Critical Information RM Guide

This guide explains what critical information is in BC Government. Knowing how to identify the critical information you are responsible for will help you manage it.

A. What is Critical Information?

Government's critical information provides operational continuity and accountability over time. The Managing Government Information Policy (MGIP) defines critical information as:

> The records and data essential to the operations of a government business area. This includes information that supports business continuity by documenting and supporting core programs, functions, responsibilities, and commitments (e.g., security and risk mitigation information, records needed to meet financial and legal requirements). Critical information also includes information of public interest and permanent value.

B. Critical Information may have Short, Medium, or Long-term Uses

Short-term and medium-term:

Critical information that sustains the organizational functions, but only until related actions are completed.

Examples include:

- records and data of routine business processes, ongoing transactions, and systems operations
- information vital for business continuity and for maintaining or restoring operations after emergencies or disasters

Long-term:

Critical information that sustains ongoing business operations, core programs, functions, responsibilities, and commitments.

Examples include records needed:

- to meet policy, security, risk management, financial and legal responsibilities, and research needs
- for permanent retention in the government archives as ongoing evidence of government's functions, decisions, and actions

C. Why is it Important to Identify Critical Information?

Critical information is among government's most valuable assets. Ministries are required to identify critical information in their custody or control and to ensure that it will "… retain its integrity and remain reliable, usable, accessible, and secure for as long as needed." (MGIP Section 1)

Identify and store critical information in an appropriate recordkeeping system to support accurate and efficient information searches, protect privacy and confidentiality, preserve long-term reliability of the information, and manage appropriate access. Provide content in paragraphs, using bullets as appropriate.

D. Managing Critical Information

Critical information requires routine management to protect its integrity and trustworthiness. To achieve this, each ministry is responsible to:

1. **Identify** critical information in the ministry's custody and control. For instance, establish a critical information inventory authorized by the relevant program or project manager. Consult the critical information features listed below for assistance with identification.
2. **Manage** critical information in an appropriate recordkeeping system with controls for security, accessibility, transfer, and disposition.
3. **Protect** critical information by ensuring timely transfers to an appropriate recordkeeping system when information is created or received elsewhere.
4. **Dispose** of critical information in accordance with policy requirements identified in the RIM Manual.

Documenting Government Decisions

If your information contains evidence of actions or decisions, it must be managed in the appropriate recordkeeping system. For more information on appropriate recordkeeping systems and the requirement to document government decisions, see the Chief Records Officer Guidelines on Documenting Government Decisions.

To comply with the *Information Management Act* government bodies must:

- ensure that an appropriate system is in place for maintaining government information
- create and maintain adequate records of their decisions

E. Critical Information Identification Checklist

The following checklist will assist you to inventory critical information that your ministry is responsible for. Review the information in all your systems and other shared storage locations, and identify data and records that have any of the critical information features described below. The resulting list will form a critical information inventory. To make sure it is comprehensive and accurate, now and over time:

- Consult colleagues, subject matter experts, and ministry records management staff to ensure the inventory is comprehensive and accurate
- Regularly update and review the inventory

Critical Information Feature	Feature Description	☑
1. Operational importance	Required for ongoing work or to document accountability for that work.	
2. Vital records	Vital to ongoing operations in business continuity plans and/or in the relevant information schedule.	
3. Risks and Security	Would result in significant public or organizational risks or security issues if lost, inappropriately accessed, or altered. This includes, but is not limited to, information designated as personal, confidential or a protected classification.	
4. Financial matters	Authorizations and/or allocation, spending, or collecting of substantive amounts of money.	
5. Legal and Access searches	Relevant to legal holds or FOI access to information requests.	
6. High public interest and expectations	Concerns rights, responsibilities, and other matters that stakeholders (e.g. citizens, MLAs, executive) expect to be documented.	
7. Permanent value	Records designated as having enduring value for the ministry and scheduled for permanent retention in the government archives.	

Additional Information

Contact your Records Officer and check out the Records Management website.