendix D: Mandatory Procedures for Collective Evaluation of Security Screening Activities

D.1 Effective date

D.1.1 These procedures take effect on January 6, 2025.

D.2 Procedures

D.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.1.2 and 4.6.1 of the *Directive on Security Screening*.

D.2.2 Mandatory procedures are as follows:

Identity verification

D.2.2.1 Administratively cancel the security screening process when identity information cannot be verified, despite reasonable and demonstrable effort.

Canadian citizenship verification

D.2.2.2 Administratively cancel the security screening process when Canadian citizenship cannot be verified, despite reasonable and demonstrable effort, for Top Secret and Enhanced Top Secret security clearance.

Collective evaluation of security screening activities

D.2.2.3 Collectively evaluate the results of security screening activities:

D.2.2.3.1 Based on:

D.2.2.3.1.1 The quality, quantity, relevance, credibility and totality of the information available relative to the

level of status or clearance being considered;

D.2.2.3.1.2 The contextual factors associated with the position, contract or other arrangement, including the totality of information related to the individual; and

D.2.2.3.1.3 Consider as a factor the presence of adverse information and information obtained through a resolution of doubt;

D.2.2.3.2 To assess:

D.2.2.3.2.1 The reliability of an individual, including their honesty and trustworthiness, based on whether they can be trusted to:

a. Safeguard information and assets, including IT systems and facilities;
b. Be relied upon to not abuse the level of trust accorded;
c. Perform the assigned duties in a manner that will reflect positively on the Government of Canada; and
d. Not pose a security risk to the Government of Canada;

D.2.2.3.2.2 Loyalty to Canada, as applicable, where there are reasonable grounds to believe

that:

a. The individual has engaged, is engaged, may engage or may be induced to engage in activities that constitute a threat to the security of Canada as defined in the *Canadian Security Intelligence Service Act*; or
b. In so far as it relates to reliability as it relates to loyalty:
    i. The individual has acted, is acting, may act or may be induced to act in a way that constitutes a threat to the security of Canada; or
    ii. The individual has disclosed, may disclose, may be induced to disclose or may cause to be disclosed sensitive information in a manner

contrary to the public interest;

D.2.2.3.2.2.1 Consider the presence of information that supports the likelihood of these scenarios as the basis to deny a security clearance or Site Access clearance;

D.2.2.3.2.2.2 Consider the absence of adverse information pursuant to a CSIS security assessment as a factor in favour of whether to grant a security clearance or Site Access clearance; and

D.2.2.3.2.2.3 Consider insufficient information required for the CSIS security assessment as grounds upon which to deny a security clearance or Site Access clearance;

Identification and assessment of adverse information

D.2.2.4 Assess the significance of adverse information based on the specific details of that information and in light of the totality of an individual's circumstances, including:

a. Mitigating and aggravating factors;
b. The nature of the adverse information;
c. The frequency of the adverse information;

d. The circumstances surrounding the adverse information, including;
    i. The impact of socio-economic and cultural factors as identified by the individual;
e. The severity of the adverse information;
f. The passage of time;
g. The duties to be performed;
h. Whether the individual has been forthcoming about the information; and
i. The remedial action and rehabilitation efforts of the individual;

D.2.2.5 Where an Internet inquiry uncovers potential adverse findings, before rendering a decision, provide the individual with the opportunity to:

D.2.2.5.1 Review a summary of the potential adverse findings; and

D.2.2.5.2 Explain the findings;

D.2.2.6 Deny a security status or clearance to an individual who cannot hold public office, contract or receive benefits under a contract pursuant to sections 750(2) and 750(3) of the *Criminal Code*;

Review and reporting of adverse information

D.2.2.7 Review adverse information as a basis for further investigation, including a resolution-of-doubt interview; and

D.2.2.8 Where the security screening function involves the provision of services to client departments, report adverse information to the chief security officer of the client department considering employment, appointment, contract or other arrangement, or assignment of the individual.

Appendix E: Mandatory Procedures for Resolution of Doubt and Review for Cause

E.1 Effective date

E.1.1 These procedures take effect on January 6, 2025.

E.2 Procedures

E.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.1.2, 4.1.1.1.3, 4.1.1.2 and 4.1.6 of the *Directive on Security Screening*.

E.2.2 Mandatory procedures are as follows:

E.2.2.1 Demonstrate and document that adverse and missing information have been thoroughly addressed; and

E.2.2.2 Conduct a resolution of doubt or review for cause as expeditiously as possible;

Resolution of doubt

E.2.2.3 Initiate a resolution of doubt when unverifiable, missing or adverse information is uncovered during the security screening of an individual;

E.2.2.4 Provide the individual with a summary of the adverse, missing and unverifiable information in question:

E.2.2.4.1 Prior to disclosure to the individual:

E.2.2.4.1.1 Consult the investigative body when adverse information is uncovered as a result of:

a. An RCMP law enforcement records check; or
b. A CSIS security assessment;

E.2.2.4.1.2 Exclude information that cannot be disclosed:

a. For reasons of national security;
b. That could endanger the safety of any person; and
c. That would be exempt under the *Privacy Act* sections 18, 19, 20 and 21, and subsections 22(1) to 22(3);

E.2.2.5 Conduct additional security screening activities:

E.2.2.5.1 To resolve doubt when information is available or reported about an individual that may cast doubt on their reliability or loyalty to Canada; and

E.2.2.5.2 Where:

E.2.2.5.2.1 Individual consent has been obtained; and

E.2.2.5.2.2 The department has the legal authority to do so;

E.2.2.6 Before a decision is rendered, conduct a resolution-of-doubt interview to provide the individual an opportunity to discuss any matters of concern and to explain the situation; and

E.2.2.7 Consider information obtained through a resolution of doubt toward the eligibility of an individual to be granted a security status or clearance;

Review for cause

E.2.2.8 Initiate a review for cause of the security status or clearance previously granted to an individual when:

E.2.2.8.1 Information is uncovered or reported about an individual that may call into question their reliability or loyalty to Canada; or

E.2.2.8.2 Adverse information reflects:

E.2.2.8.2.1 Recent questionable judgment or dishonesty; or

E.2.2.8.2.2 A recurring pattern of questionable judgment or dishonesty;

E.2.2.9 When conducting a review for cause, in accordance with subsection F.2.2.11 of Appendix F: Mandatory Procedures for Security Screening Decisions and Notifications, pending the outcome, consider a decision to suspend:

E.2.2.9.1 A security status or clearance; or

E.2.2.9.2 Access to sensitive information and assets, including IT systems and facilities;

E.2.2.10 Undertake the review-for-cause process, as an administrative investigation, including an interview of the individual;

E.2.2.11 When a review for cause is conducted in parallel to a disciplinary process for an employee:

E.2.2.11.1 Administer the processes with distinct decisional authorities; and

E.2.2.11.2 Record a disciplinary decision in the security file only where it relates to a security concern; and

E.2.2.11.3 Consult with:

a. Departmental human resources management; and

b. The Centre for Labour and Employment Law, as required; and

E.2.2.12 Consider information obtained through a review for cause on the continued eligibility of an individual to retain a security status or clearance.

Appendix F: Mandatory Procedures for Security Screening Decisions and Notifications

F.1 Effective date

F.1.1 These procedures take effect on January 6, 2025.

F.2 Procedures

F.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.1.3 and 4.6.1 of the *Directive on Security Screening*.

F.2.2 Mandatory procedures are as follows:

Decision to grant

F.2.2.1 Consider a decision to grant when the collective evaluation of the security screening results of an individual indicates:

a. There is no credible evidence that casts doubt on the reliability of an individual and, as applicable, their loyalty to Canada; and
b. Adverse information that is uncovered during security screening has been addressed; and

F.2.2.2 Render a decision to grant a security status or clearance at the time the security screening is processed;

Notification of a decision to grant

F.2.2.3 Notify the individual of the decision to grant a security status or clearance through a security briefing;

Decision to grant with conditions

F.2.2.4 Do not grant with conditions as a substitute to security screen individuals at the level required by the position;

F.2.2.5 Consider a decision to grant with conditions only when:

a. The conditions are deemed sufficient to mitigate the security risk of granting; and
b. There is a demonstrated need to engage the individual;

F.2.2.6 Impose conditions that formally detail restrictions attached to the granting of a security status or clearance, including:

F.2.2.6.1 Limits on the access to information and assets, including IT systems and facilities that are necessary to perform the assigned duties;

F.2.2.6.2 Where one or more of the following conditions applies:

a. Do not grant access to classified information from a foreign government without the written consent of that foreign government, subject to the provisions of any information-sharing agreements;
b. Do not grant access to classified information from other departments without consultation with those departments; or
c. The security status or clearance granted to the individual is not transferable to any other duty or

position in the department or to any other department;

F.2.2.6.3 As required:

F.2.2.6.3.1 Supplemental monitoring and reporting requirements to provide added assurance of the ongoing reliability or loyalty of the individual to Canada;

F.2.2.6.3.2 Limit the access of the individual to information and assets, including IT systems and facilities, to during designated working hours only; or

F.2.2.6.3.3 Setting other reasonable conditions that are necessary to effectively manage departmental or Government of Canada security risks; and

F.2.2.7 Reassess security conditions annually, at a minimum;

Notification of a decision to grant with conditions

F.2.2.8 Notify the individual of the decision to grant a security status or clearance with conditions through a security briefing, including the nature of the conditions;

F.2.2.9 Obtain acknowledgement from the individual of their security responsibilities, including the nature of the conditions; and

F.2.2.10 Retain a record of the decision and acknowledgement in their security screening file;

Decision to suspend pending an investigation

F.2.2.11 Consider a decision to suspend a security status or clearance where:

a. An investigation is pending;
b. Information suggests that the continued presence of the individual may reasonably pose a security risk to others, the department or the Government of Canada; and
    i. Alternate work arrangements are insufficient to address the security risk; or
    ii. The continued presence of an individual could undermine or impede the investigation;

F.2.2.12 Prior to rendering a decision to suspend a security status or clearance:

F.2.2.12.1 For an employee:

F.2.2.12.1.1 Consult with human resources management to ensure that the employer's labour relations obligations are considered and addressed; and

F.2.2.12.2 For a contractor or other individual:

F.2.2.12.2.1 Inform the contracting authority before informing the contractor;

Notification of a decision to suspend

F.2.2.13 Inform the individual in writing of the action to be taken, including the following:
a. The decision to suspend the security status or clearance pending an investigation;
b. The reasons the security status or clearance is being suspended;
c. Any circumstances or contributing factors that were taken into consideration in reaching this

decision;

d. The manner and time frame in which the suspension will be administered; and
e. The manner in which the individual may exercise the opportunity to respond to or challenge the action;

Decision to reinstate following a suspension

F.2.2.14 If a security status or clearance has been suspended for cause:

F.2.2.14.1 During the course of an investigation, consider the possibility of reinstatement:

a. When new facts or circumstances are identified; and
b. Within a reasonable period of time and periodically throughout the suspension;

F.2.2.14.2 Render a decision to reinstate or revoke based on:

a. Findings and recommendations from the investigation; and
b. The updated risk to the department or Government of Canada;

Notification of a decision to reinstate following a suspension

F.2.2.15 Notify the employee of the decision to reinstate a security status or clearance, through a security briefing;

Decision to deny

F.2.2.16 Consider a decision to deny when there is credible evidence that casts doubt as to an individual's:

a. Reliability and, as applicable, loyalty to Canada;

b. Ability to be trusted to safeguard sensitive information and assets, including IT systems and facilities;

F.2.2.17 Inform the deputy head of a decision to deny a security clearance within five days after the decision is made;

Decision to revoke

F.2.2.18 Consider a decision to revoke:

F.2.2.18.1 Following an update, upgrade or a review for cause of the security status or clearance previously granted to an individual;

F.2.2.18.2 When there is credible evidence that casts doubt as to an individual's:

a. Reliability and, as applicable, loyalty to Canada; and
b. Ability to be trusted to safeguard sensitive information and assets, including IT systems and facilities;

F.2.2.19 Prior to rendering a decision to revoke:

F.2.2.19.1 Consider the availability and feasibility of alternative options, including downgrading the status or clearance of an individual;

F.2.2.19.2 For an employee:

F.2.2.19.2.1 Consult with human resources management to ensure that the employer's labour relations obligations are considered and addressed;

F.2.2.19.3 For a contractor or other individual:

F.2.2.19.3.1 Inform the contracting authority before informing the contractor; and

F.2.2.19.4 Consult the deputy head in the event of a dispute as to the appropriate action to be taken;

F.2.2.20 Following a decision to revoke:

F.2.2.20.1 Prior to informing the individual, ensure that measures are taken to prevent the individual from accessing sensitive information and assets, including IT systems and facilities;

F.2.2.20.2 Inform the deputy head of a decision to revoke a security clearance within five days after the decision is made;

F.2.2.20.3 For a contractor, inform the contracting authority before the contractor; and

F.2.2.20.4 Notify CSIS via form CSIS 4160 Notification of Change in Security Clearance;

Notification of a decision to deny or revoke

F.2.2.21 Notify the individual of a decision to deny or revoke their security status or clearance:

F.2.2.21.1 Within 10 days after the decision is made;

F.2.2.21.2 In writing from the chief security officer or the deputy head;

F.2.2.21.3 Include the reasons for the decision and the information on which the decision is based:

F.2.2.21.3.1 Exclude information that cannot be disclosed:

a. Under the *Privacy Act*;

b. For reasons of national security; or
c. Under other federal legislation;

F.2.2.21.4 Inform the individual of their rights of review or redress.

F.2.2.22 Following notification of the individual, inform CSIS of the decision to deny or revoke a security clearance.

Appendix G: Mandatory Procedures for Granting, Ongoing Maintenance and Assurance of the Security Screening of an Individual

G.1 Effective date

G.1.1 These procedures take effect on January 6, 2025.

G.1.2 These procedures replace the Standard on Security Screening: Appendix F – Aftercare dated October 20, 2014.

G.2 Procedures

G.2.1 These procedures provide details on the requirements set out in subsections 4.1.1 and 4.6.1 of the *Directive on Security Screening*.

G.2.2 The chief security officer and those with subordinate responsibilities must apply the mandatory procedures below as follows:

Security briefings

G.2.2.1 The security briefing must:

G.2.2.1.1 Involve the manager of the individual or security officials;

G.2.2.1.2 Inform the individual of their responsibilities under the *Policy on Government Security*, including at a minimum:

a. Access permissions attached to their screening level;
b. The security expectations related to their position, contract or other arrangement; and
c. Shared security responsibilities within the organization;

G.2.2.1.3 Be completed before an individual is provided access to sensitive information and assets, including IT systems and facilities;

G.2.2.1.4 Be conducted in these circumstances:

a. Following a decision to grant or grant with conditions;
b. Whenever a change occurs in the security screening level of the individual;
c. As required based on the update cycle as defined in at Annex G2 or Annex G3; and
d. As determined by the department based on its security risk environment;

G.2.2.1.5 Provide an opportunity for the individual to ask questions;

G.2.2.1.6 Include the signing of the Security Screening Certificate and Briefing Form by the individual; and

G.2.2.1.6.1 Be retained in the security screening file of the individual;

G.2.2.2 Inform CSIS when a security clearance is granted, via form CSIS 4195 Notification of Security Clearance;

Security awareness

G.2.2.3 Conduct security awareness, in accordance with Appendix H: Mandatory Procedures for Security Awareness and Training Control of the *Directive on Security Management*, at minimum, as an outcome of the granting and updating phases of the security screening life cycle; and

G.2.2.3.1 Inform individuals of the requirement to report changes in personal circumstances, including at minimum the following:

a. Change in criminal record status;
b. Involvement with law enforcement;
c. Association with criminals; or
d. A significant change in financial situation;

G.2.2.3.2 Inform individuals who work in security or intelligence organizations of the requirements to report additional changes in their personal or legal status, including a change in marital status; and

G.2.2.3.3 Inform managers how to report and to whom they are to report observed changes in behaviour of individuals for whom they are responsible;

Recurring activities

G.2.2.4 Review the security screening requirements of positions when new programs or activities are established or substantially modified and, at minimum, every five years; and:

G.2.2.4.1 Inform security screening service providers of any changes in requirements;

G.2.2.5 Conduct security screening activities for individual security screening files that meet the minimum frequencies, as prescribed in Annex G1;

Updates

G.2.2.6 Update the individual's security screening prior to the end of their validity period, in addition to the conduct of recurring activities;

G.2.2.7 Re-examine the reliability or loyalty of an individual since the individual was last granted a security status or clearance:

G.2.2.7.1 Conduct the update process consistent with:

G.2.2.7.1.1 Security Screening update cycles and the activities identified in Annex G2; or

G.2.2.7.1.2 Site Access screening update cycles and the activities identified in Annex G3;

G.2.2.7.2 Evaluate whether changes in personal circumstances pose a security risk;

G.2.2.7.3 Determine the continued eligibility of an individual to hold a security status or clearance, based on the collective evaluation of security screening activities; and

G.2.2.7.4 Provide a security briefing to inform the individual of their security responsibilities consistent with subsections G.2.2.1 and G.2.2.3;

G.2.2.8 When an individual does not provide consent, withdraws consent or does not provide the required information,

proceed in accordance with subsection B.2.2.5.2 of Appendix B: Mandatory Procedures for the Management of Personal Information for the Purpose of Security Screening;

G.2.2.9 Repeat any security screening activity where:

G.2.2.9.1 Required by the update cycle; or

G.2.2.9.2 There is reason to believe:

a. The activities were conducted improperly; or
b. There is no documentation on the file of the initial conduct of the screening activities;

Upgrades

G.2.2.10 When upgrading a valid security status or clearance to a higher level:

G.2.2.10.1 Conduct additional security screening activities and years of background information required for the new level in accordance with Annex A1 of Appendix A: Standard on Security Screening Model and Position Analysis;

G.2.2.10.2 Determine the eligibility of an individual to hold the new security status or clearance, based on the collective results of all security screening activities; and

G.2.2.10.3 Provide a security briefing to inform the individual of their security responsibilities consistent with subsections G.2.2.1 and G.2.2.3

G.2.2.11 Where an individual does not provide consent, withdraws consent or does not provide the required information, proceed in accordance with subsection B.2.2.5.1 of Appendix

B: Mandatory Procedures for the Management of Personal Information for the Purpose of Security Screening;

Downgrades

G.2.2.12 When downgrading a valid status or clearance to a lower level:

G.2.2.12.1 Provide a security briefing to inform the individual of their security responsibilities consistent with subsections G.2.2.1 and G.2.2.3;

G.2.2.12.1.1 Which includes informing individuals and managers that the individual may no longer access higher levels of sensitive information and assets, including IT systems and facilities;

Security debriefing

G.2.2.13 The security debriefing must:

G.2.2.13.1 Be provided to individuals, prior to the end of employment or engagement with the department;

G.2.2.13.2 Advise individuals of their continued responsibilities to maintain the confidentiality of the sensitive information to which they had access; and

G.2.2.13.3 Use the Security Screening Certificate and Briefing Form to record:

a. Completion of the debriefing; or
b. Where it is impossible to debrief the individual;

G.2.2.13.3.1 Be retained in the security screening file of the individual in accordance with

subsection B.2.2.18 of Appendix B: Mandatory Procedures for the Management of Personal Information for the Purpose of Security Screening.

Annex G1: Minimum Frequency for the Recurring Update of Security Screening Activities

Security screening activities	Minimum frequency	Security screening activities	Minimum frequency
Reliability status • Nil	Not applicable	**Enhanced Reliability status** • Financial inquiry • Criminal record check • Internet inquiry	5 years
Secret clearance • Financial inquiry • Criminal record check	5 years	**Enhanced Secret clearance** • Financial inquiry • Criminal record check • Internet inquiry	5 years
Top Secret clearance • Financial inquiry • Criminal record check • Internet inquiry	3 years	**Enhanced Top Secret clearance** • Financial inquiry • Criminal record check • Internet inquiry	1 year

Annex G2: Security Screening Activities and Associated Minimum Update Requirements

Security screening activities	Update requirement	Security screening activities	Update requirement
Reliability status • Updated application form covering period since last update • Financial inquiry • Criminal record check	10 years	**Enhanced Reliability status:** All activities for Reliability status plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview	10 years
Secret clearance All activities for Reliability status plus: • CSIS security assessment	10 years	**Enhanced Secret clearance** All activities for Secret clearance plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview	10 years

Top Secret clearance All activities for Secret clearance plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview • Foreign travel, foreign assets, character references, education, military service	5 years	**Enhanced Top Secret clearance** All activities for Top Secret clearance plus: • Polygraph examination	5 years

Annex G3: Site Access Screening Activities and Associated Update Requirements

Site Access screening activities	Update requirement
Site Access status • Updated application form covering period since last update • Criminal record check	10 years: May be updated more frequently when employment, engagement, assignment, contract or arrangement has lapsed for 12 months or more
Site Access clearance All activities for Site Access status plus: • CSIS security assessment	10 years: May be updated more frequently when employment, engagement, assignment, contract or arrangement has lapsed for 12 months or more

Additional activities May be used in accordance with subsection A.2.2.10, “Position analysis for non-employees.” All activities for Site Access clearance plus: • Internet inquiry • Law enforcement records check • Security questionnaire or security interview • Polygraph examination	10 years: May be updated more frequently when employment, engagement, assignment, contract or arrangement has lapsed for 12 months or more

Appendix H: Mandatory Procedures on Informing Individuals of their Rights of Review and Redress

H.1 Effective date

H.1.1 These procedures take effect on January 6, 2025.

H.2 Procedures

H.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.1.4, 4.2.2.5 and 4.6.1 of the *Directive on Security Screening*.

H.2.2 Mandatory procedures are as follows:

Recourse notification requirements

H.2.2.1 In the preparation of information for the individual, identify the appropriate review and redress mechanisms in consultation with:

a. Human resources management;
b. Departmental legal services; and

c. The Centre for Labour and Employment Law, as required.

H.2.2.2 Inform the individual in writing of their rights of review and redress upon denial, revocation or suspension of a security status or clearance:

H.2.2.2.1 Within 10 business days of the decision being made;

H.2.2.2.2 Identify the appropriate review and redress mechanisms available to the individual; and

H.2.2.2.3 Document and retain evidence of communication of this information with the individual.

Appendix I: Mandatory Procedures for Chief Security Officers to Manage Temporary Access to Sensitive Information or Assets

I.1 Effective date

I.1.1 These procedures take effect on January 6, 2025.

I.2 Procedures

I.2.1 These procedures provide details on the requirements set out in subsections 4.1.1.2 and 4.6.1 of the *Directive on Security Screening*.

I.2.2 Mandatory procedures for chief security officers are as follows:

Decision to provide temporary access to sensitive information or assets

I.2.2.1 Do not consider a decision to provide temporary access when it is expected that access will be required for longer than four months;

I.2.2.2 Do not consider a decision to provide temporary access as a substitute to security screen individuals at the level required by the position;

I.2.2.3 Consider a decision to provide the individual with temporary access to sensitive information and assets, including IT systems or facilities:

I.2.2.3.1 Where there is an operational requirement for this individual that cannot be performed by another with a valid security screening at the required level; and

I.2.2.3.2 Where a risk assessment demonstrates that the need to provide the individual with temporary access outweighs the risk associated with providing the individual access

I.2.2.4 Impose restrictions that detail limits to accessing sensitive information and assets, including IT systems or facilities to which the temporary access provision includes;

Notification of a decision to provide temporary access

I.2.2.5 Notify the individual of the decision to provide temporary access to sensitive information and assets, including IT systems and facilities through a security briefing, including:

I.2.2.5.1 The duration of the access; and

I.2.2.5.2 The provisions of the access;

I.2.2.6 For the agreement of temporary access:

I.2.2.6.1 Obtain the signature of the individual receiving access;

I.2.2.6.2 Obtain the signature of the custodian of the information to be accessed;

I.2.2.6.3 Sign the agreement; and

I.2.2.6.4 Include the agreement in the security screening file of the individual;

Notification of a decision to remove temporary access

I.2.2.7 Debrief the individual following the removal of temporary access, including:

I.2.2.7.1 Advise the individual of their continued responsibilities to maintain the confidentiality of the sensitive information to which they had access;

I.2.2.7.2 Include a copy of the signed agreement in the security screening file of the individual; and

I.2.2.7.3 Retain evidence of the debriefing in the security screening file of the individual;

Managing temporary access of the individual

I.2.2.8 When temporary access is granted:

I.2.2.8.1 Prevent the individual from accessing:

a. Compartmented information;
b. Enhanced Top Secret information;
c. Protected C information
d. Information for which access is restricted in accordance with international agreements or special caveats;
e. Cabinet documents as defined within the Government of Canada, the Privy

Council Office or the Policy on the Security of Cabinet Confidences;

f. Sensitive information from other governments and levels of government; and
g. Sensitive information, assets, IT systems and facilities from other departments without their documented approval

I.2.2.8.2 Maintain positive control of access to sensitive information and assets, including IT systems and facilities to which the temporary access provision includes.

Date modified: 2025-01-07