Policy on Service and Digital

Note to reader

The Policy on Service and Digital and the Directive on Service and Digital took effect on April 1, 2020. They replace the:

- Policy Framework on Information and Technology;
- Policy on Management of Information Technology;
- Policy on Information Management;
- Policy on Service;
- Policy on Acceptable Network and Device Use;
- Directive on Management of Information Technology;
- Directive on Information Management Roles and Responsibilities; and,
- Directive on Recordkeeping.

1. Effective date

1.1 This policy takes effect on April 1, 2020.

1.2 This policy replaces the following Treasury Board policy instruments:

1.2.1 Policy Framework for Information and Technology, July 1, 2007

1.2.2 Policy on Management of Information Technology, July 1, 2007, updated April 1, 2018

1.2.3 Policy on Information Management, July 1, 2007, updated April 1, 2018

1.2.4 Policy on Service, October 1, 2014

1.2.5 Policy on Acceptable Network and Device Use, October 1, 2013

2. Authorities

2.1 This policy is issued pursuant to section 7 of the *Financial Administration Act* and section 31 of the *Public Service Employment Act*.

2.2 This policy must be read in conjunction with other requirements, including but not limited to, requirements in respect of privacy, official languages, and accessibility. Additional requirements in the policies set out in Section 8, must be applied in conjunction with this policy.

2.3 The Treasury Board has delegated to the President of the Treasury Board of Canada the authority to issue, amend, and rescind directives related to this policy.

2.4 The Treasury Board has delegated to the Chief Information Officer of Canada the authority to issue, amend, and rescind standards, mandatory procedures and other appendices, related to this policy.

3. Objectives and expected results

3.1 The objective of this policy is as follows:

3.1.1 Client service experience and government operations are improved through digital transformation approaches.

3.2 The expected government-wide results of this policy are as follows:

3.2.1 Integrated decision-making is supported by enterprise governance, planning and reporting;

3.2.2 Service delivery, business and program innovation are enabled by technology and data;

3.2.3 Service design and delivery is client-centric by design; and

3.2.4 Workforce capacity and capability development is supported.

4. Requirements

4.1 **Enterprise governance, planning and reporting**
Governance

4.1.1 The Secretary of the Treasury Board of Canada is responsible for:

4.1.1.1 Establishing and chairing a senior-level body that is responsible for providing advice and recommendations, in support of the Government of Canada's priorities and the Government of Canada Digital Standards, regarding:

4.1.1.1.1 Strategic direction for the management of external and internal enterprise services, information, data, information technology (IT) and cyber security; and

4.1.1.1.2 Prioritization of Government of Canada demand for IT shared services and assets.

4.1.2 The Chief Information Officer (CIO) of Canada is responsible for:

4.1.2.1 Providing advice to the Secretary of the Treasury Board of Canada and the President of the Treasury Board of Canada about:

4.1.2.1.1 Governing and managing enterprise-wide information, data, IT, cyber security, and service design and delivery;

4.1.2.1.2 Prioritizing Government of Canada demand for IT shared services and assets; and,

4.1.2.1.3 Using emerging technologies and the implications and opportunities of doing so for the Government of Canada.

4.1.2.2 Providing direction on the enterprise-wide transition to digital government, including:

regularly reviewing and updating the Government of Canada Digital Standards; managing information, data, IT, and cyber security; and, advising on enterprise-wide service design and delivery.

4.1.2.3 Prescribing expectations with regard to enterprise architecture.

4.1.2.4 Establishing and chairing an enterprise architecture review board that is mandated to define current and target architecture standards for the Government of Canada and review departmental proposals for alignment.

4.1.2.5 Establishing priorities for IT investments (including cyber security investments) that are enterprise-wide in nature or that require the support of Shared Services Canada (SSC).

Innovation and experimentation

4.1.2.6 Facilitating innovation and experimentation in service design and delivery, information, data, IT and cyber security.

Planning and reporting

4.1.2.7 Approving an annual, forward-looking three-year enterprise-wide plan that establishes the strategic direction for the integrated management of service, information, data, IT, and cyber security and ensuring the plan includes a progress report on how it was implemented in the previous year.

4.1.3 Deputy heads are responsible for the following:

Governance

4.1.3.1 Establishing governance to ensure the integrated management of service, information, data, IT, and cyber security within their department.

4.1.3.2 Designating a departmental CIO responsible for leading the departmental IT, information, and data management functions.

4.1.3.3 Designating an official responsible for leading the departmental service management function.

4.1.3.4 Designating an official responsible for leading the departmental cyber security management function.

4.1.3.5 Providing the departmental CIO and the official responsible for service with direct access to the deputy head.

4.1.3.6 Ensuring departmental participation in enterprise governance to support the development and implementation of enterprise-wide policy instruments and architecture.

Planning and reporting

4.1.3.7 Approving an annual forward-looking three-year departmental plan for the integrated management of service, information, data, IT, and cyber security, which aligns with the CIO of Canada's enterprise-wide integrated plan, is informed by subject-specific plans or strategies as appropriate, and includes a progress report on how it was implemented in the previous year.

Innovation and experimentation

4.1.3.8 Providing support for innovation and experimentation in service, information, data, IT and cyber security.

IT and information standards

4.1.3.9 Informing the Treasury Board of Canada Secretariat of activities related to this policy that involve the development of national or international IT, information, or data standards.

4.2 Client-centric service design and delivery

4.2.1 Deputy heads are responsible for:

4.2.1.1 Ensuring the development and delivery of client-centric service by design, including access, inclusion, accessibility, security, privacy, simplicity, and choice of official language.

4.2.1.2 Maximizing the online end-to-end availability of services and their ease of use to complement all service delivery channels.

4.2.1.3 Approving the department’s service inventory and annual updates.

4.2.1.4 Ensuring services have comprehensive and transparent client-centric standards, related targets, and performance information, for all service delivery channels in use, and this information is available on the department’s web presence.

4.2.1.5 Ensuring that services are reviewed to identify opportunities for improvement.

4.3 Open and strategic management of information

4.3.1 The CIO of Canada is responsible for:

Enterprise standards

4.3.1.1 Prescribing enterprise-wide information and data standards for quality, accessibility, and data interoperability, including common architecture taxonomies and classifications, quality requirements, and life cycle management direction.

4.3.2 Deputy heads are responsible for:

Strategic management

4.3.2.1 Ensuring that information and data are managed as a strategic asset to support government operations, service delivery, analysis and decision-making.

4.3.2.2 Ensuring that methodologies, mechanisms and tools are implemented to support information and data life cycle management.

4.3.2.3 Ensuring that departmental responsibilities and accountability structures are clearly defined for the management of information and data.

4.3.2.4 Ensuring that data are managed to reduce redundancy and enable interoperability.

Privacy and protection

4.3.2.5 Ensuring that, when managing personal information or data, including in the context of data interoperability, the privacy of individuals is protected according to the *Privacy Act* and any other relevant legislation, policy or agreement.

4.3.2.6 Ensuring that privacy is addressed in the context of any plan or strategy to manage departmental information or data.

4.3.2.7 Ensuring that sensitive information under the department’s control is protected according to the *Policy on Government Security* and any relevant legislation, policy or agreement.

Open information and open data

4.3.2.8 Maximizing the release of departmental information and data as an open resource, discoverable through the Government of Canada open government portal designated by the Treasury Board of Canada Secretariat, while respecting information security, privacy, and legal considerations.

4.3.2.9 Prioritizing departmental information and data to be added to the Government of Canada's open government portal, informed by public demand.

Recordkeeping

4.3.2.10 Ensuring that decisions and decision-making processes are documented to account for and support the continuity of departmental operations, permit the reconstruction of how policies and programs have evolved, support litigation readiness, and allow for independent evaluation, audit and review.

4.4 Leveraging technology

4.4.1 The CIO of Canada is responsible for:

Enterprise direction

4.4.1.1 Prescribing the use of specific IT business processes, technologies, applications and IT resource management approaches, including direction for their life cycle management as defined in the *Policy on the Planning and Management of Investments*.

4.4.1.2 Providing enterprise-wide advice for IT solution procurement that maximizes flexibility for the Government of Canada.

4.4.1.3 Providing direction and defining enterprise-wide requirements for Information and Communication Technologies (ICT) accessibility.

4.4.1.4 Supporting SSC procedures for assessing and accessing alternative provision of SSC services to support the authority of the Minister responsible for SSC.

4.4.1.5 Providing advice to the President of the Treasury Board to support the Treasury Board's review of the SSC Investment Plan to ensure that the plan is aligned with established strategic direction and enterprise-wide priorities and to assess progress.

Innovation and experimentation

4.4.1.6 Establishing guidance to support innovative practices and technologies, including open-source and open-standard applications, and agile application development.

4.4.1.7 Working with departments to review and endorse digital initiatives, projects and investments, and review results.

Cyber-security and identity

4.4.1.8 Defining cyber security requirements to ensure that Government of Canada and departmental information and data, applications, systems, and networks are secure, reliable and trusted.

4.4.1.9 Executing decisions on the management of cyber security risks on behalf of the Government of Canada and directing a deputy head to implement a specific response to cyber security events, including assessing whether there has been a privacy breach, implementing security controls, and ensuring that systems that put the Government of Canada at risk are disconnected or removed, when warranted.

4.4.1.10 Providing direction and defining enterprise-wide requirements for the management of identities, credentials, and access for the Government of Canada and departments.

4.4.2 Deputy heads are responsible for:

Strategic IT management

4.4.2.1 Ensuring departmental operations are digitally enabled.

4.4.2.2 Ensuring that, for newly procured or developed information, communication, and technology solutions and equipment, applicable requirements or standards regarding accessibility, official languages, protection of personal information, the environment, and security are addressed by design.

4.4.2.3 Using enterprise or shared IT solutions, assets, and services to avoid duplication, when available and appropriate.

Automated decision-making

4.4.2.4 Ensuring the responsible and ethical use of automated decision systems, in accordance with TBS direction and guidance, including:

4.4.2.4.1 Ensuring decisions produced using these systems are efficient, accountable, and unbiased; and,

4.4.2.4.2 Ensuring transparency and disclosure regarding use of the systems and ongoing assessment and management of risks.

Open access to digital tools

4.4.2.5 Providing authorized users of the departmental electronic network and of departmental devices with open access to the Internet, including Government of Canada and external Web 2.0 tools and services that enhance productivity, communication and open collaboration, in accordance with the Policy on Government Security, and limiting access only where necessary to manage security risks and address unacceptable uses.

Network and device use

4.4.2.6 Informing authorized users of departmental electronic networks and devices of:

4.4.2.6.1 Expectations for acceptable and unacceptable use of Government of Canada electronic networks and devices;

4.4.2.6.2 Monitoring practices being applied by their own department and by SSC; and

4.4.2.6.3 Consequences for unacceptable use of departmental electronic networks and devices.

Cyber security and identity

4.4.2.7 Clearly identifying and establishing departmental roles and responsibilities for reporting cyber security events and incidents, including events that result in a privacy breach, in accordance with the direction for the management of cyber security events from the CIO of Canada.

4.4.2.8 Managing departmental approaches for identity assurance and accepting trusted digital identities to support interoperability by using approved trust frameworks.

4.4.3 The deputy head of SSC is responsible for the following:

4.4.3.1 Managing tools to support the monitoring of departmental electronic networks and devices.

4.4.3.2 Providing reports as required about the use of Government of Canada electronic networks and devices to assist deputy heads in the identification and investigation of issues and in the implementation of corrective action in the event of unacceptable use.

4.5 **Supporting workforce capacity and capability**

4.5.1 The CIO of Canada is responsible for:

4.5.1.1 Providing enterprise-wide leadership on the development and sustainability of the information and IT functional community by using talent management and community development strategies.

4.5.1.2 Providing enterprise-wide leadership on knowledge standards for the information and IT community, including determining the acceptable combination of education, training and experience required for the Treasury Board Executive Group (EX) Qualification Standard.

4.5.2 Deputy heads are responsible for:

4.5.2.1 Ensuring departmental workforce awareness, capacity, and capability to meet departmental and enterprise service, information, data, IT, and cyber security requirements.

4.5.2.2 Supporting the CIO of Canada’s enterprise-wide talent management and community development initiatives.

4.5.2.3 Consulting with the CIO of Canada before appointing, deploying, or otherwise replacing the departmental CIO.

4.5.2.4 Ensuring that, for the purposes of the Treasury Board Executive Group (EX) Qualifications Standard, the departmental CIO possesses an acceptable combination of education, training and experience.

4.6 Monitoring and oversight

4.6.1 Deputy heads are responsible for:

4.6.1.1 Monitoring compliance with this policy and its supporting instruments within their department.

4.6.1.2 Advising the Secretary of the Treasury Board on a timely basis when there are significant issues with complying with this policy and its supporting instruments.

4.6.1.3 Ensuring that appropriate and timely remedial action is taken when significant issues with compliance arise within the department.

4.6.2 The Secretary of the Treasury Board, while recognizing and supporting deputy heads as the lead responsibility within their respective departments, is responsible for:

4.6.2.1 Conducting risk-based monitoring, providing guidance, and recommending corrective actions regarding:

4.6.2.1.1 Compliance with this policy and its supporting instruments;

4.6.2.1.2 Departmental performance on service, information, IT and cyber security management; and

4.6.2.1.3 The service, information, IT and cyber security management function across government.

4.6.2.2 Advising deputy heads on a timely basis when significant incidents of non-compliance with this policy and its supporting instruments are identified.

5. Roles of other government organizations

5.1 This section identifies other key government organizations in relation to this policy. In and of itself, this section does not confer any authority.

5.2 Shared Services Canada is responsible for the following:

5.2.1 Providing certain services related to email, data centres, networks and end-user technology devices. Use of SSC services is required for specified government departments; however other departments and agencies may also choose to use these services.

5.2.2 Whenever possible, SSC is responsible for delivering these services in a consolidated and standardized manner. Some of SSC's services are provided on a cost-recovery basis. In exceptional circumstances, the Minister responsible for SSC can personally authorize a department to provide itself with otherwise mandatory services (or obtain them from a third party).

5.3 Public Services and Procurement Canada is responsible for the following:

5.3.1 Providing services for federal departments and agencies, to support them in the achievement of their mandated objectives as their central purchasing agent, linguistic authority, real property manager, treasurer, accountant, integrity adviser, and pay and pension administrator.

5.3.2 Providing common enterprise solutions and services related to the following: electronic document records management systems, case and workflow tracking solutions, and collaboration platforms. Whenever possible, PSPC is responsible for delivering these services in a consolidated and standardized manner. PSPC’s services are provided on a cost-recovery basis.

5.4 Library and Archives Canada is responsible for the following:

5.4.1 Acquiring, preserving, making known and facilitating access to the documentary heritage of Canada;

5.4.2 Preserving the published heritage of the nation and of the Government of Canada;

5.4.3 Identifying, selecting, acquiring and preserving government records, as defined in the Library and Archives of Canada Act, in all media considered to be of enduring value to Canada as documentary heritage;

5.4.4 Issuing records disposition authorities, pursuant to section 12 of the Library and Archives of Canada Act, to enable departments to carry out records disposition;

5.5 Statistics Canada is responsible for the following:

5.5.1 Collaborating with and providing assistance to federal government departments in the collection, compilation, analysis and publication of statistical information, including statistics derived from the activities of federal government departments; and

5.5.2 Recognizing and addressing opportunities to avoid duplication in statistical collection across the Government of Canada.

5.6 The Communications Security Establishment is responsible for the following:

5.6.1 CSE is the lead technical authority for information and IT security including the provision of leadership, advice and guidance for technical matters related to IT security. It helps ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada, and fulfils government-wide functions by identifying emerging cyber threats, monitoring government networks and systems, and helping protect against, and mitigate potential impacts of cyber security events.

5.6.2 CSE leads the development of trusted sources of supply for government and critical infrastructure alongside mitigating the risk of untrusted equipment.

5.6.3 CSE is the national authority for communications security (COMSEC), including the procurement, distribution, control and use of cryptographic devices and encryption keying material for national security systems.

5.6.4 CSE is also Canada’s national authority for signals intelligence (SIGINT).

5.7 Public Safety Canada is responsible for the following:

5.7.1 Heading coordination and strategic policy-making on national cyber security matters.

5.8 Canada School of Public Service is responsible for the following:

5.8.1 Development and delivery of a government-wide core learning strategy and program for all public servants. These tasks are performed in consultation with the relevant functional authority centres.

6. Application

6.1 This policy and its supporting instruments apply 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 4.4.2.5 and 4.4.2.6 only apply to the core public administration as defined in section 11.1 of the FAA, unless otherwise excluded by specific acts, regulations or orders-in-council. Other departments or separate agencies not subject to these provisions are encouraged to meet these requirements as good practice.

6.3 This policy does not apply to National Security Systems, except where the Chief Information Officer of Canada is identified as the system business owner.

6.4 Agents of Parliament

6.4.1 The following organizations are considered agents of Parliament for the purposes of the policy:

- 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

6.4.2 Agents of Parliament are solely responsible for monitoring and ensuring compliance with the policy within their organizations, as well as for responding to cases of non-compliance in accordance with any Treasury Board of Canada instruments that address the management of compliance

6.4.3 With regard to agents of Parliament the following do not apply:

- 4.1.2.2, 4.1.2.3, 4.1.2.4, 4.1.2.7, 4.1.3.6, 4.1.3.7, 4.3.1.1, 4.4.1.1, 4.4.1.7, 4.4.2.3, 4.6.2.1, and 7.1

7. Consequences of non-compliance

7.1 For an outline of the consequences of non compliance, refer to the Framework for the Management of Compliance (Appendix C: Consequences for Institutions and Appendix D: Consequences for Individuals).

8. References

8.1 Legislation

- Access to Information Act
- Canada Evidence Act

- Department of Justice Act
- Emergency Management Act
- Financial Administration Act
- Library and Archives of Canada Act
- Official Languages Act
- Personal Information Protection and Electronic Documents Act (Part 2)
- Privacy Act
- Public Service Employment Act
- Security of Information Act
- Service Fees Act
- Shared Services Canada Act
- Statistics Act

8.2 Related policy instruments

- Foundation Framework for Treasury Board Policies
- Policy on Access to Information
- Policy on Communications and Federal Identity
- Policy on Green Procurement
- Policy on Government Security
- Policy on the Planning and Management of Investments
- Policy on Official Languages
- Policy on Privacy Protection
- Policy on Results
- Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service
- Policy on Transfer Payments
- Values and Ethics Code for the Public Sector
- Directive on the Management of Projects and Programmes
- Directive on Charging and Special Financial Authorities

9. Enquiries

9.1 For interpretation of any aspect of this policy, contact Treasury Board of Canada Secretariat Public Enquiries.

Appendix A: Definitions

Applications ***(Applications)***

Subclass of software that employs the capabilities of an electronic device directly and thoroughly for a task that the user wishes to perform.

Artificial Intelligence ***(Intelligence artificielle)***

Information technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours, or solving problems.

Automated Decision System ***(Système décisionnel automatisé)***

Includes any technology that either assists or replaces the judgement of human decision-makers. These systems draw from fields like statistics, linguistics, and computer science, and use techniques such as rules-based systems, regression, predictive analytics, machine learning, deep learning, and neural nets.

Client ***(Client)***

Individuals, businesses or their representatives served by or using either internal or external services provided by the Government of Canada. When describing interactions with information technologies, clients can be referred to as users.

Client-centric ***(Axé sur les clients)***

An approach that focuses on addressing client or user expectations, needs, challenges and feedback. It enables the creation of a positive experience for the client or user, considering a broad range of factors such as access, inclusion, accessibility, security, privacy, simplicity, and choice of official language.

Client feedback ***(Rétroaction du client)***

Information coming directly from recipients of services about the satisfaction or dissatisfaction they feel with a service or product, and is a critical part of service improvement. It can take several forms, including: in-service client feedback, client satisfaction surveys, user experience testing, and consultations.

COBIT ***(COBIT)***

Stands for "Control Objectives for Information and related Technology" and represents a set of best practices that provide guidance for the management of IT processes. (Source: IT Governance Institute)

Cyber security ***(Cybersécurité)***

The body of technologies, processes, practices and response and mitigation measures designed to protect electronic information and information infrastructure from mischief, unauthorized use, or disruption.

Data ***(Données)***

Set of values of subjects with respect to qualitative or quantitative variables representing facts, statistics, or items of information in a formalized manner suitable for communication, reinterpretation, or processing.

Devices ***(Dispositifs)***

Electronic tools that can include, but are not limited to, the following: desktop workstations, laptops, notebooks, tablets, cellphones, peripherals such as printers and scanners, memory drives, CD/DVD drives, webcams and any other hardware used to obtain, store, or send information.

Digital ***(Numérique)***

Processes, practices and technologies related to the production, storage, processing, dissemination and exchange of electronic information and data. It refers to, among other things, information and communications technologies, infrastructures, and the information and data they produce and collect.

Digitally enabled ***(Facilité par le numérique)***

Operations and services that are supported by strategically leveraging information and communications technologies, infrastructures, and the information and data they produce and collect.

Digital initiative ***(Initiative numérique)***

A digitally enabled service or solution, information system, or application.

Electronic network ***(Réseau électronique)***

Groups of electronic devices and systems that can communicate through wired or wireless connections with each other, including without limitation, the Internet, Government of Canada electronic data networks, voice and video network infrastructure, and public and private networks external to a department.

Emerging technologies ***(Technologies émergentes)***

New technology (or new to the Government of Canada) that when adopted will substantially change the digital footprint of the Government of Canada.

Enterprise Architecture ***(Architecture intégrée)***

Conceptual blueprint that defines the structure and operation of an organization considering and aligning business, information, data, application, technology, security and privacy domains to support strategic outcomes.

Enterprise Information Management (EIM) solution ***(Solutions de gestion intégrée de l’information (GII))***

Enterprise automated solutions used to manage, protect and preserve information resources from creation to disposition. These solutions maintain appropriate contextual information (metadata) and enable organizations to access, use, retain, and dispose of records (i.e., their destruction or transfer) in a managed, systematic and auditable way to support accountability, transparency and departmental business objectives.

External services ***(Services externes)***

A service where the intended client is external to the Government of Canada.

Identity assurance ***(Assurance de l'identité)***

A measure of certainty that an individual, organization or device is who or what it claims to be.

Information ***(Information)***

Knowledge captured in any format, such as facts, events, things, processes, or ideas, that can be structured or unstructured, including concepts that within a certain context have particular meaning. Information includes data.

Information architecture ***(Architecture de l'information)***

The structure of the information and data components of an enterprise, their interrelationships, and principles and guidelines governing their design and evolution over time. Information architecture enables the sharing, reuse, horizontal aggregation, and analysis of information.

Information life cycle ***(Cycle de vie de l'information)***

Encompasses the planning, collection, creation, receipt, capture, organization, use, re-use, dissemination, maintenance, protection and preservation, disposition, and evaluation of information.

Information management ***(Gestion de l'information)***

A discipline that directs and supports effective and efficient management of information and data in an organization, from planning and systems development to disposal or long-term preservation.

Information technology ***(Technologie de l'information)***

Any equipment or system that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of information or data. It includes all matters concerned with the design, development, installation and implementation of information systems and applications.

Interoperability ***(Interopérabilité)***

The ability of different types of electronic devices, networks, operating systems, and applications to work together effectively, without prior communication, to exchange information in a useful and meaningful manner.

Internal Enterprise Services ***(Services internes intégrés)***

A service provided by a Government of Canada department to other Government of Canada departments intended on a government-wide basis.

ITIL ***(BITI)***

Stands for "Information Technology Infrastructure Library" and represents a set of best practices that guide IT service management. (Source: ITIL)

Management of information technology ***(Gestion des technologies de l'information)***

Planning, acquiring, building, implementing and operating of IT assets, systems or services, measuring their performance, and arranging their disposal.

Monitoring practices ***(Pratiques de surveillance)***

Use of a software system that monitors networks or devices for slow or failing components, and notifies the administrator in cases of outages, and that can monitor the network or device activity of specific individuals for indicators of unacceptable usage.

Online end-to-end ***(En ligne de bout en bout)***

Services available on the internet from beginning to end, without having to move off-line to complete a step in the process. For example, the ability to receive a service online from the application, to the receipt of the final output and the provision of feedback.

Open access ***(Accès ouvert)***

The unrestricted provision of Internet access, in accordance with the Policy on Government Security, to authorized individuals via Government of

Canada electronic networks and devices.

Personal information ***(Renseignements personnels)***

Information about an identifiable individual that is recorded in any form, as defined in the *Privacy Act*.

Privacy breach ***(Atteinte à la vie privée)***

The improper or unauthorized collection, use, disclosure, retention, or disposal of personal information.

Real-time application status ***(État de demande en temps réel)***

Information on the current standing of a request for a service or product.

Real-time performance informations ***(Information sur le rendement en temps réel)***

Information on the current level of performance that clients can expect to be provided for a service, relative to an established standard..

Repository ***(Répertoire)***

A repository is a preservation environment for information and data resources which includes specified physical or electronic storage space and the associated infrastructure required for its maintenance.

Service ***(Service)***

Provision of a specific final output that addresses one or more needs of an intended recipient and contributes to the achievement of an outcome.

Service Inventory ***(Répertoire de services)***

A catalogue of external and internal enterprise services that provides detailed information based on a specific set of elements (e.g., channel, client, volume, etc.).

Service Standard ***(Normes de service)***

Public commitment to a measurable level of performance that clients can expect under normal circumstances.

ISBN: 978-0-660-31822-6

Date modified: 2024-12-02