Government of Canada Gouvernement du Canada

Directive on Service and Digital

1. Effective date

1.1 This directive takes effect on April 1, 2020.

1.2 This directive replaces the following Treasury Board policy instruments:

1.2.1 Directive on Management of Information Technology, April 1, 2009

1.2.2. Directive on Information Management Roles and Responsibilities, October 8, 2007

1.2.3 Directive on Recordkeeping, June 1, 2009

1.2.4 Policy on Acceptable Network and Device Use, October 1, 2013, Appendices A, B, C, and D.

2. Authorities

2.1 This directive is issued pursuant to the same authority indicated in section 2 of the Policy on Service and Digital.

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

2.3 The Treasury Board has delegated to the Chief Information Officer of Canada the authority to issue, amend and rescind 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 Service and Digital apply to this directive.

3.2 The expected results indicated in section 3 of the Policy on Service and Digital apply to this directive.

4. Requirements

4.1 **Enterprise governance, planning and reporting**
Enterprise architecture review

4.1.1 The departmental Chief Information Officer (CIO) is responsible for:

4.1.1.1 Chairing a departmental architecture review board that is mandated to review and approve the architecture of all departmental digital initiatives and ensure their alignment with enterprise architectures.

4.1.1.2 Submitting to the Government of Canada enterprise architecture review board proposals concerned with the design, development, installation and implementation of digital initiatives:

4.1.1.2.1 Where the department is willing to invest a minimum of the following amounts to address the problem or take advantage of the opportunity:

4.1.1.2.1.1 $2.5 million dollars for departments that do not have an approved Organizational Project Management Capacity Class or that have an approved Organizational Project Management Capacity Class of 1 according to the *Directive on the Management of Projects and Programmes* ;

4.1.1.2.1.2 $5 million dollars for departments that have an approved Organizational Project Management Capacity Class of 2;

4.1.1.2.1.3 $10 million dollars for departments that have an approved Organizational Project Management Capacity Class of 3;

4.1.1.2.1.4 $15 million dollars for the Department of National Defence;

4.1.1.2.1.5 $25 million dollars for departments that have an approved Organizational Project Management Capacity Class of 4;

4.1.1.2.2 That involve emerging technologies;

4.1.1.2.3 That require an exception under this directive or other directives under the policy;

4.1.1.2.4 That are categorized at the protected B level or below using a deployment model other than public cloud for application hosting (including infrastructure), application deployment, or application development;

4.1.1.2.5 That include the extension or creation of custom support to prevent a technology from becoming unsupported where:

4.1.1.2.5.1 The proposal is an extension for a previous support contract where the migration project has been delayed (with justification);

4.1.1.2.5.2 The technology supports a mission-critical system where there is a high degree of injury risk should the system’s functions fail; or

4.1.1.2.5.3 The technology has been discontinued by the provider, and migration to a new technology would require adoption of a completely new solution; or

4.1.1.2.6 As directed by the CIO of Canada.

4.1.1.3 Ensuring that proposals submitted to the GC Enterprise Architecture Review Board have first been assessed by the departmental architecture review board where one has been established;

4.1.1.4 Ensuring that proposals to the GC Enterprise Architecture Review Board are submitted after review of concept cases for digital projects according to the “Mandatory Procedures for Concept Cases for Digital Projects” and before the development of a Treasury Board submission or departmental business case.

4.1.1.5 Ensuring that departmental initiatives submitted to the GC Enterprise Architecture Review Board align with the GC Enterprise Architecture Framework , the GC Standards on Application Programming Interfaces , and the Government of Canada Digital Standards . The Enterprise Architecture Framework is the criteria used by the GC Enterprise Architecture Review Board and departmental architecture review boards when reviewing digital initiatives to ensure their alignment with enterprise architectures across business, information, application, technology and security domains to support strategic outcomes;

Planning

4.1.1.6 Approving the IT and information or data component of all departmental strategies, plans, initiatives, projects, procurements and spending authority requests.

4.1.1.7 Producing the departmental IT expenditure report and on-going Application Portfolio Management update reports.

4.1.1.8 Ensuring that departmental IT investments, service development and improvement initiatives are informed by and integrated into departmental business planning.

Enterprise participation

4.1.1.9 Participating, as a service provider or as a service client, in the conception, planning, evolution and oversight of enterprise-wide IT services and solutions.

4.1.1.10 Advising the CIO of Canada about decisions, plans, strategies, directions, progress, risks and challenges related to initiatives that affect the provision or use of IT services in or across departments.

4.2 Client-centric service design and delivery

4.2.1 The designated official for service, in collaboration with other officials as necessary, is responsible for the following, in accordance with TBS direction and guidance:

Client-centric service

4.2.1.1 Ensuring that client feedback, including in-service client feedback, client satisfaction surveys and user experience testing, is collected and used to inform design, delivery and continuous improvement of services;

4.2.1.2 Ensuring that newly designed or redesigned online services provide real-time application status to clients;

Service inventory

4.2.1.3 Developing and annually updating a departmental service inventory;

4.2.1.4 Working with TBS to make the departmental service inventory available through the Government of Canada open government portal;

Service standards

4.2.1.5 Ensuring the development, management and regular review of service standards, related targets and performance information, for all services and all service delivery channels in use;

4.2.1.6 Ensuring the reporting of real-time performance information for service standards is available on the department’s web presence;

Service review

4.2.1.7 Ensuring that each service is regularly reviewed with clients, partners and stakeholders, in collaboration with the departmental CIO, as appropriate, at least once every five years to identify opportunities for improvement, including redesign for client-centricity, digital enablement, online availability and uptake, efficiency, partnership arrangements, and alternate approaches to service delivery, and alignment with the Government of Canada Digital Standards .

4.3 Open and strategic management of information and data

4.3.1 The departmental CIO, in collaboration with other departmental officials as necessary, is responsible for:

Strategic management of information

4.3.1.1 Establishing departmental information architecture in alignment with prescribed enterprise-wide standards.

4.3.1.2 Ensuring digital systems are the preferred means of creating, capturing and managing information.

4.3.1.3 Ensuring information and data are managed to enable data interoperability, reuse and sharing to the greatest extent possible within and with other departments across the government to avoid duplication and maximize utility, while respecting security and privacy requirements.

4.3.1.4 Ensuring departmental information is created in an accessible format, where appropriate, in accordance with TBS guidance.

4.3.1.5 Establishing and maintaining taxonomies or classification structures to manage, store, search, and retrieve information and data in all formats according to prescribed enterprise-wide standards.

4.3.1.6 Documenting life cycle management practices within the department that align with the nature or purpose of the information or data, and that address accountability, stewardship, performance measurement, reporting, and legal requirements.

4.3.1.7 Establishing, implementing and maintaining retention periods for all information and data, as appropriate, according to format.

4.3.1.8 Developing a documented disposition process and performing regular disposition activities for all information and data, as required.

Protection

4.3.1.9 Protecting information and data by documenting and mitigating risks, and by taking into consideration the business value of the information, legal and regulatory risks, access to information, security of information, and the protection of personal information.

Recordkeeping

4.3.1.10 Identifying information of business value, based on an analysis of the functions and activities carried out by a department to enable or support its legislated mandate.

4.3.1.11 Maximizing the removal of access restrictions on departmental information that has been identified as having archival value before the information is transferred to Library and Archives Canada as part of planned disposition activities.

4.3.1.12 Ensuring that an approved Government of Canada enterprise information management solution is used to document business activities, decisions and decision-making processes.

4.3.1.13 Identifying, establishing, implementing and maintaining designated corporate repositories in which information of business value is managed throughout its life cycle while respecting privacy and security requirements.

4.3.1.14 Ensuring that the quality of information is managed and preserved to satisfy the requirements and expectations of users to meet operational needs, responsibilities, and long-term retention requirements.

4.3.2 Managers are responsible for:

4.3.2.1 Informing employees of their duty to document their activities and decisions of business value.

4.3.3 Employees are responsible for:

4.3.3.1 Documenting their activities and decisions of business value.

4.4 Leveraging technology

4.4.1 The Chief Information Officer of Canada is responsible for:

4.4.1.1 Defining requirements and criteria of Appendix D: Standard on Information Technology User and Workpoint Profiles and Appendix E: Standard on Information Technology Provisions .

4.4.2 The Deputy Head of SSC is responsible for:

4.4.2.1 Providing services within their mandate respecting the provisions, limits and thresholds specified in Appendix D: Standard on Information Technology User and Workpoint Profiles and Appendix E: Standard on Information Technology Provisions ;

4.4.2.2 Providing departmental CIOs and the CIO of Canada with details on service offering, availability and their department's actual consumption, subject to data availability;

4.4.2.3 Releasing for publication on the Open Government portal enterprise-wide annual statistics on availability and actual consumption, subject to data availability; and

4.4.2.4 Providing to departments, subject to data availability, inventories of applications and associated software and versions.

4.4.3 The departmental CIO is responsible for:

Strategic IT management

4.4.3.1 Providing IT services that are responsive to departmental priorities and to the needs of program delivery and business.

4.4.3.2 Ensuring that decisions and actions regarding IT are guided by the CIO of Canada's enterprise-wide plan and prioritization of GC demand for IT services and assets.

4.4.3.3 Adopting, as applicable, enterprise solutions within their respective department.

4.4.3.4 Developing and maintaining departmental IT management practices and processes, as informed by ITIL (Information Technology Infrastructure Library) and COBIT (Control Objectives for Information and Related Technology), while prioritizing IT asset management, the IT service catalogue and IT service costing and pricing, as appropriate.

4.4.3.5 Developing, implementing and sustaining departmental strategies for producing or using appropriate enterprise IT services and solutions, based on the integrated service, information, IT and cyber security departmental plan.

4.4.3.6 Collaborating on digitally enabled business transformation with the business owner and other stakeholders.

4.4.3.7 Identifying emerging technologies that could potentially contribute to the strategic and business goals of the department and the GC.

4.4.3.8 Ensuring that IT services are designed and managed to support interoperability.

4.4.3.9 Collecting, maintaining, approving and updating annually the department’s inventory of employees and their assigned profiles per Appendix D: Standard on Information Technology Use and Appendix E: Standard on Information Technology Provisions ;

4.4.3.10 Complying with provisions, limits, configurations and thresholds as set out in Appendix E: Standard on Information Technology Provisions , Appendix F: Standard on Enterprise Information Technology Service Usage Restrictions , and Appendix G: Standard on Enterprise Information Technology Service Common Configurations ;

4.4.3.11 Identifying planned usage of IT services in the integrated service, information, data, IT and cyber security departmental plan using the Metrics for

Government of Canada Information Technology Consumption ;

4.4.3.12 Ensuring open source software is encouraged and where used, contributing to the communities whose work is being leveraged.

Information and data residency

4.4.3.13 Supporting the use of cloud services first by ensuring they are:

4.4.3.13.1 Identified and evaluated as a principal delivery option when initiating new departmental, enterprise, and community of interest cluster IT investments, initiatives, strategies and projects;

4.4.3.13.2 Adopted when they are the most effective option to meet business needs; and

4.4.3.13.3 Compliant with appropriate federal privacy and security legislation, policies and standards.

4.4.3.14 Ensuring computing facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission, be identified and evaluated as a principal delivery option for all sensitive electronic information and data under government control that has been categorized as Protected B, Protected C or is Classified.

Network and device use

4.4.3.15 Drafting notices to authorized network and device users to inform them of:

4.4.3.15.1 Expectations for acceptable and unacceptable use of GC electronic networks and devices, including a link to the *Policy on Service and Digital* and instructions to consult Appendix A: Examples of Acceptable Network and Device Use (Non-Exhaustive List) and Appendix B: Examples of Unacceptable Network and Device Use (Non-Exhaustive List) ;

4.4.3.15.2 Electronic network monitoring practices applied by their own department or by Shared Services Canada (SSC) according to Appendix C: Privacy and Monitoring of Network and Device Use ;

Alternative IT services

4.4.3.16 Ensuring compliance with procedures established for accessing alternatives to SSC service delivery mechanisms, as necessary.

At-risk technology management

4.4.3.17 Ensuring that technologies are current and that technologies that are unsupported are not used, according to Appendix H: Standard on At-Risk Information Technology .

Cyber security

4.4.4 The designated official for cyber security, in collaboration with the departmental CIO and Chief Security Officer as appropriate, is responsible for:

4.4.4.1 Ensuring that cyber security requirements and appropriate risk-based measures are applied continuously in an identify, protect, detect, respond, and recover approach to protect information systems and services, in accordance with the Directive on Security Management, Appendix B: Mandatory Procedures for Information Technology Security Control ;

4.4.4.2 Ensuring departmental plans, processes and procedures are in place for responding to cyber security events and reporting of incidents to the appropriate authorities and affected stakeholders, in accordance with the *Government of Canada Cyber Security Event Management Plan* .

4.4.4.3 Undertaking immediate action within the department as directed to assess impacts, including whether there has been a privacy breach, and implement mitigation measures in response to cyber security events.

4.4.4.4 Liaising with the access to information and privacy office in the department and the Office of the Privacy Commissioner when there has been a material privacy breach.

4.5 **Supporting workforce capacity and capability**

4.5.1 The departmental CIO is responsible for:

4.5.1.1 Providing functional leadership in the department on the development and sustainability of the IT and information communities through talent management and community development strategies.

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 Service and Digital.

6. Application

6.1 This directive applies to departments as defined in section 2 of the Financial Administration Act unless otherwise excluded by other acts, regulations or orders in council.

6.2 Requirements 4.4.2.1, 4.4.2.2, 4.4.2.3, 4.4.2.4, 4.4.3.9, 4.4.3.10 and 4.4.3.11 apply only to departments, as defined in section 2 of the *Financial Administration Act* , that receive their IT services from SSC as set out in Order-in-Council 2015-1071 . Other departments or separate agencies that are not subject to these provisions are encouraged to meet these requirements as good practice.

6.3 Requirement 4.4.3.14 applies only to the core public administration as defined in section 11.1 of the *Financial Administration Act* , unless otherwise excluded by specific acts, regulations or orders-in-council. Other departments or separate agencies that are not subject to these provisions are encouraged to meet these requirements as good practice.

6.4 Small departments and agencies:

6.4.1 For the purposes of this directive, small departments and agencies are defined as organizations that have reference levels including revenues credited to the vote of less than $300 million per year or that have been, for the purposes of this directive, designated as small departments or agencies by the President of the Treasury Board upon recommendation of the Secretary of the Treasury Board;

6.4.2 Organizations whose reference levels change so as to bring them above or below the $300 million threshold will not be redefined as large or small departments or agencies unless their reference levels remain above or below the threshold for three consecutive years, to allow for stability and transition, unless otherwise determined by the President of the Treasury Board upon the recommendation of the Secretary of the Treasury Board;

6.4.3 With regard to small departments and agencies, this directive applies as per subsection 6.1 with the exception of section 4.1.1.1.

6.5 Agents of Parliament

6.5.1 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
- 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

6.5.2 With regard to Agents of Parliament, the following subsections do not apply: 4.1.1.1, 4.1.1.2, 4.1.1.3, 4.1.1.4, 4.1.1.5, 4.1.1.10, 4.4.3.2 and 4.4.3.15.

7. References

7.1 The references in relation to this directive are described in section 8 of the Policy on Service and Digital.

8. Enquiries

8.1 For interpretation of any aspect of this directive, contact Treasury Board of Canada Secretariat Public Enquiries .

Appendix A: Examples of Acceptable Network and Device Use (non-exhaustive list)

Provides employees with examples of acceptable uses of government electronic networks and devices: Examples of Acceptable Network and Device Use (non-exhaustive list)

Appendix B: Examples of Unacceptable Network and Device Use (non-exhaustive list of examples)

Provides employees with examples of unacceptable uses of government electronic networks and devices: Examples of Unacceptable Network and Device Use (non-exhaustive list of examples)

Appendix C: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices

Provides direction for departments to notify users how their use of government networks and devices is monitored: Mandatory Procedures for Privacy and Monitoring of Network and Device Use Information Notices

Appendix D: Standard on Information Technology User and Workpoint Profiles

Provides direction for departments on specifications for user and workpoint profiles: Standard on Information Technology User and Workpoint Profiles

Appendix E: Standard on Information Technology Provisions

Provides direction for departments on specifications for the provision of information technology: Standard on Information Technology Provisions

Appendix F: Standard on Enterprise Information Technology Service Usage Restrictions

Provides direction for departments on provisions and limits and expected maximum levels of use for enterprise IT service components: Standard on Enterprise Information Technology Service Usage Restrictions

Appendix G: Standard on Enterprise Information Technology Service Common Configurations

Provides direction for departments on the management of IT components essential to enterprise IT services: Standard on Enterprise Information Technology Service Common Configurations

Appendix H: Standard on At-Risk Information Technology

Provides direction for departments on ensuring technologies deployed are current and risks and vulnerabilities are addressed: Standard on At-Risk Information Technology

Appendix I: Interim Standard on Enterprise Resource Planning Solutions

Interim Standard on Enterprise Resource Planning Solutions sets out the designated senior departmental official’s responsibilities related to investments in and upgrades to ERP systems

Appendix J: Standard on Systems that Manage Information and Data

Standard on Systems that Manage Information and Data

Appendix K: Data reference standards

Data reference standard on Canadian provinces and territories

Data reference standard on industry classification system

Data reference standard on codes for current and past official names of countries, territories and geographic areas recognized by the Government of Canada

Data reference standard on the business number

Appendix L: Standard for Managing Metadata

Standard for Managing Metadata

Date modified: 2024-01-10