Archives of Manitoba
Government Records Office

# Recordkeeping Framework for Departments and Agencies: Policies and Requirements

## Authority

This suite of policies and requirements is issued under section 8 (a) of *The Archives and Recordkeeping Act* (C.C.S.M. c. A132) which enables the Archives of Manitoba to establish government-wide policies, standards, and guidelines for recordkeeping based on professional standards and best practices. The Government Records Office (GRO), a unit within the Archives of Manitoba, is the central agency that administers these responsibilities.

## Acknowledgements

The Framework is based on the State Records Authority of New South Wales' *Standard on records management* (2018) and *Implementation Guide* (2023) and the Archives of New Zealand's *Information and records management standard* (2016) and *Implementation Guide* (2022).

## References

The policies and requirements are in accordance with the International Standards Organization (ISO) group of standards, technical reports, and codes of best practice on Archives/records management - ISO/TC 46/SC 11.

## Contents

## Introduction

Records and information are key strategic assets of government and are the evidence of government business. In the Manitoba government, records and information help departments and agencies plan for and achieve short-term and long-term outcomes that benefit citizens, business, and government.

Ensuring that evidence of government business is created, captured, and managed is not simply about legislative compliance. A well-managed information base is the foundation of responsible, accountable government. It is a public service duty that underpins data-driven evaluation, responsible stewardship, and evidence-based decision-making in the public interest.

Records and information:

- provide the foundation for sustainable and effective programs, products, and services
- support decision-making
- outline responsibilities
- document rights and entitlements
- drive collaboration and communication
- facilitate and enable transformation, creativity, and growth
- preserve public knowledge for discovery and reuse
- make up the corporate memory of an organization
- support transparency and accountability

To provide these benefits, records and information need to be:

- routinely created and captured
- trustworthy
- available when needed, understandable, and usable
- secured and protected
- valued as critical to business operations
- part of an organization’s approach to risk management
- maintained and disposed of in an authorized way
- managed effectively and responsibly

## Purpose

This Framework sets out three high-level policies and corresponding requirements for effective records and information management in the Manitoba government. It is designed to help departments and agencies understand their records management responsibilities and meet their obligations under *The Archives and Recordkeeping Act* (ARA). The policies cover records and information in all formats, including both digital and physical records, and special attention is focussed on digital recordkeeping as the Government of Manitoba continues its transition to digital business processes.

The goal is to ensure that in complex business and information environments business is supported by sound, integrated records and information management, generally referred to as recordkeeping. The policies should be implemented in conjunction with instructions, directions, and any other standards or guidance issued by the Archives of Manitoba under the authority of the ARA.

## Scope

The policies are applicable to all Manitoba government bodies, defined in ARA as: a government department, a government agency,[1] the Executive Council Office, and the office of a minister. For the purposes of this Framework, government bodies are referred to as "departments" or "departments and agencies."

The Recordkeeping Framework can also be used by the Courts (ARA, s. 10) and the Legislative Assembly and officers (ARA, s. 11).

## Intended outcomes

Departments and agencies that comply with the policies and requirements will:

- create trustworthy, useful, and accountable records and information in evolving business environments
- ensure that meaningful, accurate, reliable, and useable records and information are available whenever required for government business
- sustain and secure the records and information needed to support short and long-term business outcomes
- enable the reliable sharing of relevant records and information
- minimise records and information volumes, preventing unnecessary digital and physical storage and management costs
- proactively protect and manage the records and information that provide ongoing value to government business and to the public
- meet obligations and requirements of *The Archives and Recordkeeping Act*

[1] A government agency is defined as "any board, commission, association, agency, or similar body, whether incorporated or unincorporated, all the members of which, or all the members of the board of management or board of directors or government board of which are appointed by an Act of the Legislature or by the Lieutenant Governor in Council, and any other body designated as a government agency in the regulations." This includes Manitoba Crown corporations.

# Policy 1 – Governance: Departments and agencies are responsible for recordkeeping

To ensure records and information can support all business functions and operations departments must:

- assign responsibilities and allocate resources
- develop business-specific strategies and priorities directing how records and information will be managed
- communicate responsibilities, strategies, and priorities throughout the department
- monitor recordkeeping activities, systems, and processes

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| 1.1 Recordkeeping is the responsibility of senior management. | Ultimate responsibility for recordkeeping lies with senior management. They must provide direction and support and ensure recordkeeping meets legislative and business requirements in their department.<br><br>Visible senior management commitment and support sets the expectation for staff to conduct business according to accepted standards of practice.<br><br>Responsibility for recordkeeping is cascaded down throughout the department, to various levels of management. | • Responsibility is identified in department strategies and policies.<br>• An executive lead is assigned by the Deputy Minister and this role is identified in recordkeeping strategies and projects.<br>• Recordkeeping is a regular agenda item in management committee meetings. |
| 1.2 Recordkeeping must be directed by department-focused strategy and policy. | Governance frameworks are critical to effective recordkeeping practices.<br><br>Departments must set a high-level strategy and internal policies for managing records and information in accordance with the ARA and the GRO's policies, standards, and guidelines. | • A departmental-wide directive on recordkeeping is adopted and communicated.<br>• Strategies and internal policies that align with GRO's government-wide policies are developed to support program areas. |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| 1.3 Departments must have skilled records management professionals. | Records management professionals are responsible for working with program managers and allied information professionals to lead or support such activities as records scheduling, development of records classification systems, analysis of recordkeeping requirements in business processes, design and implementation of records systems, and delivery of role-specific training.<br><br>A department must be able to access recordkeeping skills through recruitment, service providers, and by networking with other organizations. | • Departments have a recordkeeping professional.<br>• The role is identified in strategies and policies on recordkeeping and communicated throughout the organization.<br>• The responsibilities, skills, and capabilities are defined in job descriptions and performance plans.<br>• The recordkeeping expert is consulted in all business process transformation and system design projects.<br>• The recordkeeping expert is in regular contact with the GRO. |
| 1.4 Division, branch, and program area management must take responsibility for integrating recordkeeping into work processes, systems, and services. | This requirement places responsibilities more broadly within the department. It reflects a business manager's detailed understanding of the records and information produced by and necessary to perform their work, and their responsibility for ensuring its management.<br><br>Cascading responsibility to different business areas of the department lets business unit staff and records and information staff work together to ensure that recordkeeping is integrated into business processes, systems, and services.<br><br>Departments with strong capacity consider recordkeeping requirements in strategic, financial, and human resources planning; risk management; and the development of policies, programs, services and systems.<br><br>Business managers must be aware that recordkeeping requirements are needed when they move to a new service environment; develop new | • Responsibility is assigned and identified in a recordkeeping directive.<br>• Roles and responsibilities are understood.<br>• Recordkeeping requirements are considered upfront in any projects that impact physical or electronic records. |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | business processes, systems, or services; or improve on existing business processes, systems, or services (see Policy 2).<br><br>Business owners must demonstrate that they have considered recordkeeping requirements and assessed risks as part of the business development process. | |
| 1.5 All staff understand their recordkeeping responsibilities. | All staff, including contractors, must understand their recordkeeping responsibilities.<br><br>Policies, business rules, and procedures must include clear requirements for creating and managing records and information.<br><br>Roles and responsibilities for recordkeeping must be defined, assigned, and communicated throughout the department, so that those responsible have the authority required to carry out their duties and the appropriate position and expertise. These roles and responsibilities include:<br>• Senior managers, who have overall program responsibility and are expected to promote program compliance and allocate resources/funding (see 1.1).<br>• Records management professionals, who establish and implement policies, procedures, and standards (see 1.3).<br>• Program managers, who ensure that staff follow recordkeeping guidelines to create and keep records to document business processes (see 1.4).<br>• All staff, who must create and keep records in accordance with recordkeeping guidelines, policies, and procedures. | • The recordkeeping directive is communicated to all staff.<br>• Policies and procedures outline staff responsibilities.<br>• Orientation and training are tailored to the appropriate audience and support the department's recordkeeping responsibilities and goals. |
| 1.6 Contracts and agreements must consider recordkeeping requirements. | Corporate policy and strategy should include responsibilities for ensuring that records and information requirements are identified and met. Departments should undertake risk assessments and have recordkeeping issues addressed in any agreed upon contractual arrangements. | • Recordkeeping requirements have been analyzed and identified (see 2.1).<br>• Recordkeeping requirements have been incorporated into contracts, agreements, and |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | Departments must ensure that the portability of records and information and associated information about the records (metadata) is assessed and appropriately addressed in outsourcing and service contracts, instruments, and arrangements. | service arrangements in consultation with Legal Services and the GRO. |
| 1.7 Recordkeeping activities must be monitored and reviewed. | Policies alone will not guarantee good recordkeeping practices. Success requires active and visible support by senior management and a commitment to continuous improvement. | • All processes and systems are reviewed regularly to ensure they are meeting business requirements and recordkeeping best practices.<br>• Monitoring activities are documented. |

## Policy 2 – By design: Recordkeeping requirements are linked to business requirements

Recordkeeping is a corporate activity designed to ensure the systematic creation, maintenance, usability, and sustainability of records needed for business operations. Recordkeeping must be planned by management and linked to business requirements.

Program areas need to:

- analyze and define their key records and information requirements
- design and embed requirements into business processes and systems

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| 2.1 Records and information needed to support business must be identified and documented. | This requirement provides the foundation for managing records and information in all environments.<br><br>By analyzing and documenting functions and activities, each program area can identify what records and information it needs to support business.<br><br>Decisions on what records and information are required should be documented in business rules, policies, and procedures, and should also be | • Functions and activities of the department are analyzed to determine what records are required to document activities.<br>• Recordkeeping requirements are integrated into documented business rules. |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | incorporated in system specifications (see 2.3). The department must embody these decisions in records schedules (see 2.4). | • Up-to-date records schedules are in place and regularly reviewed. |
| 2.2 High-risk/high-value areas of business and the records and information needed to support them must be identified. | High-risk/high-value functions include those that:<br>• protect the rights and entitlements of citizens<br>• protect public safety or health<br>• collect and use sensitive personal information<br>• are subject to close scrutiny by the public or oversight bodies<br>• allocate or spend large amounts of money<br>• require long-term retention of records and information<br><br>By identifying high-value records and information at creation, a department can better manage and use these core assets. Better management can increase the value of information.<br><br>Departments must identify the potential risks to records and information and mange or mitigate them. This includes protecting the systems that manage records and information that are high-risk/high-value from loss and damage.<br><br>Departments should set up appropriate security measures and business continuity strategies and plans. | • Risks are identified, managed, or mitigated.<br>• Systems managing high-risk/high-value records are protected by business continuity strategies and plans. |
| 2.3 Recordkeeping must be an essential consideration in design of all systems. | It is important to build in recordkeeping requirements from the start (see Policy 3).<br><br>Where systems supporting high-risk/high-value records and information have not included recordkeeping requirements, mitigation strategies must be adopted. | • Systems specifications include recordkeeping requirements.<br>• Systems design and configuration is documented and maintained.<br><br>Systems that do not meet requirements:<br>• are identified<br>• risks are mitigated |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | | • are redesigned to include requirements. |
| 2.4 Records and information are managed comprehensively across all operating environments. | Regardless of format, records that relate to the same transaction, case, or business event/decision should be managed comprehensively, so that they can easily be identified, retrieved, or disposed of.<br><br>Records schedules are a basic mechanism for managing business records. They identify records held by government and provide an important inventory for planning, protecting, and providing access (see 3.6). Under *The Archives and Recordkeeping Act*, all government records must be scheduled, regardless of how long they need to be kept or what format they are in. | • Internal inventories, policies, procedures, and processes document where records are created and held, and in what form.<br>• Records schedules are prepared and approved. |
| 2.5 Recordkeeping is designed to safeguard records and information with long-term value. | This requirement ensures that the Archives of Manitoba can identify which systems and service environments hold records and information with long-term or archival value.<br><br>This requirement builds on requirements 2.1, 2.2 and 2.4 and works in conjunction with approved records schedules.<br><br>Records and information designated as having archival value must be safeguarded and managed appropriately over time to ensure authenticity, reliability, trustworthiness, and accessibility.<br><br>Permanent or long-term records and information will outlive the systems in which they currently reside and will also outlive outsourcing arrangements and contracts with service providers. Departments must ensure that they plan and manage the protection of permanent or long-term records and information through transitions of systems (system migration, conversion, and/or decommissioning) and changes to service arrangements (termination of services, new outsourcing arrangements). | • Program areas develop records schedules in conjunction with the Archives, in order to identify records with long-term value.<br>• Records are kept in accordance with approved records schedules. |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | Permanent and long-term records must also be protected during and after administration and machinery of government changes. This includes records and information that must be transferred between organizations, as well as records that may remain with the creating department. | |
| 2.6 Records and information requirements are maintained through systems and service transformations. | Rapid changes in information technology can leave critical business records and information inaccessible. Many government records need to be kept for longer than the expected lifespan of the systems they depend on. Ensuring continued access to electronic records requires inclusion of retention requirements in system design and a planned approach to migration.<br><br>A department must have documented migration strategies, and appropriate planning and testing processes. These must ensure that records and information are not 'left behind' or disposed of unlawfully.<br><br>A department must use a migration, conversion, and/or decommissioning process that ensures that records and information are kept for as long as needed. | • A migration strategy is implemented and regularly reviewed.<br>• The process of migrating or converting records, information, and metadata from one system to another is managed to ensure records remain trustworthy and accessible.<br>• The portability of records and information and associated metadata is addressed in outsourcing or service arrangements.<br>• The decommissioning of systems follows the requirements for disposing of records and information.<br>• System documentation is maintained. |

## Policy 3 – Management regime: Records and information are well managed

Effective recordkeeping is based on trustworthy and reliable records and information that are accessible, reliable, and maintained for as long as they are needed to meet business requirements. This extends to all formats, business environments, types of systems, and locations.

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| 3.1 Records and information must be created and managed as part of normal business activities. | Decisions about what records to create are business decisions that must be based on the requirements and obligations of the department and agency.<br><br>Policy, rules, and processes articulate and inform the department and its staff of the requirements and responsibilities for creation, capture, and management of records.<br><br>A department must identify, assess the risk, resolve or mitigate, and document any exceptions that affect the creation, integrity, accessibility, and usability of its records and information.<br><br>Staff and contractors must conform to policies, business rules, and procedures to ensure records and information are routinely created and managed. | • Policies, business rules, and procedures articulate staff requirements and responsibilities for the creation, capture, and management of records.<br>• Assessments or audits demonstrate that systems operate routinely.<br>• Exceptions to routine operations that affect information integrity, usability, or accessibility are identified, resolved, and documented. |
| 3.2 Records and information must be reliable and trustworthy. | A key purpose of records is to provide evidence of business activities. The value of records as evidence depends on the department's ability to demonstrate that the records have not been modified or altered.<br><br>Demonstrating this requirement is accomplished by ensuring that records have adequate descriptive information (metadata) to provide meaning and context, and that the metadata remains associated with the record. | • Systems are in place that create and capture adequate metadata.<br>• System audits test management controls of systems, including information integrity, reliability and trustworthiness. |
| 3.3 Records and information must be identifiable, retrievable, accessible, and usable. | A department must associate or link appropriate minimum metadata to records and information to ensure they can be identified, retrieved, and shared. | • Testing verifies that systems can locate and produce records and information that are viewable and understandable. |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| | To maintain the accessibility and usability of digital records and information, an organization must ensure it regularly migrates or moves records from one system or platform to another (see 2.5 and 2.6).<br><br>Departments must regularly test systems and perform assessments or audits to demonstrate that the systems can locate and produce records and information that can be read and understood.<br><br>To maintain the accessibility and usability of physical records and information, departments must keep them in appropriate storage areas and conditions. | • Appropriate minimum metadata is in place.<br>• Appropriate storage of physical records is deployed in the active phase (in office) and the Government Records Centre is used to store semi-active records. |
| 3.4 Records and information must be protected from unauthorized access, alteration, loss, deletion and/or destruction. | Records and information must be protected.<br><br>Clearly defined, documented, and distributed guidance and procedures are essential and the organization should implement appropriate security mechanisms.<br>Security measures should include:<br>• access and use permissions in systems<br>• processes to protect records and information no matter where they are located, including in transit and outside the workplace<br>• secure physical storage facilities<br><br>Undertaking regular assessments or audits will help a department verify that access controls have been implemented and are working. | • Information security and protection mechanisms are in place.<br>• Records and information are protected wherever they are located, including in transit, outside the workplace, and on removable storage media or mobile devices.<br>• Assessments or audits can test that access controls are implemented and maintained.<br>• Physical records are stored at the Government Records Centre when active business use has ceased. |
| 3.5 Access to, use, and sharing of records and information must be | Departments must ensure that access to, use, and sharing of records and information is in compliance with legal requirements such as *The Freedom of Information and Protection of Privacy Act*, *The Personal Health* | • Policies, business rules, and procedures identify how access, |

| Requirements | Explanation | Examples demonstrating compliance |
|---|---|---|
| managed appropriately, in line with legal and business requirements. | *Information Act*, *The Mental Health Act*, *The Child and Family Services Act*, *The Youth Criminal Justice Act,* etc.<br><br>Undertaking regular assessments or audits of systems will help departments verify that access to, use, and sharing of records and information is managed in accordance with business requirements and legal obligations. | use, and appropriate sharing of information are managed.<br>• Assessments and audits confirm access requirements. |
| 3.6 Records and information are kept for as long as needed for business, legal, and accountability requirements. | Records schedules are a basic mechanism for managing business records. They establish minimum retention periods and are required to authorize disposal of all government records. Records schedules should be regularly reviewed to ensure they reflect current recordkeeping arrangements and needs.<br><br>Records must be scheduled and disposed of according to the provisions of authorized records schedules. This includes records located in business systems, in outsourcing or service agreements, or in physical storage.<br><br>A department must implement policies, business rules, and procedures to ensure that records and information are kept for as long as required and in accordance with approved records schedules. | • Retention requirements are identified and reflected in up-to-date, approved records schedules.<br>• Policies, business rules, and procedures support retention requirements.<br>• Records that have been designated as archival are protected and maintained according to the provisions of approved records schedules and the direction of the Archivist of Manitoba (see 2.5). |
| 3.7 Records and information must be systematically disposed of when no longer required, and when authorized and legally appropriate to do so. | Records (physical and digital) must be disposed of in accordance with approved records schedules and Government Records Office policies and procedures. | • Disposal complies with authorized records schedules.<br>• GRO procedures and processes for disposal of records and information are followed.<br>• Disposal of records and information is documented. |

## Further information

For definitions of specific terms used in this policy, refer to the Glossary of Records and Information Management Terms.

To obtain a baseline and measure progress in meeting the policy requirements see Compass: A Capacity Assessment Tool for Recordkeeping.

## Version Control

| | |
|---|---|
| Initiated | July 2017 |
| Final Draft | February 2018 |
| Endorsed by the Archivist of Manitoba | April 2018 |
| Published | May 2018 |
| Revision Initiated | January 2024 |
| Version 2 Finalized | March 2024 |
| Endorsed by the Archivist of Manitoba | March 2024 |
| Published | March 2024 |

Government Records Office, Archives of Manitoba
T: 204-945-3971 | E: GRO@gov.mb.ca
Visit our website to learn more about Government Recordkeeping