Directive on Identity Management

(Publié aussi en français sous le titre *Directive sur la gestion de l'identité*)

FINAL 22 May 2018

Contents

1. Effective date

1.1 This directive takes effect on [month] [day], [year]. (Note: date to be set three months after date of Treasury Board approval.)

1.2 This directive replaces the Directive on Identity Management, dated July 1, 2009.

2. Authorities

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

3. Objectives and expected results

3.1 The objectives of this directive are as follows:

3.1.1 To manage identity in a manner that mitigates risks to personnel and organizational and national security, while protecting program integrity and enabling trusted citizen-centred service delivery;

3.1.2 To manage identity consistently and collaboratively within the Government of Canada and with other jurisdictions and industry sectors, where identity of employees, organizations, devices and individuals is required; and

3.1.3 To manage credentials, authenticate users or accept trusted digital identities for the purposes of administering a program or delivering an internal or external service.

3.2 The expected results of this directive are as follows:

3.2.1 Interoperability, as appropriate, that supports participation in arrangements for trusted digital identity; and

3.2.2 Integration of a standardized identity assurance level framework into departmental programs, activities and services, consistent with a government-wide approach.

4. Requirements

4.1 Program and service delivery managers are responsible for the following:

4.1.1 Applying identity management requirements when any of the following conditions apply:

4.1.1.1 Unique identification is required to administer a federal program or service enabled by legislation;

4.1.1.2 Disclosure of identity is required before receiving a government service, participating in a government program, or becoming a member of a government organization; or

4.1.1.3 Accuracy and rightful use by individuals, organizations and devices of credential and identity information are required;

4.1.2 Ensuring that there is a need and the lawful authority for identification to support program administration, government-wide service delivery and, as required, to facilitate law enforcement, national security and defence-related activities;

4.1.3 Documenting identity management risks, program impacts, required levels of assurance, and risk mitigation options;

4.1.4 Selecting sufficient and appropriate identity attributes to distinguish a unique identity to meet program needs, in a manner that balances risk and flexibility and allows other methods of identification, where appropriate;

4.1.5 Evaluating identity and credential risks by assessing potential impacts to a program, activity, service or transaction;

4.1.6 Applying the required identity and credential assurance levels and related controls for achieving assurance level requirements, in accordance with Appendix A: Standard on Identity and Credential Assurance;

4.1.7 Accepting trusted digital identities provided through an approved trust framework as an equivalent alternative to in-person interactions, by assessing the following:

4.1.7.1 **Identity and program-specific information:** Selecting sufficient and appropriate attributes to uniquely identify individuals and personal information required to administer a program or deliver a service;

4.1.7.2 **Identity assurance and credential assurance**, as outlined in Appendix A: Standard on Identity and Credential Assurance;

4.1.7.3 **Identity registration:** Associating identity and personal information with a credential issued to an individual; and

4.1.7.4 **Notice and consent:** Ensuring that notices are clear, appropriate for the purpose, and accessible in order to obtain meaningful consent for the collection, use and disclosure of personal information;

4.1.8 Consulting the Chief Information Officer for the Government of Canada when establishing agreements or adopting trust frameworks; and

4.1.9 Using mandatory enterprise services for identity management, credential management and cyber authentication.

4.2 Heads of Human Resources are responsible for the following:

4.2.1 Assigning each federal public service employee a unique Personal Record Identifier (PRI) for the management of employee-related information and transactions; and

4.2.2 Assigning an additional unique identifier to each employee who must be identified to an organization external to the federal public service.

5. Roles of other government organizations

5.1 The roles of other government organizations in relation to this directive are described in section 5 of the Policy on Government Security.

6. Application

6.1 This directive applies to the organizations described in section 6 of the Policy on Government Security.

7. References

7.1 The references indicated in section 8 of the Policy on Government Security apply to this directive.

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 information about 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 any aspect of this directive.

Appendix A: Standard on Identity and Credential Assurance

A.1 Effective date

A.1.1 This standard takes effect on [month] [day], [year]. (Note: date to be set three months after date of Treasury Board approval.)

A.1.2 This standard replaces the Standard on Identity and Credential Assurance, dated February 1, 2013.

A.2 Standards

A.2.1 This standard provides details on the requirements set out in subsection 4.1.7 of the Directive on Identity Management.

A.2.2 Standards are as follows:

Identity assurance levels

A.2.2.1 **Level 4:** very high confidence required that an individual is who they claim to be;

A.2.2.2 **Level 3:** high confidence required that an individual is who they claim to be;

A.2.2.3 **Level 2:** some confidence required that an individual is who they claim to be; and

A.2.2.4 **Level 1:** little confidence required that an individual is who they claim to be.

Credential assurance levels

A.2.2.5 **Level 4:** very high confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised;

A.2.2.6 **Level 3:** high confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised;

A.2.2.7 **Level 2:** some confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised;

A.2.2.8 **Level 1:** little confidence required that an individual has maintained control over a credential that has been entrusted to them and that the credential has not been compromised.

A.2.3 The minimum requirements for establishing an identity assurance level are shown in Table 1.

A.2.3.1 Ensure that the minimum requirements are met, or appropriately manage the related risks.

Table 1: minimum requirements for establishing an identity assurance level

Requirement	Level 1	Level 2	Level 3	Level 4
Uniqueness	• Define identity information • Define context			
Evidence of identity	• No restriction on what is provided as evidence	• **One** instance of evidence of identity	• **Two** instances of evidence of identity (at least one must be foundational evidence of identity)	• Three instances of evidence of identity (at least one must be foundational evidence of identity)
Accuracy of identity information	• Acceptance of self-assertion of identity information by an individual	• Identity information acceptably matches assertion by an individual and evidence of identity, **and** • Confirmation that evidence of identity originates from an appropriate authority	• Identity information acceptably matches assertion by an individual and all instances of evidence of identity, **and** • Confirmation of the foundational evidence of identity, using an authoritative source, **and** • Confirmation that supporting evidence of identity originates from an appropriate authority, using an authoritative source Whenever any of the above cannot be applied: • inspection by trained examiner	
Linkage of identity information to individual	• No requirement	• No requirement	At least **one** of the following: • knowledge-based confirmation • biological or behavioural characteristic confirmation • trusted referee confirmation	At least **three** of the following: • knowledge-based confirmation • biological or behavioural characteristic confirmation • trusted referee confirmation

Requirement	Level 1	Level 2	Level 3	Level 4
			• physical possession confirmation	• physical possession confirmation

A.2.4 Assurance levels for trusted digital identities when participating in an approved trust framework are as follows:

A.2.4.1 **Level 4:** very high confidence required in the electronic representation of a person, used exclusively by that same person;

A.2.4.2 **Level 3:** high confidence required in the electronic representation of a person, used exclusively by that same person;

A.2.4.3 **Level 2:** some confidence required in the electronic representation of a person, used exclusively by that same person; and

A.2.4.4 **Level 1:** little confidence required in the electronic representation of a person, used exclusively by that same person.

Appendix B: Definitions

Definitions to be used in the interpretation of this directive can be found in Appendix B of the Policy on Government Security.