Privacy Management Framework

Innovation, Privacy and Policy Division, Technology and Innovation

Version: 1.0

Approved by: ADM, Innovation, Privacy and Policy Division	**Owner:** Innovation, Privacy and Policy Division	
Approval date: January 25, 2024	**Last Reviewed:** January 22, 2024	**Review Date:** January 22, 2026
Contact: SA.FOIP-PolicyInstruments@gov.ab.ca	**Policy Instrument type:** Framework	

Contents

Introduction and Purpose

Under the *Freedom of Information and Protection of Privacy Act* (FOIP Act), the Government of Alberta (GoA) is accountable for, and committed to, protecting and securing the personal information in its custody and/or under its control from unauthorized collection, access, use, disclosure and destruction.

This framework provides high-level strategic direction to maintain consistent and effective privacy management across the GoA in today's rapidly evolving digital world. The Privacy Management Framework demonstrates the GoA's commitment to the protection of personal information by:

- defining "privacy by design";
- specifying Framework Principles that will inform the development and revision of new and/or existing policy instruments;
- highlighting privacy-related commitments the GoA will be implementing in support of the Framework Principles; and
- providing an overview of the roles, policy instruments and processes that support and articulate the Framework Principles.

The framework must be interpreted in the context of all applicable legislation, including the FOIP Act, *Health Information Act* (HIA), and/or legislation specific to any department's governance and operations.

Executives and staff must also apply this framework in the context of:

- the Oath of Office,
- Alberta Public Service Vision and Values, and
- the Code of Conduct and Ethics for the Alberta Public Service.

This framework is not intended to provide operational recommendations or implementation insight, as subsequent policy instruments will be developed in alignment with the framework principles.

NOTE: There are legislated, mandatory requirements for information that are part of Freedom of Information and Protection of Privacy (FOIP) requests and/or information that is subject to the *Health Information Act* (HIA); these requirements are paramount to this directive and the associated guidance. For more information, please contact the appropriate FOIP Coordinator and/or the HIA Help Desk.

Vision

The GoA is an accountable steward of personal information that uses a privacy by design approach for the secure exploration and/or implementation of emerging, innovative technologies, programs and services.

The GoA's privacy by design approach establishes an environment in which Albertans trust that their privacy is respected and their personal information is protected.

Framework Scope

The framework applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards, and commissions designated in Schedule 1 of the Freedom of Information and Protection of Privacy Regulation (FOIP Regulation). Agencies, boards, and commissions that are not designated in Schedule 1 of the FOIP Regulation are encouraged to align with the framework.

Benefits

Effective and thorough implementation of the Privacy Management Framework has benefits for both the GoA and Albertans.

- For the GoA, comprehensive privacy management:
    - is an investment that reduces legal and operational risks to GoA;
    - results in the development and implementation of better, more robust systems and services; and
    - dramatically increases the quality, availability and trustworthiness of the content in the custody and/or under the control of government.
- For Albertans, comprehensive privacy management:
    - will help ensure that personal information is protected from unauthorized or inappropriate collection, access, use, disclosure or destruction;
    - allows for the creation of more responsive government programs and service delivery options;
    - improves trust of, and in, government.

Privacy by Design

Privacy by Design advances the view that the future of privacy management cannot be assured solely by compliance with regulatory requirements; rather, privacy management must become a default mode of operation to assure Albertans that their personal information is protected. Privacy considerations (including the identification of, and reasonable steps taken to mitigate, risks) must be emphasized repeatedly at all levels, in all aspects of design, operation, and management.

Framework Principles

This framework is organized around four core principles necessary for a privacy by design approach:

- **Planning**: Privacy is an integral, embedded consideration when developing any government priorities, activities, initiatives and operations.
- **Security and Control**: Reasonable security and privacy protection measures are developed and implemented to prevent and/or mitigate the unauthorized collection, access, use, disclosure and destruction of personal information.

- **Openness**: Information pertaining to privacy management and how personal information is collected, accessed, used, disclosed and destroyed must be readily available to Albertans.
- **Accountability**: Processes and governance must be in place to ensure personal information is protected; avenues for recourse or resolution, if required, must be provided.[1]

Planning

Privacy is an integral, embedded consideration when developing any government priorities, activities, initiatives and operations. To fully embed privacy into the planning of government priorities, activities, initiatives, and operations, the GoA will:

- Develop and implement technology and data strategic initiatives that fully recognize the importance of privacy while continuing to support innovation.
- Apply a user-centric approach in developing, refining, and improving privacy policies by keeping the users' privacy interests as a primary focus of all privacy-related decision-making.
- Ensure that awareness of, and communication regarding, privacy policies is further integrated into mandatory training.
- Ensure that privacy evaluations and controls are integrated when implementing or modifying any system, practice, project, program, or initiative involving the collection, access, use, disclosure and destruction of personal information.
- Review privacy controls (e.g., process requirements, technical system specifications, etc.) regularly in collaboration with subject matter experts (e.g., OIPC).

Support Mechanisms

The policy instruments and processes that support planning include (but are not limited to):

- The Content Management Policy that defines content (which includes personal information) and states the requirements to which departments will adhere when managing content.
- The Data Ethics Framework that guides the ethical collection, management, and use of data including respecting individuals' rights to privacy.
- Privacy obligations for each aspect of the Information Management Lifecycle; create/collect, organize, use/access, disposition, management, and security.
- Codification and clarification of privacy expectations and requirements focused specifically on emerging technologies and associated practices (e.g., de-identification, data fabric, etc.).

Security and Control

Reasonable security and privacy protection measures are developed and implemented to prevent and/or mitigate the unauthorized collection, access, use, disclosure and destruction of personal information. To maintain and enhance security and control, the GoA will:

- Continue to recognize content and technology as critical assets, and that the management, control and protection of these assets has a significant impact on service delivery.

[1] These four core framework principles were developed based on the seven principles of privacy by design but take into account the particular GoA business environment and processes. The seven principles of privacy by design are: 1. privacy is proactive, not reactive; 2. privacy as the default setting; 3. privacy embedded into design; 4. full functionality – positive-sum, not zero-sum; 5. end-to-end protection – lifecycle security; 6. visibility and transparency; and 7. respect for user privacy – keep it user-centric.

- Proactively identify and assess risks to privacy and personal information, and make reasonable security arrangements to mitigate those risks.
- Ensure appropriate physical, technological, administrative and/or operational safeguards proportionate to the sensitivity of the information are in place.

Support Mechanisms
The policy instruments and processes that support security and control include (but are not limited to):

- Technical standards and directives (e.g., the Data and Information Security Classification Standard).
- Official information management systems (e.g., file rooms, M365), and established and approved hardware/software platforms.
- Privacy assessments to identify potential privacy risks and mitigation strategies when implementing or modifying systems, practices, projects, programs, or initiatives involving the collection, access, use, disclosure or destruction of personal information.
- A breach response process to be followed when breaches occur.
- Requirements detailing how and when personal information can be accessed within and outside of the department, and how information should be protected.
- A requirement that personal information can only be destroyed in alignment with approved records retention schedules.

Openness

Information pertaining to privacy management and how personal information is collected, accessed, used, disclosed and destroyed must be readily available to Albertans. To enhance openness, the GoA will:

- Provide clear, consistent communication to Albertans regarding how and/or why their information is collected, accessed, used, disclosed and destroyed.
- Publicly disclose information regarding how the government leverages evolving and innovative technologies to inform decision-making and provision of services.
- Continually inform Albertans of the steps taken to protect personal information, including (but not limited to) risk assessments and general mitigation activities.
- Continue to modernize and improve the delivery of information access services that allow individuals the ability to request access to their personal information.
- Provide notice of how personal information will be used and stored when interacting with service technology, artificial intelligence and automated decision-making software.

Support Mechanisms
The policy instruments and processes that support openness include (but are not limited to):

- Mandatory collection notices when personal information is collected directly from the individual it is about.
- Regular review of collection notices by business areas to ensure alignment with the purpose of collection and relevant privacy policy instruments.
- Publication of a directory that lists a department's personal information banks.
- Function-based records retention and disposition schedules that will clearly communicate how long personal information is being retained and how and/or when personal information will be disposed.

Accountability

Processes and governance must be in place to ensure personal information is protected; avenues for recourse or resolution, if required, must be provided. To maintain accountability, the GoA will:

- Enhance the existing privacy management governance structure by codifying processes, clarifying reporting structures, and exceeding legislated obligations.
- Ensure content management requirements (and privacy requirements in particular) are met or exceeded through monitoring and compliance measures.
- Continue to revise and improve mandatory training in alignment with privacy management best practices.
- Support efforts by senior management and executive to champion effective, consistent privacy practices.
- Promote a culture in which all staff know and understand their privacy responsibilities and obligations.

Support Mechanisms

The roles, policy instruments, and processes that support accountability include (but are not limited to):

- The Information and Privacy Commissioner, an Independent Officer of the Legislature of Alberta that serves as the regulator and oversight body for Alberta's access to information and privacy laws.
- Service Alberta and Red Tape Reduction, and Technology and Innovation, the GoA departments that are responsible for the provision of access and privacy services, and that have legislated authority for establishing enterprise content management requirements (e.g., rules, obligations, definitions, etc.) and policy instruments.
- The Government of Alberta's Chief Privacy Officer and Chief Data Officer, who approve enterprise data definitions and governance requirements, and is responsible for creating, maintaining, and promoting the Government of Alberta privacy framework.
- Privacy Services - A dedicated business unit within Technology and Innovation focused on ensuring government departments are compliant with privacy requirements through the use of privacy tools, such as, Privacy Impact Assessments.
- The requirement that deputy heads will ensure successful implementation of enterprise policy instruments for content management (including, but not limited to, privacy and security) within their departments.
- Mandatory training on information management, FOIP, and cyber security that must be completed annually by GoA staff (which includes, but is not limited to, employees, contractors, volunteers, appointees, interns, and students working with a public body).
- A requirement that organizations delivering services for, or on behalf of, the GoA (i.e., service providers) follow GoA privacy policies and procedures.
- Regular review and revision of privacy management policy instruments.
- A process for handling privacy inquiries and complaints.

Contact

For more information on privacy management and/or the protection of personal information, please contact privacy@gov.ab.ca.