Information Management and Technology (IMT) Policy Program

Program Overview

Contents

Introduction

Information and technology are key strategic resources in the Government of Alberta (GoA) and are at the very core of its operations. Programs and services that Albertans rely on, decision-making, and policy development and planning activities are all founded on information and technology. To help ensure information and technology are identified and used as strategic resources, the necessary rules, requirements and safeguards must be established, maintained and communicated across the GoA through a variety of policy instruments (for example, guidelines, standards, and directives).

Purpose

Technology and Innovation's (TI) Information Management and Technology (IMT) Policy Program (the Program) plays a critical role in the development and maintenance of enterprise IMT policy instruments. The Program provides central governance and ensures a collaborative and coordinated approach to the development and enhancement of the GoA's enterprise IMT policy instruments.

The Program:
- establishes a corporate approach to develop, plan, coordinate, review and manage IMT policy instruments (as outlined in Appendix 1);
- provides oversight for policy development across TI, including providing guidance to TI divisions on the responsibilities of IMT policy instrument ownership;
- outlines roles and responsibilities and establishes channels for communication and policy coordination between TI divisions;
- establishes governance and accountability for approvals; and
- establishes a portal for IMT policy instruments that is accessible to GoA staff, public agencies, external parties, and the public.

> ### IMT Policy Program Vision
> Consistent and effective IMT policy instruments are developed and maintained through collaborative and common processes, while respecting the specialized knowledge and interests within Technology and Innovation and across the Government of Alberta.

Within the Government of Alberta's policy environment, IMT policies include:

- strategic policy: sets overall GoA direction and long-term objectives;
- operational policy: sets how the GoA delivers functions; and
- program policy: provides specific guidance and rules on how to interpret strategic policy or administer programs.

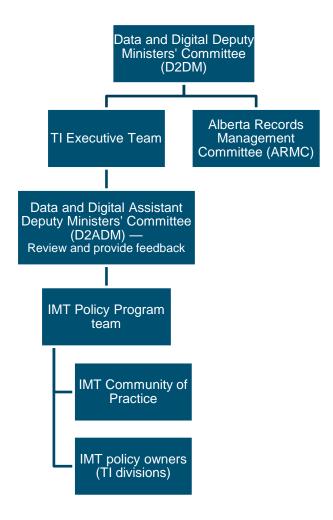Specific IMT Policy Program policy instruments are outlined in Appendix 1.

Objectives
- The GoA will function as a single corporate entity with regards to IMT policy.
- High quality enterprise IMT policies that are meaningful to their intended audience will be developed and maintained.
- Common IMT processes will be used to implement directives and related controls to manage delivery of IMT services.
- Strong, clear, and consistent communication and awareness methods will be utilized to communicate about the Program and policies across the GoA.
- IMT policy development and maintenance will be collaborative and integrated across TI divisions.

Classification: Public

Scope

- The Program applies to the development of enterprise IMT policy instruments, including mandatory policies, directives, and standards, along with supporting guidelines and tools.
- Operational processes and procedures are the responsibility of the accountable program area. Program areas are to ensure these documents align with established IMT policy instruments and consult with the applicable IMT policy instrument owner(s) if required.

Governance

```
Data and Digital Deputy Ministers' Committee (D2DM)
   ├── TI Executive Team
   │      └── Data and Digital Assistant Deputy Ministers' Committee (D2ADM) — Review and provide feedback
   │             └── IMT Policy Program team
   │                    ├── IMT Community of Practice
   │                    └── IMT policy owners (TI divisions)
   └── Alberta Records Management Committee (ARMC)
```

Roles and Responsibilities

Each section below describes the major roles within the Program.

IMT Policy Program Team
Policy Development
The Program team develops IMT policy instruments (see Appendix 1) on behalf of TI divisions. This includes:

- coordinating the overall operation of the Program;
- leading development of strategic policy, operational policy and program policy (working with program areas);
- leading and providing secretariat support for the Community of Practice (CoP) and escalating items that are unable to be resolved to the Executive Director responsible for the Program;

- coordinating and conducting SME reviews, in collaboration with the applicable policy owners, of draft or revised IMT policy instruments to ensure a variety of perspectives are considered (e.g., privacy, cybersecurity, application support, and other departments, including Health, the Public Service Commission, Communications and Public Engagement, and Justice);
- reviewing IMT policy instrument proposals drafted by TI divisions for submission to CoP;
- researching policy topics to inform options and support decision-making;
- engaging subject matter experts (SMEs) and TI divisions in the development of policy instruments;
- working collaboratively with IMT policy owners to develop, update, and enhance policy instruments in an integrated manner;
- tracking scheduled review dates for approved IMT policy instruments and initiating the review process with policy owners;
- supporting a consistent communications approach for IMT policy; and
- assisting policy owners in obtaining necessary approval(s) for IMT policy instruments, including briefing development and inclusion on the agenda for the appropriate approval committee (e.g., TI Executive Team, ARMC).

Program Administration

The Program team also carries out several administrative and coordination functions, which include:
- developing and maintaining:
  - templates for IMT policy instruments;
  - guidance materials, including documentation on how to seek approval for new and updated IMT policy instruments;
  - forms for documenting scheduled reviews and approvals; and
  - a Communication and Awareness Guide to guide IMT policy instrument owners in communicating their policy instruments.
- providing advice to policy owners on policy development, implementation, and communication;
- maintaining the Program's internal repository and public portal;
- monitoring and managing the imt.policy@gov.ab.ca mailbox; and
- providing secretariat support for D2ADM.

IMT Community of Practice (CoP)

The CoP consists of directors and managers from each division of TI. Its function is to enhance collaboration between TI divisions for the development and review of IMT policy instruments; it is not a decision-making body. This may include:
- identifying areas of common interest;
- identifying policy gaps and opportunities;
- reviewing policy proposals;
- recommending whether a raised issue requires the development/enhancement of a policy instrument, or if it can be resolved through processes, procedures, etc.
- recommending the appropriate type of policy instrument to address a raised issue;
- accepting terms (defined in approved IMT policy instruments) to be included in an authoritative glossary on the public portal; and
- vetting SMEs who can be engaged for consultation and review.

IMT Policy Owners (TI Divisions)

TI divisions provide a variety of IMT services to the GoA and require IMT policy instruments in their areas of operation and expertise.

IMT policy instrument owners are **accountable** for their IMT policy instruments throughout the policy cycle, while sharing the responsibility for certain processes with the IMT Policy Program team. For instance, while the Program team may develop a new policy instrument, owners are responsible for ensuring instruments meet their policy objectives. Owners have the primary responsibility for policy implementation and compliance.

Key accountabilities include:
- ensuring that IMT policy instruments are current and relevant;
- implementing IMT policy instruments, including the development and delivery of training;
- communicating IMT policy instruments to all applicable stakeholders (for example, any staff expected to comply with them);

- ensuring compliance with governance requirements, including responding to audits; and
- establishing mechanisms to encourage compliance with IMT policy instruments.

IMT Policy owners (or their delegates) are responsible for:
- identifying the need for a new/enhanced IMT policy instrument;
- developing proposals for new/enhanced IMT policy instruments to be submitted to the CoP through the IMT Policy Program team;
- collaborating with the IMT Policy Program team in the development and enhancement of IMT policy instruments;
- leading the development of operational procedures;
- briefing the appropriate division leadership prior to submitting an IMT policy instrument for approval and ensuring representation for the division at the approval meeting (if applicable);
- providing notification to the IMT Policy Program team when a new/enhanced policy instrument can be submitted to the appropriate approval body or role;
- leading the implementation and evaluation of policy instruments, including briefing leadership, communicating, and monitoring compliance with the IMT policy instrument;
- reviewing approved IMT policy instruments on a regular basis for currency and relevancy, according to the review schedule (see Appendix 2 and IMT Policy Program Operational Processes); and
- reviewing and revising outdated IMT policy instruments or seeking their rescindment.

> The development (including revision and enhancement) of IMT policy instruments is a shared responsibility between the IMT Policy Program team and policy owners. TI program areas may, when appropriate, choose to do their own policy development, provided that the templates and approvals process mandated by the Program are used. The IMT Policy Program team must be engaged to review and provide feedback to any new or revised policy instruments prior to approval.

Data and Digital Assistant Deputy Minister Committee (D2ADM)
As part of its broad oversight function, D2ADM reviews and provides feedback to the IMT Policy Program and policy owners on current and proposed policy instruments. D2ADM may also direct TI divisions (in conjunction with the IMT Policy Program) to develop policy instruments to address specific areas of concern.

IMT Policy Instrument Approvers
See Appendix 3 for the approval bodies (or roles if individual) for all IMT policy instrument types.

IMT policy instruments approvers are responsible for the final review and approval (or rejection) of IMT policy instruments. The approver may provide additional feedback to the IMT policy instrument owner for consideration prior to granting approval. Based on the recommendations of IMT policy instrument owners, approvers are also responsible for rescinding obsolete or superseded IMT policy instruments. Approvals and rescindments must be documented, and copies of the documentation must be provided to the IMT Policy Program.

The following is an overview of the various committees that act as approvers:

Data and Digital Deputy Minister Committee (D2DM)
D2DM approves GoA-wide IMT policies, frameworks, and strategies, and may also direct TI divisions (in conjunction with the IMT Policy Program) to develop policy instruments to address specific areas of concern.

TI Executive Team
The TI Executive Team approves the Digital Service Standards and IMT directives that are outside of the scope of the ARMC.

Alberta Records Management Committee (ARMC)
ARMC approves Records Retention and Disposition Schedules and IMT directives that relate specifically to the management of content, inclusive of all records, data, and information, regardless of format, state and/or classification.

Compliance and Risk Acceptance

All policy instruments under the scope of the Program are mandatory, except for guidelines and tools.

When non-compliance is reported to the IMT Policy Program team, the Program will work with the IMT policy instrument owner and applicable TI divisions to educate the non-complying business area or department. Legitimate circumstances exist in which a department cannot comply with one or more mandatory policy requirements or when the choice may be made to accept the risk of non-compliance. For example, a legacy system that does not meet current content management or security requirements. In these circumstances, the information controller may accept the risk of non-compliance.

Non-compliance instances will be identified and the IMT Policy Program notified. Instances of non-compliance will first be addressed with education and awareness. The IMT Policy Program will work with key partners across Alberta Technology and Innovation, including but not limited to Cybersecurity, Enterprise Content Management, Privacy Services, Technology Support and Operations, to provide education and awareness of the policy and risk of non-compliance. Should the non-complying business area or department choose to accept the risk of non-compliance, the above referenced acceptance of risk of non-compliance form will be completed and approved by the information controller. The Program will provide a standard form to document the acceptance of the risk of non-compliance and maintain a repository of completed risk acceptance forms.

IMT Policy Instruments Public Portal

The IMT Policy Program owns and manages the IMT Policy Instruments public portal, the primary source of current and accurate information and documentation regarding IMT policy instruments.

In general, IMT policy instruments are publicly accessible through the portal, except in circumstances where additional safeguards are necessary to mitigate potential risk. External visitors (including stakeholders, vendors, government agencies, other jurisdictions, and the general public) can access the landing page for any IMT policy instrument from the public internet, but a user must be authenticated to access the full text (usually a PDF file) of a Protected (A or B) IMT policy instrument—this effectively restricts access to GoA employees.

The portal will include a glossary of terms of approved definitions that can be found throughout IMT policy instruments, which will help policy instrument developers and owners to use terms consistently.

Classification: Public

Appendix 1: IMT Policy Instruments

The list below identifies IMT policy instruments that are in scope of the IMT Policy Program; please note, that acts and regulations are not in scope of the Program.[1]

The IMT policy instruments, listed in order of authority:

Acts are legislation, the laws of the province.

Regulations fall under an Act and carries out the intent of legislation.

Strategies outline and inform the strategic direction of the organization.

Frameworks provide context, rationale, principles, and broad strategic direction. It supports the effective and consistent development and implementation of all IMT policy instruments that flow from it.

Policies define a course of action or set of principles within government that directs, guides or influences decision-making and actions.

Directives establish expected behaviours and actions of employees. Directives provide formal instruction to take or avoid specific actions in order to meet specific objectives.

Digital Service Standards set expectations and actionable behaviours for teams that are responsible for the delivery of public-facing digital services.

Records Retention and Disposition Schedules outline the closure criteria, length of time (retention), and final disposition (archive or destruction) of government records.[2]

Standards are a set of mandatory operational or technical measures, requirements, or practices for government-wide use.

Guidelines and Tools provide guidance, advice, or explanation to assist in implementation of an approved IMT policy instrument (examples may include, best practices, handbooks, frequently asked questions, etc.).

---

[1] Not listed above are **circulars**, a legacy IMT policy instrument that outlines records management requirements set by the ARMC. Circulars are under review, and information contained in existing circulars will be redistributed to other IMT policy instruments where appropriate and the circular will be decommissioned.

[2] Schedules are not developed by the Program, but some GoA-wide schedules are published on the portal.

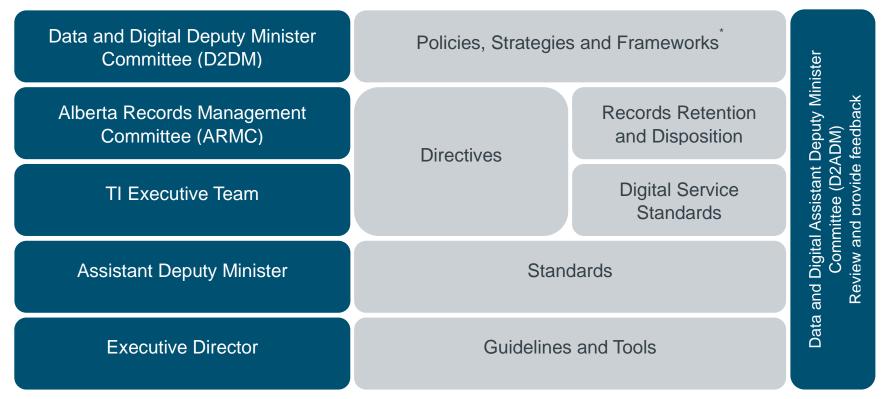# Appendix 2: IMT Policy Instrument Review Schedule

Policy owners are required to review their IMT policy instruments on a regular basis to determine if they are still required and ensure they are current. The minimum review frequency is determined by the type of IMT policy instrument as per the table below:

IMT Policy Instrument Types	Review Cycle
Strategies and Frameworks	Every 5 years
Policies	Every 5 years
Directives	Every 2 years
Digital Service Standards	Every 2 years
Standards	Every 2 years
Guidelines and Tools	As needed

IMT policy instrument owners may choose to review/update prior to a scheduled review date. Changes in technology, organizational structure, or business processes may also necessitate that a policy instrument review be conducted more frequently than indicated above.

Appendix 3: IMT Policy Approvals Matrix

Approver	Policy Type		Review
Data and Digital Deputy Minister Committee (D2DM)	Policies, Strategies and Frameworks *		Data and Digital Assistant Deputy Minister Committee (D2ADM) Review and provide feedback
Alberta Records Management Committee (ARMC)	Directives	Records Retention and Disposition	
TI Executive Team		Digital Service Standards	
Assistant Deputy Minister	Standards		
Executive Director	Guidelines and Tools		

* Approvals can be escalated to the Deputy Minister Council (DMC) or the Minister at the discretion of the Deputy Minister.