CIHR IRSC

ITAMS

Canadian Institutes of Health Research | Instituts de recherche en santé du Canada

Personnel Security Screening Policy

Table of contents

1. Effective Date

1.1. This policy takes effect on February 9th, 2011.

1.2. It replaces *2005 CIHR Security Screening Policy*.

2. Application

2.1. This policy applies to:

- all individuals who will have access to CIHR's information and assets; and
- all employees, Institute staff, consultants, contractors, students, volunteers or agents of these organizations under the control of CIHR. For the purposes of this policy, they will collectively be referred to as "Personnel".

3. Context

The Government of Canada's Policy on Government Security requires CIHR to ensure that all individuals who will have access to government information and assets are security screened at the appropriate level before the commencement of their duties and are treated in a fair and unbiased manner.[1] This policy describes how CIHR will manage Personnel Security in accordance with the Policy on Government Security.

Security begins by establishing trust in interactions between government and Canadians and within government. Within government, there is a need to ensure that those having access to government information, assets and services are trustworthy, reliable and loyal. CIHR's Personnel Security Program has been established to support these requirements.

The Personnel Security Program limits access to information and assets to those individuals with a need to know. It ensures that an individual is appropriately screened based on the information and access required for the performance of her or his job. Effective Personnel Security management enables CIHR:

- To ensure that individuals with access to government information/assets and/or privileged access to critical systems are reliable and trustworthy;
- To ensure the individual's loyalty to Canada in order to protect itself from foreign intelligence gathering and terrorism; and
- To prevent malicious activity and unauthorized disclosure of classified and protected information or damage affected on critical systems by a disaffected individual in a position of trust.

4. Definitions

For definitions of terms used in this policy, refer to Appendix A –Glossary

[1] Policy on Government Security, Section 6.1.5

5. Policy Statement

5.1. OBJECTIVE

The objective of this policy is to ensure that CIHR provides the appropriate access to Government of Canada (GoC) information and assets to Personnel who have been deemed trustworthy and loyal in accordance with the GoC's Policy on Government Security.

5.2. EXPECTED RESULTS

- Compliance with the Policy on Government Security (PGS);
- Personnel understand their responsibilities regarding the security of Government information and assets;
- Information, assets and services are safeguarded from compromise and employees are protected against workplace violence;
- Interoperability and information exchange with other Government of Canada Personnel Security Departments & Agencies; and
- Mechanisms and resources are in place to ensure effective and efficient management of Personnel Security at CIHR.

6. Requirements

To deliver its programs and services effectively, CIHR's Personnel Security Program must:

- Determine the security level for each position. To do so, each role profile must describe what access to any protected or classified information / assets and/or critical systems are required to perform job duties. For generic role profiles, any additional access to protected or classified information required to perform job duties must be identified at the position level. Examples of classified information are:
  - Cabinet documents, including Memoranda to Cabinet (Secret)
  - Treasury Board Secretariat (TBS) submissions (Secret)
- Ensure that all individuals who require access to Classified/Protected information or/and assets or/and privileged access to critical systems, have been granted the required Security level **prior** to the start of any assignment, appointment or secondment.
  - Reliability status is required if access to Protected (A, B or C) information is a requirement of the work duties. A Reliability Status or a security clearance is a condition of employment at CIHR.
  - A Secret security clearance is required if access to Classified information is a requirement of the work duties. It is also required when privileged access to critical systems is needed to perform work duties.

7. Roles and Responsibilities

7.1. PRESIDENT

The President of CIHR is responsible for effectively managing security activities within CIHR and contributing to effective government-wide security management. The President is responsible for:

- Ensuring CIHR's compliance to the PGS and other related policy instruments and legislation;
- Approving CIHR's Security Plan and establishing a security program for the coordination and management of overall security activities, including Personnel Security;
- Appointing a Departmental Security Officer to manage the departmental security program;
- Ensuring that managers at all levels integrate Personnel Security requirements into plans, programs, activities and services;
- Denying or revoking a Security Clearance in the case of just cause; and
- Ensuring that when significant issues arise regarding policy compliance, allegations of misconduct, suspected criminal activity, security incidents, or workplace violence, they are investigated, acted on and reported to the appropriate authorities.

7.2. DEPARTMENTAL SECURITY OFFICER (DSO)

The Departmental Security Officer (DSO) is responsible for the management of CIHR's Security Program and has the following responsibilities with regards to Personnel Security:

- Developing, implementing, monitoring and maintaining a departmental security plan which incorporates Personnel Security
- Ensuring a coordinated approach to all aspects of CIHR Security: Personnel Security, IT, Contract and Physical Security.
- Ensuring that accountabilities, delegations, reporting relationships, and roles and responsibilities of CIHR employees with security responsibilities are defined, documented and communicated to relevant persons
- Authorizing exceptions to appointments to positions without the appropriate security clearance.
- Giving advice and making recommendations to the President in cases of denial or revocation of a Security Clearance, and
- Where just cause:
  - Denying, revoking or suspending a Reliability Status and inform the manager or Scientific Director.
  - Suspending a Security Clearance and inform the manager or Scientific Director.

7.3. SECURITY OFFICER

The Security Officer is responsible for the coordination of all functions related to the technical and operational aspects of Personnel Security, specifically:

- Maintaining a functional or direct reporting relationship with the DSO to ensure departmental security activities are coordinated and integrated;
- Selecting, implementing and maintaining security controls related to the Personnel Security;

- Determining the security requirements of each position based on the sensitivity of the information, assets and privileged access to critical systems to which the incumbent has access;
- Advising managers and/or Human Resources (HR) of the status of the security assessment;
- Processing requests for security screenings, including conducting name checks, criminal records (fingerprints if required), credit checks and security clearances;
- Advising HR in writing of the candidate's security screening results;
- Ensuring that all employees receive an official briefing and sign the Security Screening Certificate and Briefing Form;
- Maintaining employee security files;
- Ensuring that Reliability Status and Security Clearances are updated before they expire, in accordance with the Security requirements of the position. The Security Officer will update:
  - a Reliability Status : every 10 years
  - a Secret Level: every 10 years
  - a Top Secret: every 5 years
- Update the Reliability Status and/or Security clearance in these following situations:
  - Notification of a criminal offence
  - Change of Circumstances (e.g.: marriage, common in law, etc…)
  - Failure to comply with requirements
  - Re-assessment
  - Granting of a pardon.

7.4. HUMAN RESOURCES

The HR units are responsible for:

- Verifying the following information for the new employees:
  - Personal data (i.e. date of birth, address)
  - Education / professional qualifications
  - Employment history
  - Personal Character
- Initiating the Security Screening process; and
- Ensuring that no employee is hired without being screened and granted his or her required Security Level by the Security Section.

7.5. SCIENTIFIC DIRECTORS

Scientific Directors are responsible for:

- Identifying the sensitivity of the information, assets and privileged access to critical systems for which each external position having access to CIHR information and / or assets.
- Verifying the following information for the Institute staff:
  - Personal data (i.e. date of birth, address.)
  - Education / professional qualifications
  - Employment history
  - Personal Character
- Ensuring that Institute staff has been granted the appropriate Security level prior to the commencement of their duties.

7.6. CIHR MANAGERS

Managers are responsible for ensuring an appropriate level of security for their programs and services. In designing programs and services, managers will work with departmental security specialists to effectively manage risk. Managers will be supported and assisted by the Security officer in order to fulfill the following responsibilities:

- Ensuring that security requirements are integrated into business planning, programs, services and other management activities;
- Ensuring employees apply effective security practices;
- Identifying the sensitivity of the information, assets and privileged access to critical systems for each position of their unit and inform CIHR Security Section to obtain the proper Security requirement for the position;
- Ensuring that no employee is hired without being screened and granted his or her required Security Level by the Security Section; and
- When contracts are required, identifying any security requirements and ensuring that no temporary help, contractor or consultant is hired without being screened and have been granted the appropriate security level as required in the contract or agreement.

7.7. EMPLOYEES

Employees are responsible for:

- Safeguarding information and assets under their control whether working on CIHR premises or off-site;
- Applying security controls related to their area of responsibility to ensure that security requirements are part of their day-to-day processes, practices and program delivery;
- Reporting security incidents through the appropriate channels; and
- Informing the DSO of any issues affecting their status or clearance:
  - Arrest or Criminal conviction;
  - Bankruptcy;
  - Single/cohabitating/marriage/divorce;
  - If approached by a criminal, a representative of a foreign government, a fringe interest group or a foreign national who is seeking information about CIHR or the activities of CIHR, which would compromise the national interest, or the integrity of the Agency.

8. Consequences

The President is responsible for investigating and responding to issues of non-compliance with this policy and to take remedial action. Consequences for non-compliance with this policy can include:

- Poor performance ratings for CIHR on section 19 of MAF (Effective Management of Security and Business Continuity);
- External audit by the Auditor General of Canada, and/or
- Investigation by the Privacy Commissioner of Canada.

9. References

Legislation relevant to this policy includes the following:

- Policy on Government Security
- Staffing Policy
- Directive on Identity Management
- Directive on departmental Security Management
- Personnel Security Standard
- Operational Security Standard: Management of Information Technology Security (MITS)

10. Enquiries

Please direct enquiries about this policy to CIHR's DSO, Senior Security Advisor or Personnel Security Officer.

Security Program
Information, Management, and Administration Management Services (ITAMS)
Canadian Institutes of Health Research
Ottawa, Ontario, K1A 0W9

Email: Security@cihr-irsc.gc.ca.
Telephone: 613-954-7216 / 613-948-4636 / 613-954-1942
Fax: 613-954-1800

Appendix A: Glossary

Classified Information: Information related to the national interest that may qualify for an exemption or exclusion under the Access to Information Act or Privacy Act, and the compromise of which would reasonably be expected to cause injury to the national interest.

The levels of classification are:

- **Confidential:** applies when compromise could reasonably be expected to cause injury to the national interest**.**
- **Secret:** applies to information that; if compromised, could reasonably be expected to cause serious injury to the national interest; and
- **Top Secret:** applies to the very limited amount of information that, if compromised, could reasonably be expected to cause exceptionally grave injury to the national interest

Critical Services: A service whose compromise in terms of availability or integrity would result in a high degree of injury to the health, safety, security or economic well-being of Canadians or to the effective functioning of the Government of Canada (GC).

Critical Systems: Systems required to perform critical services**.**

Protected Information: Information is "Protected" if its disclosure could harm interests other than the "national interest".

The three levels are:

- **Protected A (low-sensitive**): applies to information that, if compromised, could reasonably be expected to cause injury outside the national interest, for example, disclosure of exact salary figures.
- **Protected B (particularly sensitive):** applies to information that, if compromised, could reasonably be expected to cause serious injury outside the national interest, for example, loss of reputation or competitive advantage
- **Protected C (extremely sensitive):** applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the national interest, for example, loss of life.

For Cause: A determination that there is sufficient reason to review revoke, suspend or downgrade a reliability status, a security clearance or a site access.

Foreign National: A person who is not a Canadian citizen or a permanent resident,

Interoperability: The ability of federal government departments to operate synergistically through consistent security and identity management practices.

National interest: The security and the social, political and economic stability of Canada.

Need-to-know: The need for someone to access and know information in order to perform his or her duties

Reliability Status: Indicates the successful completion of reliability checks; allows regular access to government assets and with a need to know to PROTECTED information.

Security Clearance: Indicates successful completion of a security assessment; with a need to know, allows access to classified information. There are three Security Clearance levels: Confidential, Secret and Top Secret.

Security program: A group of security-related resource inputs and activities that are managed to address a specific need or needs and to achieve intended results.