



Privacy Management Framework Toolkit

Introduction

Technology and Innovation is dedicated to assisting departments, agencies, boards, and commissions in applying the [Privacy Management Framework](#) (PMF) when initiating a new program, service, and/or application.

The PMF Toolkit is intended to help staff understand the application of its four guiding principles (**Planning, Security and Control, Openness, and Accountability**). The toolkit is available to all Alberta Public Service employees and is intended to be used in combination with the PMF.

There are legislated, mandatory requirements for information that are part of the *Freedom of Information and Protection of Privacy Act* (FOIP) and/or information that is subject to the *Health Information Act* (HIA); these requirements are paramount to the PMF.

Overview of the Privacy Management Framework

The PMF provides high-level strategic direction to maintain consistent and effective privacy management across the Government of Alberta (GoA) in today's rapidly evolving digital world.

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 Principles

Planning

Privacy is an integral, embedded consideration when developing any government priorities, activities, initiatives, and operations.

Applying the Principle

- Complete all mandatory privacy training and become familiar with and adhere to enterprise privacy policies and guidance; mandatory training is identified in the Learning section of 1GX and enterprise policy instruments can be found on the [Information Management and Technology Policy Instruments site](#) and are referenced in the PMF).
 - If gaps in privacy policy or training are identified or there is a lack of clarity or understanding, contact the [Privacy Services team](#) in Technology and Innovation.
- If you are considering doing any new work involving personal information, consult with the Privacy Services team for advice regarding authority to collect, use, and disclose personal information.
- When developing or implementing new technologies or programs, ensure privacy considerations are incorporated into all stages of program and service design, development, and implementation. This means engaging with the necessary parties (such as [Privacy Services](#), [Cybersecurity](#), etc.) early in program development.
- Work with the Privacy Services team to ensure privacy concerns and mitigation strategies are identified and captured in the appropriate risk assessments.
- Engage with potential stakeholders at the outset of policy development to understand a variety of perspectives.

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.

Applying the Principle

- Complete all mandatory privacy training and become familiar with and adhere to enterprise privacy and information management and technology policy instruments; mandatory training is identified in the Learning section of 1GX and includes topics such as FOIP/Privacy, Information Management, and Cybersecurity (enterprise policy instruments on these topics can be found on the [Information Management and Technology Policy Instruments site](#) and are referenced in the PMF).
 - Ensure there is a foundational understanding of legislated privacy responsibilities and obligations.
- Ensure GoA devices, including mobile devices, are promptly updated when system updates are released.
- Routinely refresh your knowledge of the agreements that all APS staff are bound by (for example, Oath of Office, Code of Conduct and Ethics).
- Work with the appropriate team (i.e., [Privacy Services](#), [Cybersecurity](#)) to ensure the appropriate risk assessments and arrangements are completed when developing new programs.
- Report privacy breaches promptly to the Privacy Services team as prescribed in the [Privacy Breach Procedure](#).
- Familiarize yourself with and routinely implement practices to safeguard government information, such as:
 - practicing a clean desk policy, including when working remotely;
 - not distributing government content through personal email;
 - locking your computer when away from your desk; and
 - using locked bins for the secure destruction of physical transitory documents.

Openness

Information pertaining to privacy management and how personal information is collected, accessed, used, disclosed, and destroyed must be readily available to Albertans.

Applying the Principle

- When collecting personal information for programs and services, consult with the Privacy Services team to develop clear and detailed FOIP collection notices that meet legislative requirements.

Accountability

Processes and governance must be in place to ensure personal information is protected; avenues for recourse or resolution, if required, must be provided.

Applying the Principle

- Complete all mandatory training with the intent to meaningfully apply it and ensure awareness and familiarity with policy instruments for privacy management as they are frequently reviewed/enhanced/created to ensure relevance; mandatory training is identified in the Learning section of 1GX and includes topics such as FOIP/Privacy, Information Management, and Cybersecurity (enterprise policy instruments on these topics can be found on the [Information Management and Technology Policy Instruments site](#) and are listed on the PMF page).
- Ensure awareness of key privacy roles that have been designated in your area and engage them appropriately when handling privacy-related matters.
- Ensure that accountability measures exist and are documented to ensure requirements established under policy instruments and legislative obligations are being followed.
- Communicate the need for a consistent approach to privacy management and seek guidance from the Privacy Services team as required.

Resources

- Additional resources and support mechanisms are provided in the [PMF](#).

Contacts

- If you have questions about the PMF, or privacy related policy instruments, contact imt.policy@gov.ab.ca
- For more information on and assistance with privacy management processes, contact privacy@gov.ab.ca