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

Directive on Identity Management

Published: Aug 01, 2011

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

Catalogue Number: BT39-8/2011E-PDF
ISBN: 978-0-660-09646-9

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 la gestion de l'identité

Directive on Identity Management

1. Effective date

1.1 This directive takes effect on July 1, 2009.

2. Application

2.1 This directive applies to:

- All departments within the meaning of Schedules I, I.1, II, IV and V of the *Financial Administration Act* (FAA),unless excluded by specific acts, regulations or Orders in Council; and
- Only those departments using the Public Works and Government Services Canada (PWGSC) pay system for responsibilities outlined in Section 6.2.

3. Context

3.1 Identity management is the determination by a government institution that the identity of an individual or institution with whom it is transacting is legitimate. Identity management is at the heart of the public administration and most government business processes. Once an identity is established, all subsequent government activities, ranging from safeguarding assets to delivering services, benefits and entitlements to responding to disasters and emergencies, rely upon this identity.

3.2 Different identity management practices across the Government of Canada (GC) and other jurisdictions may increase the risks of fraudulent use of identity documents, identity theft, improper granting of entitlements, benefits leakage, financial losses to individuals and governments, and invasion of privacy.

3.3 Without a coherent, consistent, standardized and interoperable approach for dealing with identity across the federal government and other jurisdictions, successful risk mitigation strategies are increasingly difficult to develop and deploy to manage challenges to national security, respect for privacy, program integrity and the delivery of citizen-centred services.

3.4 There is a clear need for a consistent approach to identity management that is supported by standards. This will ensure that security requirements are met and that services are developed, administered and delivered to the right clients. The development and implementation of this standardized approach will also permit a robust, scalable and flexible solution for the proper validation of identity information.

3.5 The responsibility for identity management must be fulfilled by departments when:

- Unique identification is required for the purposes of administering a federal program or service enabled by legislation;
- Disclosure of identity is required before receiving a government service, participating in a government program or becoming a member of a government organization.

3.6 This directive is issued pursuant to section 7 of the FAA.

3.7 This directive is to be read in conjunction with the *Foundation Framework for Treasury Board Policies*the *Policy on Government Security,* and the *Directive on Departmental Security Management*.

3.8 Additional mandatory requirements are set out in standards supporting the following subject areas:

- Information and identity assurance
- Personnel security screening
- Physical security
- Information technology security
- Emergency and business continuity management
- Security in contracting

4. Definitions

4.1 For definitions of terms used in this policy, refer to the Appendix–Definitions.

5. Directive statement

5.1 Objective

The objective of this directive is to ensure effective identity management practices by outlining requirements to support departments in the establishment, use and validation of identity.

5.2 Expected results

The expected results of this directive are:

5.2.1 Sound identity management practices that are aligned with an integrated government-wide approach to achieve effective identity management across the GC;

5.2.2 Identity management is an identifiable and integral element of departmental programs, activities and services;

5.2.3 Effective identity management ensures that departmental service and security requirements are met and that departments are dealing with the right client when delivering services; and

5.2.4 Departments ensure that their identity management activities allow for interoperability, when appropriate, which enables the exchange of individuals' identity information to meet the overall objectives of the GC and the respective mandates of departments.

6. Requirements

6.1 Managers at all levels with responsibilities for identity management will manage identity in a manner that mitigates risks to personal, organizational and national security, protects program integrity and enables well-managed, citizen-centred service delivery. Managers at all levels with this responsibility are responsible for:

6.1.1 Ensuring there is a rightful need for identification and the lawful authority to identify for a specific program or in support of law enforcement, national security or defence activities;

6.1.2 Articulating identity management risks (e.g., change of circumstances, errors, malfeasance), program impacts, required levels of assurance and risk mitigation options;

6.1.3 Selecting an appropriate set of identity data (such as personal attributes or identifiers) to sufficiently distinguish a unique identity to meet program needs, which is proportionate to identified risks and flexible enough to allow for alternative methods of identification, when appropriate; and

6.1.4 Implementing identity information sharing solutions that adhere to common GC standards.

6.2 Human resources managers are responsible for:

6.2.1 Ensuring each federal public service employee is assigned a unique personal record identifier (PRI) for the management of employee-related information and transactions; and

6.2.2 Ensuring each employee who must be identified to one or more remittance agencies outside the federal public service is assigned an individual agency number (IAN).

6.3 Monitoring and reporting requirements

Within departments

Managers at all levels with responsibilities for identity management are responsible for:

- Monitoring adherence to this directive within their department and ensuring that appropriate remedial action is taken to address any departmental deficiencies.

Government-wide

TBS is responsible for:

- Monitoring compliance with all aspects of this directive and the achievement of expected results in a variety of ways, including but not limited to assessments under the Management Accountability Framework (MAF), examination of Treasury Board submissions, departmental performance reports, annual reports and results of audits, evaluations and studies, and ongoing dialogue and committee work.

7. Consequences

7.1 The deputy head is responsible for investigating and responding to issues of non-compliance with this directive. The deputy head is also responsible for ensuring appropriate remedial actions are taken to address these issues.

7.2 If the secretary of the Treasury Board determines that a department may not have complied with any requirements of this directive, the secretary of the Treasury Board may request that the deputy head:

7.2.1 Conduct an audit or a review, the cost of which will be paid from the department's reference level, to assess whether requirements of this directive have been met; and/or

7.2.2 Take corrective actions and report back on the outcome.

8. References

Legislation relevant to this directive includes the following:

- *Access to Information Act*
- *Canadian Charter of Rights and Freedom*
- *Canadian Human Rights Act*
- *Criminal Code*
- *Criminal Records Act*
- *Financial Administration Act*
- *Library and Archives of Canada Act*
- *Privacy Act*

Treasury Board policies and directives relevant to this directive include the following:

- *Access to Information, Policy on*
- *Duty to Accommodate Persons with Disabilities in the Federal Public Service, Policy on the*
- *Evaluation, Policy on*
- *Government Security, Policy on*
- *Information and Technology, Policy Framework for*
- *Information Management, Policy on*
- *Management of Information Technology, Policy on*
- *Integrated Risk Management Framework*
- *Internal Audit, Policy on*
- *Internal Control, Policy on*
- *Management, Resources and Results Structure, Policy on*
- *Privacy Impact Assessment, Policy on*
- *Privacy Protection, Policy on*
- *Risk Management, Policy on*
- *Social Insurance Number, Directive on the*
- *The Values and Ethics Code for the Public Service*

9. Enquiries

Please direct enquiries about this directive to your department's headquarters. For interpretation of this directive, departmental headquarters should contact the Security and Identity Management Division.

Appendix–Definitions

Identity (*identité*)
: A reference or designation used to distinguish a unique and particular individual, organization or device.

Identity Management (*gestion de l'identité*)
: the set of principles, practices, policies, processes and procedures used to realize an organization's mandate and its objectives related to identity.

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

Remittance agency (*organisme de remise*)
: An organization outside the federal Public Service to which federal government institutions remit money on behalf of employees (e.g. charitable organizations, financial institutions and insurance administrators).