

# Enterprise Information Management Handbook

*Revised December 2021*



## 0001 Table of Contents

Section	Title	Issued	Revised	Revoked
<b>0000</b>	<b>Introduction</b>			
0001	Table of Contents	July 2018	July 2021	
0002	About this Handbook	July 2018	July 2021	
0003	About Enterprise Information Management	Nov. 2018	Dec. 2021	
0004	Enterprise Information Management Service Catalogue	Dec. 2021		
0005	About Departmental Records and Information Management Programs	July 2021		
0006	About the Recorded Information Management Committee	July 2021		
0007	About the <i>Archives Act</i>	July 2021		
<b>1000</b>	<b>Recorded Information Management Policy Framework</b>			
1001	About the RIM Policy Framework	April 2019	July 2021	
1100	Recorded Information Management Policy	April 2019	July 2021	
1200	Management of Electronic Information Policy	April 2019	July 2021	
1220	Directive – Scheduling and Disposition of Electronic Mail Messages	April 2019	July 2021	
1221	Managing Electronic Mail Messages Guideline	April 2019	July 2021	
1230	Directive - Digitizing	April 2019	July 2021	
1231	Standard - Digitizing	April 2019	July 2021	
1232	Guideline - Digitization	April 2019	July 2021	
1300	Records Scheduling Policy	April 2019	July 2021	
1310	Administrative Records Standard	April 2019	July 2021	
1320	Operational Records Standard	April 2019	July 2021	
1321	ORCS Development Guidelines	April 2019	July 2021	
<b>2000</b>	<b>Enterprise Records Management</b>			
2001	About Enterprise Records Management	Jan. 2020	July 2021	

<b>Section</b>	<b>Title</b>	<b>Issued</b>	<b>Revised</b>	<b>Revoked</b>
2002	Agencies, Boards, Commissions, Crown Corporations, and other Branches of Government	Jan. 2020	Dec. 2021	
2100	Advice and Assistance Services	Jan. 2020	July 2021	
2200	Records Management Training Services	Jan. 2020	July 2021	
2400	Common Records Schedule Maintenance	Jan. 2020	July 2021	
2500	Agreement on Records with the Government of Nunavut	Jan. 2020	July 2021	
2600	Records Transfer Agreement with the Government of Canada	Jan. 2020	July 2021	
<b>3000</b>	<b>Enterprise Content Management</b>			
3001	About Enterprise Content Management	Jan. 2020	July 2021	
<b>4000</b>	<b>GNWT Records Centres</b>			
4001	About the GNWT Records Centres	July 2018	Dec. 2021	
4002	Records Centre Contact Information	July 2018	Dec. 2021	
4003	Transporting Files and Boxes	July 2018	Dec. 2021	
4100	Requirements for Accessing Records Centre Services	July 2018	Dec. 2021	
4110	Standard Box Sizes	July 2018	Dec. 2021	
4111	Damaged Boxes	July 2018	July 2021	
4200	Transfers to Storage	July 2018	Dec. 2021	
4210	Re-inventorying Boxes in Storage	Nov. 2018	July 2021	
4300	Retrievals from the Records Centres	Nov. 2018	July 2021	
4301	Retrieval of Records Approved for Disposition	April 2019	July 2021	
4310	Returning Files and Boxes	Nov. 2018	Dec. 2021	
4320	Permanent Returns	Nov. 2018	July 2021	
4321	Permanent Returns following a Records Centre Program Review	Nov. 2018	July 2021	
4330	Missing Files and Boxes	April 2019	Dec. 2021	
4400	Records Dispositions	July 2018	July 2021	
4410	Disposition of Physical Records	July 2018	Dec. 2021	

<b>Section</b>	<b>Title</b>	<b>Issued</b>	<b>Revised</b>	<b>Revoked</b>
4420	Disposal of Transitory Records in Paper and Other Media	April 2019	July 2021	
4430	Disposition Holds for Records Stored in the Records Centres	April 2019	July 2021	
<b>5000</b>	<b>Vital Records and Emergency Management</b>			
5001	About Vital or Essential Records	Jan. 2020	July 2021	
5501	About Emergency Management Planning for Records	Dec. 2021		
<b>6000</b>	<b>Electronic Records</b>			
6001	About Electronic Records	July 2021		
6100	Managing Electronic Records using DIIMS	July 2021		
6200	Managing Electronic Records on the Network Shared Drives	July 2021		
6400	Disposal of Electronic Records	July 2021		
6430	Disposition of Transitory Electronic Records	July 2021		
<b>7000</b>	<b>Paper Records and Other Media</b>			
7001	About Paper Records and Other Media	July 2021		
7100	Active Filing of Paper Records	July 2021		
7110	Filing Equipment and Supplies	July 2021		
7111	File Labels	July 2021		
7200	Closing Paper Files	July 2021		
7300	Managing Legacy Paper Records (Backlogs)	July 2021		
<b>8000-9000</b>	<b>Records and Information Management Related Topics</b>			
8100	Government Reorganization	Jan. 2020	July 2021	
8110	Division or Program Renamed	Jan. 2020	July 2021	
8120	Division or Program Moving to a New Department	Jan. 2020	July 2021	
8130	Departments Amalgamating or Merging	Jan. 2020	July 2021	
8140	Department Disbanded	Jan. 2020	July 2021	
8200	Ministers Records	Jan. 2020	July 2021	

<b>Section</b>	<b>Title</b>	<b>Issued</b>	<b>Revised</b>	<b>Revoked</b>
8300	Managing Government Records When Working Remotely	Apr. 2020	July 2021	
8310	Using Online Chat and Collaboration Tools	Apr. 2020	July 2021	
8311	Considerations for Online Meetings	July 2021		
8400	Naming Conventions and Titling Files	July 2021		
<b>Appendices</b>	<b>Appendices</b>			
Appendix A	Records Centre Label Placement	Jan. 2020	Dec. 2021	
Appendix B	Examples of Vital or Essential Records	Jan. 2020	July 2021	
Appendix C	Examples of Substantive and Transitory Records	July 2021		
Appendix D	Example Disaster Salvage and Recovery Workflow	Dec. 2021		
Appendix E	Glossary	July 2021	Dec. 2021	

## 0002 About this Handbook

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

This handbook is for Departmental Records Management Teams, supervisors, and employees. Its purpose is to support the GNWT's records and information management program. It describes the services offered by the Department of Infrastructure's Enterprise Information Management division and the steps to follow when using these services. It also provides guidance on the development and implementation of the GNWT's records and information management program.

Please send questions about the handbook to [Corporate\\_Records@gov.nt.ca](mailto:Corporate_Records@gov.nt.ca).

## 0003 About Enterprise Information Management

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

Enterprise Information Management (EIM) is a division within the Department of Infrastructure. Although located within the Department of Infrastructure, EIM has a reporting relationship with the GNWT's Chief Information Officer in the Department of Finance.

Enterprise Information Management is a shared services provider for the GNWT and is responsible for:

- The development and maintenance of the Recorded Information Management Policy and related policies and standards for the management of recorded information.
- The development of procedures and guidelines for the management of recorded information.
- The provision of advisory and training services.
- The development, operation, and maintenance of the shared systems and infrastructure used by government departments and agencies to manage their recorded information, such as the Digital Integrated Information Management System (DIIMS).
- Providing, with the Department of Infrastructure's regional offices, records storage, retrieval, and disposal services.

Service delivery is provided by EIM's two sections, Enterprise Records Management (ERM) and Enterprise Content Management (ECM).

#### 1.1 Benefits to the GNWT

Information is widely recognized as an important organizational asset. The GNWT realizes a number of benefits from centralizing the services that support the management of the information, these include:

- Economies of scale – by consolidating some of the GNWT's information management requirements, such as DIIMS licensing, records centre storage, and records

destruction services, economies of scale can be achieved leading to lower overall costs.

- Consistency across the government – centralizing service provision encourages the standardization of government information handling processes. This reduces the GNWT’s risk of information loss through mishandling or failure to apply appropriate security and controls to the information.
- Creation of centres of excellence – by consolidating information management services, the GNWT is able to create centres of excellence for document management and records management knowledge in order to support GNWT initiatives, programs, and services.

## 1.2 History

From its earliest days, the Government of the Northwest Territories has recognized the value of managing its information assets. EIM can trace its origins back to the Central Registry that was established by the GNWT in Sòmbak'è (Yellowknife) in 1967/68. In 1977 it evolved into the Records Management Unit. The services provided have evolved over time in response to the changing needs of the government. Records centre services have been provided since 1984.

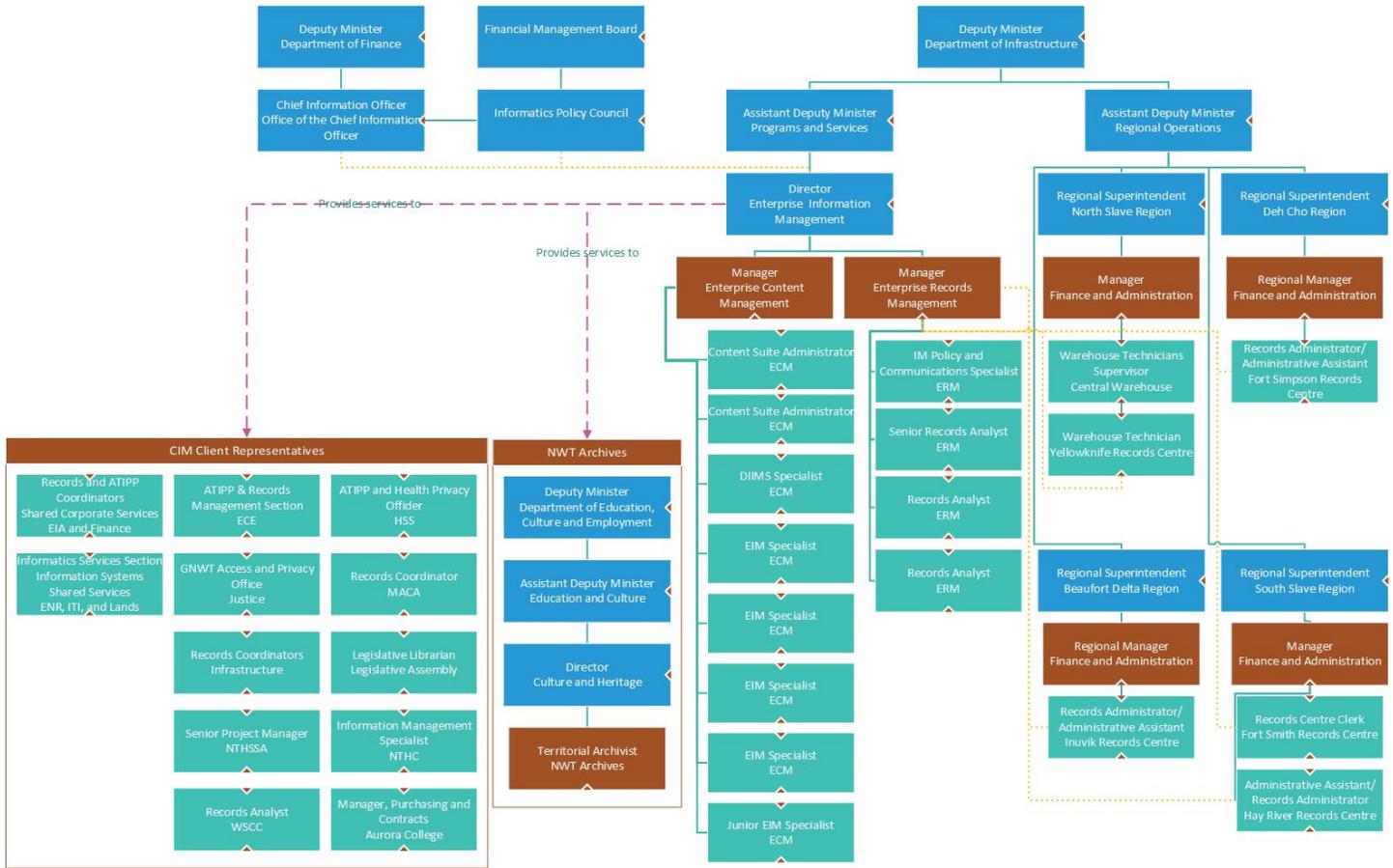
In 1998/99, the Records Management unit introduced iRIMS, which was an electronic records management system used by the records centres to manage boxes and by some departments and agencies to manage paper file folders. iRIMS also had some limited document management capabilities.

In 2011/12, the Records Management unit collaborated with the Office of the Chief Information Officer in a pilot of DIIMS, the GNWT’s Digital Integrated Information Management System. DIIMS combines content management and records management capabilities into a single software solution, replacing iRIMS. After the pilot, responsibility for further implementation of DIIMS, as well as system support and maintenance, was given to the Records Management unit. To accommodate the new responsibilities created by DIIMS, the Corporate Information Management division was created in 2014. The division was renamed Enterprise Information Management in 2021.

## 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

### 3. Organization and Relationships



## 0004 Enterprise Information Management Service Catalogue

<b>Issued:</b>	December 2021
<b>Last Updated:</b>	December 2021

### 1. Introduction

The Service Catalogue is an inventory of services performed by Enterprise Information Management (EIM). It includes a description of each service, information about who can access the service, and information on how to access the service.

EIM services are included in the [Information and Technology Services Portal](#), which is accessible via [Bear Net](#). A PDF copy of the Service Catalogue is available from EIM on request.

### 2. References

Enterprise Information Management Service Catalogue

## 0005 About Departmental Records and Information Management Programs

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Government departments and agencies are responsible and accountable for the management of records and information in their custody and under their control. The management of records must comply with the *Archives Act* and other applicable legislation. In addition, records and information management programs must conform to the *Recorded Information Management (RIM) Policy* and its related policies, standards, and guidelines.

Within this governance framework, departments and agencies develop records and information management programs to suit their individual needs and achieve their program objectives.

While each department or agency implements its own records management program, the programs share common features which support common principles. The guiding principles of a records management program are articulated in the *Generally Accepted Recordkeeping Principles* of Accountability, Transparency, Integrity, Protection, Compliance, Availability, Retention, and Disposition, as well as other foundational documents such as the Canadian General Standards Board and International Organization for Standardization records and information management standards.<sup>1</sup>

Enterprise Information Management (EIM) provides advice and support to departmental records and information management programs. It does not oversee or direct these programs.

This guidance is intended to identify potential components of government records management programs. Each department or agency may have a different mix of program components and may include some components which are not listed here.

### 2. References

Archives Act, R.S.N.W.T. 1988, c.A-6

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

---

<sup>1</sup> The GNWT has not formally adopted or endorsed the Principles or any other national or international standard; however, they are useful for articulating the universal goals of a records management program and for assessing records management programs.

Records Scheduling Policy, IMT Policy Manual

[Generally Accepted Recordkeeping Principles](#), ARMA International, 2017

CAN/CGSB 72.34-2017 Electronic records as documentary evidence

ISO 15489-1:2016 Information and documentation – Records management – Part 1: Concepts and principles

ISO 30300:2020 Information and documentation – Records management – Core concepts and vocabulary

ISO 30301:2019 Information and documentation – Management systems for records – Requirements

ISO 30302:2015 Information and documentation – Management systems for records – Guidelines for implementation

### **3. Guidelines - Accountability**

- 3.1 The department identifies a member of the senior management team, usually a director, who has overall responsibility for the records and information management program (RIM director). Ideally the senior management team acts as a steering committee to set priorities and address issues. The RIM director also liaises with CIM's management team as the customer of CIM's services and advises CIM of departmental requirements.
- 3.2 The department identifies at least one employee to work with the RIM director as part of a Department Records Management Team. The team members hold positions of trust. Department Records Management Team members necessarily have access to a considerable amount of highly confidential and personal information. Typical duties for the Department Records Management Team may include some or all of the following,
- Developing Operational Records Classification Systems (ORCS).
  - Coordinating or managing the implementation of the Administrative and Operational Records Classification Systems (ARCS and ORCS).
  - Developing records management procedures for the department.
  - Developing and delivering department-specific training in records management procedures and assisting supervisors in developing training plans for employees.
  - Coordinating the application of records retention and disposition schedules to the department's records with Enterprise Information Management.
  - Coordinating the creation and maintenance of records inventories.
  - Coordinating the transfer of paper records to the GNWT records centres operated by the Department of Infrastructure.
  - Monitoring retrievals of records from the records centres.

- Supporting the implementation and use of DIIMS within the department.<sup>2</sup>
- Monitoring and reporting to management on the use of DIIMS.
- Supporting the effective organization and use of network shared drives within the department, if applicable.
- Leading a departmental records management committee.
- Monitoring or assessing the departmental records management program and preparing recommendations for improvements.
- Acting as the primary point of contact with respect to records and information management issues and concerns for employees and management.
- Acting as the primary point of contact with the Enterprise Information Management division and the NWT Archives.
- Representing the department or agency on the interdepartmental Recorded Information Management Committee and other records and information management or DIIMS related committees and working groups.
- Regularly visiting headquarters and regional offices to provide training and support.
- Coordinating the transfer of custody and control over records due to re-organization or transfer of programs to another department or agency.

3.3 The department establishes an internal records management committee comprised of the RIM director, the Department Records Management Team, and representatives from each division and region. The purpose of this committee is to help organize the records management activities within the department and ensure consistency in records management practices between different divisions and regions.

Issues of concern for the committee include employee training, implementation and maintenance (clean-up) of filing systems and electronic folders in DIIMS or on network shared drives, setting priorities for the departmental records management program, participating in records management projects, and providing input into departmental procedures.

## 4. Guidelines - Transparency

4.1 The department creates a records management procedures manual, which addresses such topics as,

- The creation of records and files.
- Filing procedures.
- File naming conventions.
- The use of DIIMS or network shared drives.
- The use of DIIMS workflows.
- Records retrieval procedures.

---

<sup>2</sup> DIIMS stands for Digital Integrated Information Management System. DIIMS is an enterprise content management system used by the GNWT to manage electronic documents and paper records. It is maintained and supported by the Enterprise Information Management division of the Department of Infrastructure.

- Records sharing, distribution, and tracking procedures.
- Digitization procedures.
- Vital/essential records protection procedures.
- Procedures for the preservation of long-term records.
- Remote work procedures.
- The management of records posted to SharePoint and other collaboration tools in use in the department.

The procedures manual is a key component of the records management program and supports the authenticity and reliability of the records as evidence of government business.

## 5. Guidelines - Integrity

- 5.1 In compliance with the *Archives Act* and the *Records Scheduling Policy*, the Department Records Management Team prepares functional analysis and ORCS for all divisions and regions which require them.
- 5.2 In compliance with the *Records Scheduling Policy*, the Department Records Management Team reviews approved ORCS at least once every five years with the relevant program areas to confirm the ORCS is current and prepares amendments to the ORCS as required.
- 5.3 Paper files are classified and organized in filing cabinets based on the file classifications in ARCS and ORCS.
- 5.4 The ARCS and ORCS folder structure in DIIMS is used to save electronic records, including e-mail. The Department Records Management Team monitors and reports on the use of DIIMS by employees to the RIM director.<sup>3</sup>
- 5.5 Departments which have not implemented DIIMS organize their shared drives into folder hierarchies which reflect the file classification structure of ARCS and ORCS. The Department Records Management Team monitors and reports on the use of all network shared drives by employees to the RIM director. This could include monitoring duplication.

## 6. Guidelines - Security

- 6.1 The Department Records Management Team works with Enterprise Information Management to identify security groups and security requirements for DIIMS.
- 6.2 The Department Records Management Team provides the GNWT records centres with lists of employees who are authorized to retrieve records from the records centres and make sure those lists are kept up to date.
- 6.3 The department takes steps to ensure paper records are kept in secure locations which are inaccessible to the public or to those who do not have a need to know.

---

<sup>3</sup> DIIMS is the preferred solution for managing the government's electronic records. DIIMS reporting tools allow for reporting on use of the Enterprise and Personal workspaces, access and permissions, use of General folders, and records centre retrievals for boxes and volumes entered in DIIMS.

- 6.4 The department takes steps to protect electronic information, particularly when employees are working remotely.

## **7. Guidelines - Compliance**

- 7.1 The Department Records Management Team works with managers and supervisors across the department to identify employees who require records management training. This includes new employees and existing employees who may require “refresher” training or training on new procedures.

Ideally, employees are required to participate in annual records management training activities.

Training for most employees should cover the ownership of government records, creation and use of records, saving records, searching for records and records retrieval, using ARCS and ORCS, the identification and disposal of transitory records, and use of DIIMS.

- 7.2 The Department Records Management Team provides records management training to employees on department-specific records management procedures. This training is in addition to the GNWT-wide training provided by Enterprise Information Management.
- 7.3 The Department Records Management Team regularly visits all headquarters and regional offices to provide advice, guidance, and to review the state of the records management program.
- 7.4 The Department Records Management Team reports on compliance issues to the RIM director.
- 7.5 The department includes the general competency, [Attention to Detail](#), as an evaluation criterion in all performance evaluations.

## **8. Guidelines - Availability**

- 8.1 The department uses DIIMS to inventory or register all paper files from the moment they are created. DIIMS is used to manage paper records throughout their life cycle.

If a department does not use DIIMS to manage active paper files, it creates and maintains file inventories or file lists so that it is possible to locate and account for all of its physical records holdings.

File charge-out tools are used to keep track of the movement of physical records in an office.

- 8.2 The Department Records Management Team has access to all locations in DIIMS, all shared drives, and to online collaborative workspaces so they can effectively coordinate the management of the records.

## **9. Guidelines – Retention and Disposition**

- 9.1 The department designates appropriate storage equipment and locations for active paper records.

- 9.2 The department annually reviews paper and electronic records, and close records which have met their file closure criteria.
- 9.3 The department routinely transfers paper records to GNWT records centres for semi-active storage.
- 9.4 Directors and regional superintendents review the disposal of paper and electronic records, in accordance with the retention and disposition schedules in ARCS and ORCS and identify records which should be retained due to a current legal matter, audit, or access to information request.
- 9.5 Disposition holds are put in place for records which are subject to audits or a legal matter such as an investigation or lawsuit.
- 9.6 The department establishes projects to schedule unscheduled records stored in department office space and in the GNWT records centres.
- 9.7 The department establishes a strategy for the long-term preservation of records which it is required to keep for more than 10 years.

## 0006 About the Recorded Information Management Committee

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Recorded Information Management Committee (RIMC) is an interdepartmental committee established under the authority of the Informatics Policy Council (IPC).

The RIMC was established in 2002. New Terms of Reference were issued in 2021.

The RIMC's objectives include supporting Information Management and Technology governance; promoting the adoption of records management (RM) principles, standards, and best practices; working in collaboration to implement RM strategies and recommendations; assessing and analyzing RM opportunities; endorsing RM solutions; advocating for continued learning opportunities; and contributing to corporate reporting on RM.

The RIMC is chaired by the Manager, Enterprise Records Management, representing the Enterprise Information Management division in the Department of Infrastructure. The membership includes representatives from GNWT departments, the Northwest Territories Housing Corporation, the Northwest Territories Health and Social Services Authority, the Workers' Safety and Compensation Commission, the Northwest Territories Archives, and the Office of the Chief Information Officer.

The RIMC reports through the Director of Enterprise Information Management to the Chief Information Officer, who reports in turn to the Informatics Policy Council.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Informatics Policy Council, Financial Administration Manual Policy 115

Information Management and Technology (IMT) Governance Policy, IMT Policy Manual

Recorded Information Management Policy, IMT Policy Manual

Recorded Information Management Committee Terms of Reference, approved January 2021

## 0007 About the *Archives Act*

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

The *Archives Act* is the NWT legislation which supports the GNWT's records and information management program and governs the life cycle of the government's records. In addition to establishing the mandate for the NWT Archives, it:

- Provides a definition for a public record and a government body.
- Establishes the process for the transfer of public records which have archival value by government bodies to the custody and control of the NWT Archives.
- Prohibits the unauthorized destruction of public records. Government bodies can only destroy public records with the written approval of the Territorial Archivist.

The *Archives Regulations* provide further direction on the retention and disposal of public records and authorize government bodies to create plans for the preservation and disposal of public records. These plans, which are commonly referred to as Records Disposition Authorities, provide a classification system for identifying, categorizing, and organizing public records as well as a records retention and disposition schedule which outlines how long records will be kept and whether they will eventually be transferred to the NWT Archives or destroyed.

### 2. References

Archives Act, R.S.N.W.T. 1988, c.A-6

Archives Regulations, R-028-2008

Designation of Government Body Regulations, R-110-99

## **Recorded Information Management Policy Framework**

## 1001 About the Recorded Information Management Policy Framework

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

In 2002, the Informatics Policy Committee (IPC) issued a Knowledge Management Strategy for the GNWT. A number of records management and document management issues were brought up during the consultations on the strategy. The main issue was the need to set up a governance structure for records management in the GNWT. In response to these concerns, IPC created the Recorded Information Management Community of Interest (RIMCOI) and gave it the task of developing a records management policy framework.

RIMCOI developed the Recorded Information Management Policy. IPC approved the Policy in November 2002. RIMCOI also developed a Go Forward Plan. This plan listed other policies, standards, and guidelines that were required to guide the GNWT's records management program. The Corporate Records Management unit in the Department of Public Works and Services and the Recorded Information Management Committee completed the Go Forward Plan.

The Recorded Information Management policy framework has been incorporated into the Department of Finance's [Information Management and Technology \(IMT\) Policy Manual](#).

### 2. References

Financial Administration Act, S.N.W.T. 2015, c.13

Archives Act, R.S.N.W.T. 1988, c.A-6

Finance Establishment Policy, Executive Council Policy 15.00

Infrastructure Establishment Policy, Executive Council Policy 31.00

Education, Culture and Employment Establishment Policy, Executive Council Policy 71.00

Northwest Territories Archives, Executive Council Policy 71.06

Informatics Policy Council, Financial Administration Manual directive 115

IMT Policy Manual

### 3. Authority

- 3.1 The *Financial Administration Act* establishes the Financial Management Board (FMB). The Act assigns the FMB with responsibility for approving information management plans,

policies and strategies. FMB has delegated some of this responsibility to the Informatics Policy Council.

- 3.2 The Informatics Policy Council (IPC) is responsible for making sure that the GNWT's information and communications technology functions are compliant with strategies and policies.

IPC Policies apply to all departments and public agencies that operate within the GNWT's Data Communications Network.

- 3.3 The Office of the Chief Information Officer (OCIO) in the Department of Finance supports IPC. The OCIO leads the development and implementation of the information management and technology strategy and policy framework (IMT strategy). The Government Chief Information Officer has the authority to approve interpretation bulletins associated with the IMT strategy.

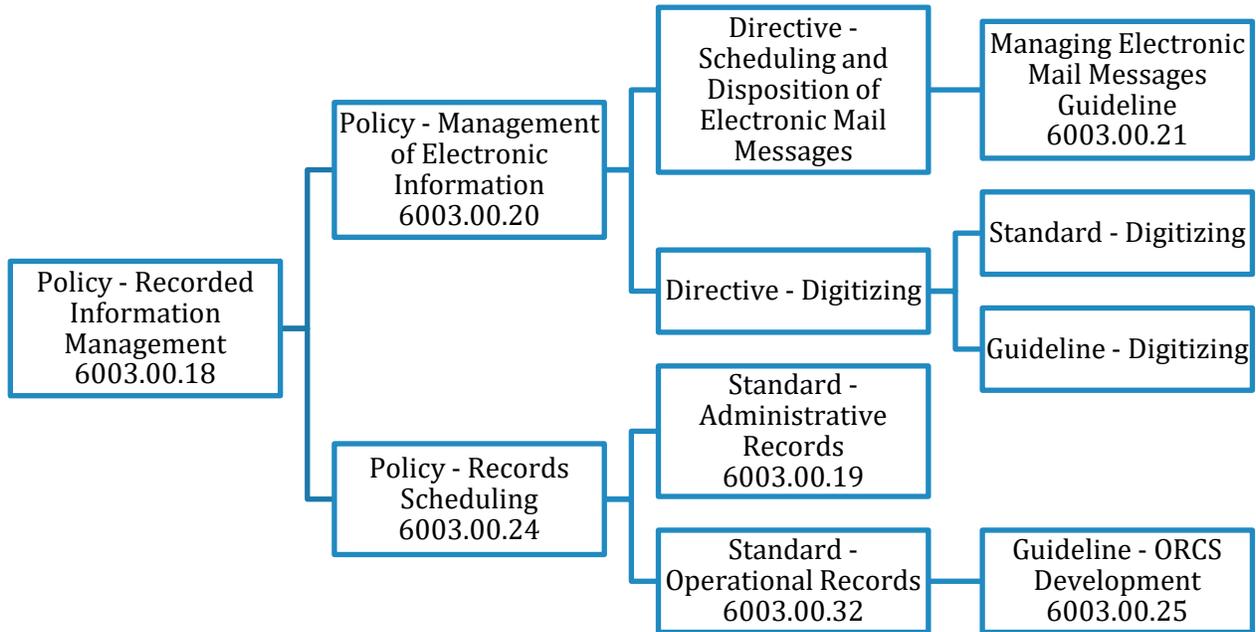
- 3.4 The Department of Infrastructure is responsible for developing policies and providing advice and assistance to support the management of the Government's recorded information.

- 3.5 The Recorded Information Management Committee (RIMC) is responsible for providing advice and recommendations to IPC on the management of recorded information. It is also a forum for discussing common records and information management issues. RIMC's members include representatives from Enterprise Information Management, NWT Archives, the Office of the Chief Information Officer, and each department and some public agencies. The Manager, Enterprise Records Management, is the chair of RIMC.

- 3.6 The Northwest Territories Archives is responsible for acquiring and preserving records that document the history of the GNWT. The Territorial Archivist has the authority to identify government records that have archival value and approve the disposal of the remainder.

- 3.7 Each department and agency is responsible for the management of the records and information in its custody or under its control, in compliance with GNWT-wide policies, directives, and standards.

#### 4. Overview of the RIM Policy Framework



## 1100 Recorded Information Management Policy

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Recorded Information Management Policy was approved by the Informatics Policy Committee in November 2002. Non-substantive changes to the policy were approved by the Informatics Policy Council in September 2018.

A copy of the policy may be accessed [here](#).

### 2. References

Recorded Information Management Policy, IMT Policy Manual

## 1200 Management of Electronic Information Policy

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Management of Electronic Information Policy was approved by the Informatics Policy Committee in May 2005. Non-substantive changes to the policy were approved by the Informatics Policy Council in September 2018.

A copy of the policy may be accessed [here](#).

### 2. References

Management of Electronic Information Policy, IMT Policy Manual

## 1220 Directive – Scheduling and Disposition of Electronic Mail Messages

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Directive – Scheduling and Disposition of Electronic Mail Messages was approved by the Chief Information Officer in February 2018.

A copy of the directive may be accessed [here](#).

### 2. References

Directive – Scheduling and Disposition of Electronic Mail Messages

## 1221 Managing Electronic Mail Messages Guideline

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Managing Electronic Mail Messages Guideline was approved by the Informatics Policy Committee in May 2005.

Contact Enterprise Information Management for a copy of the guidelines.

### 2. References

Managing Electronic Mail Messages Guideline

## 1230 Directive - Digitizing

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Directive - Digitizing was approved by the Chief Information Officer in November 2016. A revised version of the directive was approved in February 2019.

A copy of the directive may be accessed [here](#).

### 2. References

Directive - Digitizing

## 1231 Standard - Digitizing

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Standard - Digitizing was approved by the Chief Information Officer in February 2019.

A copy of the standard may be accessed [here](#).

The Checklist – Digitizing was developed as a reference resource. It summarizes the compliance requirements for a digitization program. A copy of the checklist is available [here](#).

### 2. References

Standard - Digitizing

## 1232 Guideline - Digitization

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Guideline - Digitization was approved by the Chief Information Officer in February 2019.

A copy of the guideline may be accessed [here](#).

### 2. References

Guideline - Digitization

## 1300 Records Scheduling Policy

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Records Scheduling Policy was approved by the Informatics Policy Committee in June 2007. Non-substantive changes to the policy were approved by the Informatics Policy Council in September 2018.

A copy of the policy may be accessed [here](#).

### 2. References

Records Scheduling Policy, IMT Policy Manual

## 1310 Administrative Records Standard

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Administrative Records Standard was approved by the Informatics Policy Committee in August 2004. Non-substantive changes to the policy were approved by the Informatics Policy Council in September 2018.

A copy of the standard may be accessed [here](#).

### 2. References

Administrative Records Standard, IMT Policy Manual

## 1320 Operational Records Standard

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Operational Records Standard was approved by the Informatics Policy Committee in June 2007. Non-substantive changes to the policy were approved by the Informatics Policy Council in September 2018.

A copy of the standard may be accessed [here](#).

### 2. References

Operational Records Standard

## 1321 ORCS Development Guideline

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The ORCS Development Guideline was approved by the Informatics Policy Committee in June 2007.

A copy of the guideline may be accessed [here](#).

### 2. References

ORCS Development Guideline, IMT Policy Manual

## **Enterprise Records Management**

## 2001 About Enterprise Records Management

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Enterprise Records Management (ERM) is a section of the Enterprise Information Management Division of the Department of Infrastructure. It looks after a number of government-wide records and information management programs and services which support the division's mandate.

Enterprise Records Management:

- Develops policies, standards, and guidelines.
- Provides advice and training services to departments.
- Develops government-wide common records disposition authorities.
- Reviews records disposition authorities developed by government bodies to confirm compliance with the Records Scheduling Policy and related standards and guidelines. ERM also reviews records disposition authorities to ensure that records retention schedules make reasonable use of the government's physical and electronic records storage capacity.
- Researches and evaluates innovations and industry trends.
- Provides, with the Department of Infrastructure's regional offices, secure records storage, retrieval, and disposal services for government records.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

## 2002 Agencies, Boards, Commissions, Crown Corporations, and Other Branches of Government

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	December 2021

### 1. Introduction

Enterprise Records Management (ERM) provides services to GNWT departments and to agencies, boards, commissions, and government corporations (ABCs) that are listed as government bodies in the *Regulations to the Archives Act*. ERM also provides services to the legislative and judicial branches of government which are exempt from the *Archives Act*.

### 2. References

Archives Regulations, R-026-2008

Infrastructure Establishment Policy, Executive Council Policy 31.00

### 3. Guidelines

- 3.1 ERM does not provide services directly to ABCs unless the ABC has a records management program in place. The ABC should have its own Records Management Team or be supported by the Department Records Management Team for a GNWT department.
- 3.2 Exceptions to Guideline 3.1 may be made due to historic arrangements with the Enterprise Records Management program.
  - 3.2.1 The Northwest Territories Health and Social Services Authority – Stanton Territorial Hospital may not transfer records which are classified and scheduled by RDA 2001-07 into storage in the GNWT records centres because RDA 2001-07 does not conform to the [ORCS Development Guideline](#) and the retention schedules cannot be implemented in the GNWT records centres.
  - 3.2.2 Aurora College is permitted work directly with ERM to transfer financial records out of the President's office in Tthebacha (Fort Smith) to a GNWT records centre. However, expansion of records centre services to other branches of Aurora College will only be possible if the College hires a full-time records coordinator or makes arrangements to use the services of ECE's Department Records Management Team.
  - 3.2.3 NWT Power Corporation may not transfer records which are classified and scheduled by RDA 2001-04 into storage in the GNWT records centres because RDA 2001-04 does not conform to the [ORCS Development Guideline](#) and the retention schedules cannot be implemented in the GNWT records centres.

- 3.3 Enterprise Records Management provides services to the Legislative Assembly of the Northwest Territories.
- 3.3.1 Elections NWT, the NWT Human Rights Commission, and other statutory officers of the Legislative Assembly are permitted to work directly with ERM to transfer records to a GNWT records centre.
- 3.4 Enterprise Records Management provides records services to the NWT Courts. The Courts must make arrangements to access records services through the Department Records Management Team for the Department of Justice.

## 2100 Advice and Assistance Services

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Enterprise Records Management section (ERM) provides advice and assistance on recorded information management issues to all government bodies. The advisory services promote consistency across government by providing a government-wide perspective on the management of records which then informs each government body's records and information management program.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

### 3. Guidelines

- 3.1 The Department Records Management Team for a government body is primarily responsible for managing the government body's specific records and information management program. ERM provide support to the Department Records Management Team and its managers and directors.
- 3.2 Where someone from a government body other than a member of the Department Records Management Team contacts ERM for advice and assistance, ERM will either refer the person to the Department Records Management Team or will answer the question and inform the Department Records Management Team that someone else from the department has been seeking advice from ERM.
- 3.4 Advice will be provided on the following:
- ORCS development
  - Records management program planning
  - ARCS and ORCS implementation planning
  - Departmental records management procedures
  - File classification
  - Creating and managing paper files
  - Creating and managing electronic records
  - Document scanning and imaging
  - Records centre transfer and disposition procedures
  - Records centre retrieval and permanent return procedures
  - Transfer of records between departments and agencies or between the GNWT and other governments
  - Disaster planning and recovery
  - Training
  - Records inventories and audits

- Other records and information management topics

#### **4. Procedures**

- 4.1 Advice may be given on the phone, by e-mail, or through in-person meetings.
- 4.2 E-mail inquiries should be directed to [Corporate\\_Records@gov.nt.ca](mailto:Corporate_Records@gov.nt.ca).

## 2200 Records Management Training Services

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Enterprise Records Management delivers a records management training program for GNWT employees. The purpose of the training program is to improve awareness and understanding of records and information management responsibilities and practices within the GNWT and to support the delivery of records management services in government bodies.

The Enterprise Records Management training program supports but does not replace training programs delivered by a government body's Department Records Management Team.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

### 3. Guidelines

- 3.1 Enterprise Records Management delivers online and in person records and information management training sessions, they include:
- [Part 1 of 3 – Records & Information Management Fundamentals](#)
  - [Part 2 of 3 – Using the Administrative & Operational Records Classification System](#)
  - [Part 3 of 3 – Records Transfers and Dispositions](#)
  - [Managing Information Management Programs](#)
  - [Introduction to the GNWT's Digitization Framework](#)
  - [DIIMS Records Classifier Training](#)
- 3.2 Most records management training is delivered through self-directed online training modules. Some training is delivered online as a live training event and in person.
- 3.3 Other GNWT-wide training may be developed from time-to-time when a requirement for new training is identified.
- 3.4 ERM may develop and/or deliver department-specific training or information sessions at the request of a client department. Requests for department-specific training will be considered on a case-by-case basis. Acceptance of the request will depend on a number of factors, including but not limited to ERM's workload, the state of ORCS development in the government body, the amount of post-training support that the records coordinator can provide, and the priorities of the Enterprise Information Management division.

- 3.5 Copies of training materials will be provided to Department Records Management Teams upon request. They are free to use or modify ERM training materials to suit their in-house training needs.
- 3.6 Registration for training sessions will be handled through the Department of Finance Learning and Development Catalogue (<https://my.hr.gov.nt.ca/learning-development/catalogue>).

#### **4. Procedures**

- 4.1 The Enterprise Records Management team will assess training needs based on feedback from course participants and Department Records Management Teams. They will develop or revise training sessions accordingly.
- 4.2 The Manager, Enterprise Records Management will determine the training schedule.
- 4.3 The ERM team member responsible for each training session will prepare course materials and send out reminders to course participants.
- 4.4 Class attendance will be kept and updated in the HR Training Calendar, as per the HR Training Calendar procedures manual.

## 2400 Common Records Schedule Maintenance

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Enterprise Records Management (ERM) looks after the development, maintenance, and coordination of approval of records disposition authorities for use by all government departments and agencies. Common Records Disposition Authorities include, but are not limited to, the GNWT Administrative Records Classification System (ARCS), the Transitory Records Schedule, and the Converted Source Analogue Records Schedule.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

Administrative Records Standard, IMT Policy Manual

### 3. Guidelines

3.1 ERM develops and maintains Common RDAs on the behalf of other government bodies.

3.2 A Common RDA or an amendment to a Common RDA is in force and takes effect when it is signed by the Territorial Archivist.

3.3 A Common RDA or an amendment to a Common RDA is approved for use and may be implemented within a government body when it is signed by the Deputy Head or equivalent.

### 4. Procedures

4.1 ERM initiates and manages projects to develop new or amend existing Common RDAs.

4.2 ERM determines the scope of the new Common RDA or an amendment based on comments received from Department Records Management Teams, the NWT Archives, and the creators of common records.

4.3 ERM researches recordkeeping requirements and drafts the new or amended Common RDA based on the research. ERM may form working groups comprised of representatives from Department Records Management Teams, the NWT Archives, and others, as well as ERM records analysts to assist with researching and writing new or amended Common RDAs.

- 4.4 Common RDAs are reviewed by the NWT Archives to identify requirements for records having historical value.
- 4.5 Common RDAs are reviewed and endorsed by the Recorded Information Management Committee (RIMC).
- 4.6 Common RDAs come into force when they are approved by the Territorial Archivist.
- 4.7 Common RDAs are approved for use within each government body when they are approved by the Deputy Head or equivalent.

## 2500 Agreement on Records with the Government of Nunavut

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

In 1999 the Government of the Northwest Territories signed an agreement with the future Government of Nunavut to provide for the smooth transfer of records from the GNWT to the new territory. The Government of Nunavut (GN) required these records in order to deliver services which were previously delivered by the GNWT. The separation of Nunavut from the Northwest Territories was known as “Division.”

The agreement had several provisions:

- The GNWT would transfer records pertaining to Nunavut to the GN upon receiving a request for the records from Nunavut.
- On April 1, 1999, all records situated within Nunavut would automatically transfer to the GN unless they were specifically excluded from the agreement.
- The GN would take on any contractual or other obligations associated with the records transferred to it.
- The GN would notify the GNWT of any access to information requests made for confidential records transferred to the GN.
- The GNWT could determine if it would transfer original records or copies to the GN.
- Each government must notify the other if it is going to destroy records created before April 1, 1999 and the other government has the opportunity to review or acquire the records.
- In all cases, costs are born by the government receiving the records.

In the GNWT, the agreement applies to records held by all departments, and some boards, agencies, commissions, and crown corporations. The GNWT is not obliged to transfer the following records:

- Records relating exclusively to the NWT.
- Vital Statistics Records.
- Adoption records.
- Cabinet confidence records.
- Information forming parts of libraries.

A copy of the agreement can be requested from Enterprise Records Management.

## **2. References**

Nunavut Act (Canada)

Agreement on records between the Government of the Northwest Territories and the Government of Nunavut

## **3. Guidelines**

- 3.1 The transfer of active pre-Division records held in departmental office space is the responsibility of the department which currently holds the records. The Manager, Enterprise Records Management may assist departments which find pre-Division records which pertain to Nunavut by connecting the department with the records management program in the GN.
- 3.2 Enterprise Records Management coordinates the offer of GNWT records to the GN when pre-Division records are ready for disposal as part of the records disposition process for paper records.
- 3.3 Electronic records which date from before Division are transitory copies of the master paper records and may be disposed of without being offered to the GN.
- 3.4 Enterprise Records Management coordinates the offer of GN records to the GNWT when the GN is going to destroy pre-Division records.

## 2600 Records Transfer Agreement with the Government of Canada

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

In 2014 the Government of the Northwest Territories (GNWT) signed an agreement with the Government of Canada to provide for the smooth transfer of records relating to the devolution of responsibility over land and resources from the Government of Canada to the GNWT. The Government of the Northwest Territories required these records in order to deliver services which were previously delivered by the Government of Canada.

The agreement had several provisions:

- Canada would transfer records relating to the management of land and resources to the GNWT.
- In most cases, Canada would provide copies of records, but for certain types of records, Canada would transfer the original records to the GNWT.
- Records would be transferred in either hard copy or electronic formats.
- Each government may request a copy of any record relating to the devolved responsibilities over land and resources from the other government.

### 2. References

Northwest Territories Devolution Act (Canada)

Northwest Territories Lands and Resources Devolution Agreement

### 3. Guidelines

- 3.1 Requests for records relating to devolved land and resources programs should be submitted to Enterprise Records Management. Enterprise Records Management will coordinate the transfer of the records with the Government of Canada.

# **Enterprise Content Management**

## 3001 About Enterprise Content Management

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Enterprise Content Management (ECM) is a section of the Enterprise Information Management Division of the Department of Infrastructure. It looks after a number of government-wide records and information management programs and services which support the division's mandate.

Enterprise Content Management:

- Operates and maintains DIIMS, the GNWT's document management and electronic records management system. DIIMS stands for Digital Integrated Information Management System.
- Provides project management, document migration, and communications, training, and support services for departments to implement DIIMS.
- Operates a DIIMS Support Desk.
- Provides advice and training services to departments.
- Provides reporting, collaboration, and workflow solutions.
- Supports the management of electronic and hard copy records through their life cycle.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

DIIMS End User Guide

## **GNWT Records Centres**

## 4001 About the GNWT Records Centres

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The Department of Infrastructure provides records storage, retrieval, and disposal services on behalf of GNWT departments and some agencies.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 There are five GNWT records centres, located in Łíídlı Kúé (Fort Simpson), Tthebacha (Fort Smith), Xátł'odehchee (Hay River), Inuvik (Inuvik) , and Sòmbak'è (Yellowknife).
- 3.2 The records centres are staffed and operated by the Department of Infrastructure's regional offices.
- 3.3 Records centre services include storage of boxes of records that are in the semi-active phase of their life cycle; retrieval of files and boxes from storage; disposal of records that have reached the final disposition stage of their life cycle.
- 3.4 Enterprise Records Management establishes procedures for the records centres.

## 4002 Records Centre Contact Information

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The Department of Infrastructure provides records storage, retrieval, and disposal services on behalf of GNWT departments and some agencies.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

3.1 Each records centre is maintained by an employee in the Department of Infrastructure's regional offices. The records centres may be contacted via the following e-mail addresses:

- Łíídlı Kúé (Fort Simpson): FortSimpson\_Records@gov.nt.ca
- Tthebacha (Fort Smith): FortSmith\_Records@gov.nt.ca
- Xátł'odehchee (Hay River): HayRiver\_Records@gov.nt.ca
- Inuvik (Inuvik): Inuvik\_Records@gov.nt.ca
- Sòmbak'è (Yellowknife): records\_management@gov.nt.ca

3.2 The records centre administrators may be contacted using the above e-mail addresses in order to request the retrieval of files not entered in DIIMS and to arrange delivery and pick-up of files and boxes that have been accepted by Enterprise Records Management (ERM) for storage or disposal.

Retrieval requests for boxes and files (volumes) entered into DIIMS should be made through DIIMS.

All other correspondence related to the records centres should be directed to ERM at Corporate\_Records@gov.nt.ca.

## 4003 Transporting Files and Boxes

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

Government records contain confidential and personal information that must be protected from unauthorized access and disclosure. Appropriate safeguards must be in place to protect information when transporting files or boxes containing government records to and from the GNWT records centres.

### 2. References

Government of the Northwest Territories, Information Security Awareness Training (<https://my.hr.gov.nt.ca/courses/information-security-awareness-training>)

Workers' Safety and Compensation Commission, Hazard Alert – Lifting Injuries (<http://www.wscc.nt.ca/documents/lifting-injuries>)

### 3. Guidelines

- 3.1 GNWT departments and agencies are responsible for any files or boxes containing government records that are being transported to a GNWT records centre until the records are delivered to the records centre and accepted by the records centre administrator. The records centres and Enterprise Records Management (ERM) are not responsible for any damage or unauthorized disclosure that may occur prior to or in transit.
- 3.2 Departments and agencies should clearly identify boxes of government records that are awaiting transport to the records centres. The boxes awaiting transport should be isolated from boxes not being transferred to the records centres.
- 3.3 Moving and courier contractors who are hired to transport files or boxes containing government records between departmental offices and the records centre should be bonded and be able to pass a criminal records check. If a suitable contractor is not available in the community, then government employees may be required to deliver or pick up files or boxes of files in person.
  - 3.3.1 In Sòmbak'è (Yellowknife), the Department of Infrastructure's North Slave Regional Office has contracted a moving company to deliver boxes of records and surplus furniture between government offices and the Central Warehouse. ERM records analysts arrange with the Central Warehouse to have transfers to the records centre picked up by the contractor. This service is not available in other communities.

- 3.4 Internal mail is not recommended for transporting files that contain confidential or personal information between government offices and the records centres because the chain of custody is not tracked.
- 3.5 When shipping files and boxes containing government records between communities by all weather or winter road, boxes should be taped shut with a single strip of tape, placed on pallets, and shrink wrapped. The truck should be locked, and it should be sealed if possible. The moving contractor should transport the boxes from the originating office to the records centre directly, without making any additional stops. If it is necessary to store the boxes overnight before delivering them at the records centre, the boxes must be stored in a secure, locked facility, where they will be protected from potential water, insect, or rodent damage.
- 3.6 When shipping boxes of government records between Tłegóhtı (Norman Wells) and Inuvik (Inuvik) by water, boxes should be taped shut with a single strip of tape, placed on pallets, and shrink wrapped. The originating department is responsible for hiring a transportation provider, such as the Department of Infrastructure's Marine Transportation Service (MTS), to ship the boxes. The originating department is also responsible for arranging transportation between the government office space, the shipping facilities, and the records centre. If it is necessary to store the boxes overnight before delivering them at the records centre, the boxes must be stored in a secure, locked facility, where they will be protected from potential water, insect, or rodent damage.
- 3.7 Safe lifting practices should be observed when handling boxes of files. Dollies or carts should be used to transport boxes to and from vehicles and within buildings. Avoid carrying more than one box at a time.

## 4100 Requirements for Accessing Records Centre Services

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

To offer the best possible service, the Department of Infrastructure has several requirements for how boxes containing government records are packed, inventoried, and shipped. Boxes that do not meet these requirements will be returned to the department that owns them at that department's expense.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Government records must be packed in standard storage boxes purchased from the Department of Infrastructure's Central Warehouse. See *4110 Standard Box Sizes* in this handbook for more information.
- 3.2 The files and boxes must be in good shape and labeled. Boxes that are not in good shape will not fit properly on records centre shelves and may pose a health and safety hazard to records centre personnel.
  - ✓ There should be no signs of water, mould, insect, or rodent damage.
  - ✓ The boxes should not be damaged or deformed.
  - ✓ The lids or flaps on the boxes must close completely and lie flat. The tops of the boxes must not bulge.
  - ✓ The bottoms of the Small Rec/Ship Boxes must be taped shut. It is not necessary to seal the bottom or sides of the ARC File Boxes used in the Yellowknife Records Centre as this style of box is designed to hold together without tape.
  - ✓ The lids or flaps on the boxes may be sealed with a single strip of packing tape for security purposes.
    - Tape should not cover the barcodes on the box labels because this makes it difficult to scan the barcodes.
    - It is not necessary to use multiple strips of tape to seal the boxes unless the boxes are being shipped between communities.
    - Tape may be removed by records centre personnel on receipt of the boxes or when retrieving records.

- ✓ Map tubes may be sealed with a plastic cap, or a piece of paper or cardboard taped over the end if they do not have flaps that can be closed.
- ✓ The boxes should not weigh more than 15 kg (33 lbs) but they should be mostly full.
- ✓ All boxes should have a barcoded box label attached. See section 3.7 below for more information about the labels and *Appendix A – Records Centre Label Placement* for proper placement of labels for each records centre.
  - The text on the label must be clear. Poorly printed barcodes cannot be read by the records centre's barcode scanner.
  - Labels must have the Box ID, Temp ID, and Transfer ID, and barcodes clearly visible.
- ✓ Boxes should not have content descriptions written on or taped to the outside of the box as this poses a security risk.
- ✓ Sticky notes and other papers should not be attached to the boxes. They may be removed by records centre personnel on receipt.
- ✓ Documents must be in file folders or other containers. It is recommended that papers be removed from binders and placed into file folders before packing the boxes. Loose papers are difficult to retrieve and binders are difficult to process for disposal.
- ✓ File folders should be placed upright with their spines on the bottom of the box. It is difficult to retrieve files that are lying on their side.
- ✓ File folders should not be bound with elastic bands, binder clips, string, etc.
- ✓ File folders should not be tightly packed. Records centre personnel must have room in the box to be able to remove a file from the box by hand.
- ✓ All the files in a box must have the same final disposition (destroy (D) or archival selection (AS/D)).
- ✓ All the files in a box should have the same closed date, retention period, and final disposition date. When reviewing records for transfer to the records centre, Enterprise Records Management (ERM) records analysts will look at the date ranges of the records in the boxes.
  - The ERM records analyst will accept boxes that have a range of closed dates and retention periods into storage in the records centres as long as all of the files in a box are eligible for storage and reach final disposition within five years of each other.
  - The ERM records analyst will accept boxes that have a range of closed dates and retention periods for final disposition if all the files in the box have reached their final disposition stage.

3.3 Each individual file folder or volume in each box must be inventoried. If a file has more than one volume, each volume must be inventoried separately. Failure to inventory all volumes may result in records being lost.

ERM **recommends using DIIMS** to inventory paper files or volumes and assign them to boxes. DIIMS provides better tools for file retrieval and tracking. This reduces the risk of losing information assets. See the [DIIMS Records Classifier Guide](#) for instructions on how to inventory boxes using DIIMS.

If DIIMS is not chosen as an option for inventorying the boxes, a [Box Inventory Form](#) may be used. See the [Box Inventory Form Procedures – Excel Version](#) for information on how to complete the form.

Use a single method for inventorying all the boxes in a transfer. Do not mix boxes that were inventoried using the Box Inventory Forms with boxes that have volumes assigned to them in DIIMS in the same transfer.

- 3.4 A copy of the appropriate **DIIMS Box Inventory Report** or the **Box Inventory Form** should be placed inside each box.
- 3.5 Each box must be entered into DIIMS, the GNWT's electronic records and document management system, and assigned to a transfer.<sup>1</sup>

The boxes in a transfer must be assigned consecutive temporary box numbers (Temp. Box ID); i.e. 01, 02, 03, 04, etc. Each new transfer must start with box number 01. There is no minimum or maximum size for a transfer.

- 3.6 All the boxes in a transfer must be in the same stage of their life cycle. Transfers should be sorted as follows:
- ✓ All the boxes are eligible for semi-active storage in the records centre; or
  - ✓ All the boxes are ready to be transferred to the NWT Archives immediately (final disposition of AS/D); or
  - ✓ All the boxes are ready to be destroyed immediately (final disposition of D).
- 3.7 Each box must have a DIIMS generated [GNWT Box Label](#) attached to it, printed on Avery 5163 or equivalent label stock.<sup>2</sup>
- ✓ Department personnel must take care to ensure that the correct label is attached to the correct box. The label must have the transfer ID on it. See the *DIIMS Records Classifier Guide* for instructions on how to print box labels.
  - ✓ The printing on the label must be clearly visible. Poorly printed labels cannot be scanned using the records centre barcode reader.
  - ✓ The label must display the Transfer ID, DIIMS Box ID, and Transfer ID in addition to the barcode.
  - ✓ Labels should not be placed over top of packing tape as they may fall off.

---

<sup>1</sup> ERM will enter boxes into DIIMS for public agencies that do not have access to DIIMS because they are outside the GNWT network.

<sup>2</sup> ERM will provide GNWT Box Labels to public agencies that do not have access to DIIMS because they are outside the GNWT network.

- ✓ If it appears that the labels are not sticking to the boxes, glue the labels to the boxes. Taping the labels to the boxes is not recommended. Tape dries out over time and may peel off. Tape may also make the labels and barcodes difficult to read or scan.
  - ✓ Labels must be placed in one of the following locations, based on the type of box and which records centre will be receiving the boxes. This placement is required so that the label is visible when the box is placed on the shelf. Placing labels in the same location improves retrieval times and facilitates records centre audits. See *Appendix A* for the correct label placement.
    - ARC File Boxes, Small Rec/Ship Boxes, and cheque boxes:
      - **Tthebacha, Xátl'odehchee, and Sòmbak'è** (Fort Smith, Hay River, and Yellowknife) – place the label in the lower right corner of the smaller side (short side) of the box.
      - **Łíídlı Kúé and Inuvik** (Fort Simpson and Inuvik) – place the label in the lower right corner of the larger side (long side) of the box.
    - Map Tubes:
      - Box labels are placed over on the flaps at one end of the tube. They should be taped on to secure them. Place the label on the long side of the tube if the tube does not have a flap and was sealed by taping a piece of paper or cardboard over the end.
      - Drawing labels may be placed along the long side of the tube.
- 3.8 Each transfer of boxes must be accompanied by a completed [Records Transfer Slip](#) (DIIMS link).
- 3.9 Each transfer must be submitted to ERM by the Department Records Management Team. Transfer requests should be e-mailed to [Corporate.Records@gov.nt.ca](mailto:Corporate.Records@gov.nt.ca). ERM prefers to receive one transfer request per e-mail message.
- 3.10 Each transfer must be reviewed and accepted by an ERM records analyst.
- 3.11 For complete procedures on transfers to storage, see *4200 Transfers to Storage*. For complete procedures on dispositions, see *4400 Records Dispositions* and *4410 Disposition of Physical Records*.

## 4110 Standard Box Sizes

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The GNWT Records Centres can only accommodate certain sized boxes. These boxes are to be purchased from the Department of Infrastructure's Warehouse and Surplus Services section, which is part of the North Slave Regional Office.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Inventories – Warehousing, Interpretation Bulletin, Financial Administration Manual 505.01

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Boxes that do not meet the required specifications will be returned to the originating department because they do not fit on the records centres shelves. Standard boxes are required for both transfers to storage and transfers for disposition.

Some of the current stock of Square Tube Boxes (map tubes) does not have flaps that can be used to close the boxes. The tubes can be closed with plastic caps which departments must purchase from an external supplier. If appropriate caps cannot be located, departments may seal the boxes with a piece of cardboard or paper taped over the ends.

Warehouse Stock Item Number	SAM Item Number	Description	Notes
22721	W22721	Small Rec/Ship Box 15½" x 11¼" x 10"	This box is accepted in the Łíídlı Kúé, Tthebacha, Xátł'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik) records centres.
22821	W22821	ARC File Box 15½" x 11½" x 10"	This box is only accepted in the Sòmbak'è (Yellowknife) records centre.
224430	W224430	Square Tube Box 4" x 4" x 30"	This map tube is accepted in the Tthebacha, Xátł'odehchee, Inuvik, and Sòmbak'è (Fort Smith, Hay River, Inuvik, and Yellowknife) records centres.

Warehouse Stock Item Number	SAM Item Number	Description	Notes
224436	W224436	Square Tube Box 4" x 4" x 36"	This map tube is accepted in the Tthebacha, Xátł'odehchee, Inuvik, and Sòmbak'è (Fort Smith, Hay River, Inuvik, and Yellowknife) records centres.
226630	W226630	Square Tube Box 6" x 6" x 30"	This map tube is accepted in the Tthebacha, Xátł'odehchee, Inuvik, and Sòmbak'è (Fort Smith, Hay River, Inuvik, and Yellowknife) records centres.
226636	W226636	Square Tube Box 6" x 6" x 36"	This map tube is accepted in the Tthebacha, Xátł'odehchee, Inuvik, and Sòmbak'è (Fort Smith, Hay River, Inuvik, and Yellowknife) records centres.
		Cheque boxes 9½" x 24" x 4½"	This box is only accepted in the Sòmbak'è (Yellowknife) records centre. Purchase at office supply stores.

#### 4. Procedures

- 4.1 Order boxes several weeks before they will be required. The Department of Infrastructure cannot guarantee there will always be stocks of boxes on hand.
- 4.2 Look up the boxes in the [GNWT Warehouse Catalogue](#) to ensure that the required boxes are in stock and to verify the current price. The Catalogue is available internally to GNWT departments.
- 4.3 Go to the [Internal Services](#) website. You may be required to set up or update your account information. This site is available internally to GNWT departments.
- 4.4 Select Requisitions – Requisition of Warehouse Stocked Items.
- 4.5 Complete the SAM user fields.
- 4.6 Select the items to be ordered and the quantity and complete the shipping information.
- 4.7 Place the order and print a copy of the order form. The order form must be signed by someone with spending authority and the funds must be committed in SAM before the items will be released.
- 4.8 Agencies, boards, commissions, and corporations which do not use SAM or cannot access the Internal Services site can submit a purchase order (PO) to [ykwarehouse@gov.nt.ca](mailto:ykwarehouse@gov.nt.ca).
- 4.9 Questions regarding purchasing of stocked items may be directed to the Warehouse Supervisor at (867) 767-9049 ext. 32176.

## 4111 Damaged Boxes

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

The GNWT records centres only accept boxes containing government records that are in good condition. Boxes that are not in good shape will not fit properly on records centre shelves and may pose a health and safety hazard to the records centre administrators.

Boxes that are not in good condition will be returned to the originating department at that department's expense.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 The records centre administrator will inspect the condition of the boxes to ensure that they meet the records centre requirements.
- 3.2 The records centre administrator will notify Enterprise Records Management of any issues with the boxes.
- 3.3 Enterprise Records Management will work with the Department Records Management Team and the records centre administrator to arrange the return of the boxes to the originating department.

### 4. Procedures

- 4.1 The records centre administrator will inspect the condition of the boxes upon receipt in the records centre loading area.
- 4.2 Boxes that are in good shape and that meet records centre requirements will be accepted into the records centre for storage or disposal, as appropriate. See *4100 Requirements for Accessing Records Centre Services*.
- 4.3 The records centre administrator will notify Enterprise Records Management of any issues with the boxes.
  - 4.3.1 The records centre administrator may open some boxes to determine the extent of any water, insect, or rodent damage.

- 4.3.2 The records centre administrator may take preventative measures and seal the boxes in plastic bags to prevent the spread of mould or pests.
- 4.4 The records analyst from Enterprise Records Management will notify the Department Records Management Team that there are issues with the boxes and explain that the boxes will be returned to the department.
- 4.5 The records centre administrator will return the boxes to the originating department. If the boxes have been shipped to the records centre from another community they will be returned to the nearest office belonging to the originating department.

## 4200 Transfers to Storage

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The GNWT records centres provide storage and retrieval services for semi-active records belonging to government departments and some agencies.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

3.1 In order to be accepted for transfer into storage, files in each box must:

- Be closed (i.e. no additional paper will be added to them);
- Have reached the semi-active stage in their life cycle; and
- Be scheduled by an approved Records Disposition Authority (RDA), such as the GNWT Administrative Records Classification System (ARCS), an Operational Records Classification System (ORCS), or a One-Time Schedule.

3.2 To be accepted for transfer into storage, the boxes must meet the records centre requirements. See *4100 Requirements for Accessing Records Centre Services*.

3.3 Files that have reached the end of their semi-active period at the time of transfer or that have a semi-active period of Nil (zero years) will not be accepted into storage in the records centre.

3.4 Unscheduled records (records that are not classified and scheduled by an approved RDA) and transitory records will not be accepted for storage in the records centre.

3.5 Copies of records centre forms and procedures for completing the forms are available on the Department of Infrastructure's website, <https://www.inf.gov.nt.ca/en/services/corporate-information-management/legislation-policies-procedures-and-guidelines>.

3.6 The following service standards apply:

- **Sòmbak'è (Yellowknife):**
  - Boxes will be picked up every second Wednesday by a moving contractor hired by the Department of Infrastructure's North Slave Regional Office. Contact [Corporate\\_Records@gov.nt.ca](mailto:Corporate_Records@gov.nt.ca) for a copy of the schedule. If there is a priority move of surplus furniture, then the pick-up date will be moved to Thursday.
  - Transfer requests must be received by the Wednesday before the pick-up date to ensure that Enterprise Records Management has time to review and process the requests.
- **All Records Centres**
  - Boxes will be shelved, and box location information will be uploaded to DIIMS within 24 hours of receipt of the boxes or as soon as possible.

#### 4. Procedures

4.1 Pack files into boxes. Make sure that the boxes comply with the records centre requirements. See *4100 Requirements for Accessing Records Centre Services*.

4.2 Enter the boxes into DIIMS and assign them to a collection. Instructions on how to enter boxes and create collections are available in the [DIIMS Records Classifier Guide](#).

Assign the volumes to the boxes in DIIMS or complete and save the [Excel Box Inventory Forms](#). Use a single method for inventorying all the boxes in a transfer. Do not mix boxes that were inventoried using the Box Inventory Forms with boxes that have volumes assigned to them in DIIMS in the same transfer.

Instructions on how to enter volumes and assign them to boxes are available in the *DIIMS Records Classifier Guide*.

4.3 Fill out and save a [Records Transfer Slip](#) (DIIMS link).

4.4 Forward the DIIMS box and collection information, the **Records Transfer Slip** and any **Box Inventory Forms** to the Department Records Management Team. Box Inventory Forms are not required if the volumes have been entered into DIIMS and assigned to boxes.

4.5 The Department Records Management Team will review the transfer for errors or missing information and may ask for changes.

4.6 The Department Records Management Team assigns the boxes to a transfer in DIIMS.

Instructions on how to assign boxes to a transfer are available in the *DIIMS Records Classifier Guide*. This action is only available to Department Records Management Team members who have Records Coordinator access permissions in DIIMS.

- 4.7 Print **GNWT Box Labels** from the [DIIMS Records Classifier Reports](#). These labels contain both the transfer ID, the temporary box ID, and the DIIMS box ID. Place the labels on the boxes.

Make sure that the correct label goes on the correct box. Placing the wrong label on the wrong box could lead to difficulty in retrieving boxes. It could also lead to premature or incorrect disposal of the records.

Instructions for printing the labels are available in the *DIIMS Records Classifier Guide*. See *4100 Requirements for Accessing Records Centre Services* or *Appendix A* for the correct placement of the labels.

- 4.8 The Department Records Management Team updates the **Records Transfer Slip** and any **Box Inventory Forms** with the transfer ID number and then e-mails them to Enterprise Records Management (ERM) (Corporate\_Records@gov.nt.ca). ERM prefers to receive one transfer request per e-mail message.

Box Inventory Forms are not required if the volumes have been entered into DIIMS and assigned to boxes.

- 4.9 An ERM records analyst will review the transfer for errors or missing information. If there are no errors or missing information the records analyst will approve the transfer.
- 4.10 In Sòmbak'è (Yellowknife), the ERM records analyst will arrange with the Department of Infrastructure's Central Warehouse to have the boxes picked up by a moving contractor. Boxes are usually picked up every second Wednesday. Enterprise Records Management can provide the schedule.
- 4.11 In Łíídlı Kúé, Tthebacha, Xátł'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik), departments are responsible for hiring a moving contractor and for scheduling a delivery time with the records centre administrator.

Boxes must be dropped off at the records centre loading area. They will not be accepted if delivered to Department of Infrastructure's regional office.

Boxes must not be dropped off at the records centre outside of scheduled times. The records centre administrator must be on hand to receive the boxes.

- 4.12 Records should be shipped to the records centre soon after they have been accepted by ERM.

ERM may cancel a transfer that is not shipped within one month of acceptance. The risk increases for the contents of the boxes to have changed while they sit in government office space. Files may have been removed and new ones added. These changes may impact the retention and disposition of a box. They may also result in missing or misplaced files.

- 4.13 Records shipped from a community that does not have a records centre are the responsibility of the originating department until they are received by the records centre.

Enterprise Records Management and the records centres are not responsible for any damage that may occur in transit.

Enterprise Records Management may request photographs of the boxes before they are accepted to ensure that the boxes are in good shape before they leave the originating office.

- 4.14 The records centre administrator will visually inspect the boxes on arrival at the records centre to make sure that the boxes comply with the records centre requirements.
- 4.15 If the records centre administrator does not identify any concerns with the boxes, the boxes will be shelved and assigned to a locator code in DIIMS.
- 4.16 The records analyst will notify the Department Records Management Team that the boxes have been shelved.<sup>1</sup>

---

<sup>1</sup> The Department of Infrastructure will provide a Box Location/Status Listing to public agencies that do not have access to DIIMS. The Box Location/Status Listing provides information required to retrieve files and boxes from the records centres. Departments that have access to DIIMS can obtain a copy of the Box Location/Status Listing from the DIIMS Records Classifier Reports.

## 4210 Re-inventorying Boxes in Storage

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

It is sometimes necessary to re-inventory boxes already in storage in the GNWT records centres. Some of the reasons why this may happen include the following:

- Someone has discovered an error in the Box Inventory Forms or the box inventories entered in DIIMS.
- The Box Inventory Forms do not contain enough detail to effectively manage the records.
- A department or agency has decided to enter older file folders (boxes) into DIIMS to improve searching and retrieval capabilities.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Department Records Management Teams should discuss any plans to re-inventory boxes with an Enterprise Records Management (ERM) records analyst. It is helpful if ERM is provided with a list of the boxes to be re-inventoried in case the re-inventorying project exceeds the regular 90-day retrieval period.
- 3.2 Boxes must be retrieved from the records centre as regular 90-day retrievals. The records centres do not have on-site facilities for departmental staff to review and re-inventory boxes.
- 3.3 Re-inventoried boxes may be returned to the records centre as part of their original transfer.

### 4. Procedures

- 4.1 The Department Records Management Team submits a retrieval request to the records centre via DIIMS to retrieve the box that is to be re-inventoried.<sup>1</sup> See the *DIIMS Records Classifier Guide* for information on how to request boxes from the records centres using DIIMS.

---

<sup>1</sup> Agencies which do not have access to DIIMS may request boxes by filling out a **Request for Records** form and e-mailing it to the records centre.

- 4.2 The Department Records Management Team or a designated employee re-inventories the box and either enters the volumes into DIIMS and adds them to the box or updates the Box Inventory Forms. If the volumes are in DIIMS, DIIMS will automatically send a notification to Enterprise Records Management that a change has been made to the box.
- 4.3 The Department Records Management Team sends an e-mail to Enterprise Records Management (Corporate\_Records@gov.nt.ca) to confirm that the box has been updated.
- 4.3.1 If the volumes have been entered into DIIMS and this has resulted in a change to the box level information, the Department Records Management Team should provide ERM with the following information:
- New box From Date.
  - New box To Date.
  - New box SO Date, if applicable.
  - New box RSI (retention schedule)
  - New box RDA, if applicable)
- 4.3.2 If the volumes have not been entered into DIIMS, the Department Records Management Team must provide ERM with updated **Box Inventory Forms**.
- 4.4 The ERM records analyst updates the box dates, the RSI, and the RDA fields in DIIMS (if applicable).
- 4.5 The ERM records analyst updates ERM's PDF copy of the Box Inventory Forms (if applicable).
- If volumes have been entered into DIIMS, the ERM records analyst will update ERM's PDF copy of the Box Inventory Forms with a note indicating that the volumes have been entered into DIIMS and that the Box Inventory Forms should not be used for retention and disposition of records.
- 4.6 The Department Records Management Team returns the box to the records centre.

## 4300 Retrievals from the Records Centres

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

The GNWT records centres provide storage and retrieval services for semi-active records belonging to government departments and some agencies. Records placed in storage may be retrieved by the department that owns them at any time prior to final disposition.

The GNWT is going through a period of change in the way it manages its paper files. For many years, records boxes and the paper file folders inside them were managed using manual systems that relied on typed or handwritten Box Inventory Forms. This changed in 1998 when a new computer system, known as iRIMS, was introduced to manage the boxes. This system was replaced by DIIMS in 2012. Every box in the records centre is listed in DIIMS. The circulation feature in DIIMS can be used to retrieve any box.

DIIMS is used to manage paper file folders, which DIIMS refers to as volumes. However, only a portion of the paper file folders housed in the records centres have been entered into DIIMS. Some departments and agencies use DIIMS to list the paper file folders that they send to the records centres while some do not. The use of DIIMS to list paper file folders may vary between divisions within a single department or agency as well.

The differences in the management of paper file folders affect how retrieval services are delivered.

Enterprise Information Management recommends the use of DIIMS to inventory all paper files at all stages of their life cycle, including files being transferred to the records centres for storage or disposal.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

3.1 Retrieval requests must be submitted by using the circulation feature in DIIMS or by e-mail.

3.1.1 To request an **entire box**, use the circulation feature in DIIMS.<sup>1</sup> See the [DIIMS Records Classifier Guide](#) for more information on how to make a request using DIIMS.

---

<sup>1</sup> Aurora College and other agencies that are unable to use DIIMS due to network access issues may request entire box by filling out a Request for Records form and e-mailing the form to the records centre that houses the records.

- 3.1.2 To request a **file folder (volume) that is listed in DIIMS**, use the circulation feature in DIIMS. See the [DIIMS Records Classifier Guide](#) for more information on how to make a request using DIIMS.
- 3.1.3 To request a **file folder (volume) that it is not listed DIIMS**, fill out a [Request for Records](#) form and e-mail it to the records centre. See the [Request for Records Form Procedures](#) for information on how to fill out the form.
- 3.2 Requests that do not have all of the required information may not be filled.
- 3.3 The following service standards apply:
- **Urgent requests:** within three hours.
  - **Non-urgent requests:** within 24 hours.
- 3.4 There are two types of retrievals:
- **Regular 90-day retrievals:** items charged out for 90 days will be returned to the records centre within 90 calendar days of when they were retrieved.
  - **Permanent returns:** items charged out as a permanent return will not be returned to the records centre.
- 3.5 Departments and agencies are responsible for picking up their items from the records centre. The records centres do not deliver retrieved items. Instead, departments can:
- Send a courier to pick up the item.
  - Pick up the item in person.
  - Ask the records centre administrator to put the item in internal mail. Internal mail is not recommended for items that contain confidential or personal information because the chain of custody is not tracked.
- 3.6 The records centres do not ship items to another community. Instead, the person who made the request must arrange to have the item picked up and delivered to the other community.
- 3.7 Departments and agencies may put restrictions on who can retrieve items from the records centres. Department Records Management Teams are advised to give each records centre a list of employees who are authorized to retrieve items and keep these lists up-to-date. If no list is provided, the records centres will accept retrieval requests from any employee in that department.
- 3.8 No one can request records belonging to a department or agency other than the one for which they are employed.
- 3.9 Departments and agencies are responsible for keeping track of the items that they retrieve.

#### **4. Procedures – Retrieving Items using DIIMS**

The following procedures apply to all requests for items that are listed in DIIMS.

- 4.1 Search or browse DIIMS to find the item that you would like to request.

- 4.2 Follow the procedures for requesting physical items in the [DIIMS Records Classifier Guide](#).
- 4.3 The records centre administrator will receive your request, print a request slip, and retrieve the item. They will attach a copy of the request slip to the item. **Do not remove** the slip. If the item is a regular retrieval, this slip will be used by the records centre to make sure that the item is returned to the correct location when you send it back to the records centre.
- 4.4 The records centre administrator will contact you or your Department Records Management Team when the item is ready to be picked up.

## 5. Procedures – Retrieving Items using the Request for Records Form

The following procedures apply to all requests for paper file folders (volumes) that are not listed in DIIMS. These procedures may also be used to request entire boxes by agencies that do not have access to DIIMS.

- 5.1 Review Box Inventory Forms and Box Location Status Lists to find the item that you would like to request. Double-check the location of the box in DIIMS, as the box may have moved to a new location in the records centre since it was originally shelved.
- 5.2 Follow the [Request for Records Form Procedures](#) and fill out a [Request for Records](#) Form.
- 5.3 E-mail the completed **Request for Records** Form to the records centre that has the records. See *4002 Records Centre Contact Information* for the records centre e-mail addresses.
- 5.4 The records centre administrator will receive your request, print a request slip, and retrieve the item. They will attach a copy of the request slip to the item. **Do not remove** the slip. If the item is a regular retrieval, this slip will be used by the records centre to make sure that the item is returned to the correct location when you send it back to the records centre.
- 5.5 The records centre administrator will contact you or your Department Records Management Team when the item is ready to be picked up.

## 4301 Retrieval of Records Approved for Disposition

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

From time to time, it may be necessary to retrieve a file folder (volume) or a box that has already been approved for final disposition but which has not yet been destroyed or transferred to the NWT Archives. Enterprise Records Management (ERM) recommends that retrieval of records from boxes which are part of an approved disposition should be restricted to situations where the records are required for a legal matter, an audit, or an access to information request.

Retrieving files from boxes that have been approved for disposition complicates the disposition process. It may cause delays in the disposal of other records. It is also time consuming for records centre administrators, who may have to sort through 60 boxes that have been stored on a pallet and shrink wrapped in preparation for shredding.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Retrieval requests must be sent to the records centre administrator by e-mail or by using the circulation feature in DIIMS.
  - 3.1.1 To request an **entire box**, use the circulation feature in DIIMS.<sup>1</sup> See the [DIIMS Records Classifier Guide](#) for more information on how to make a request using DIIMS.
  - 3.1.2 To request a **file folder (volume) that is listed in DIIMS**, use the circulation feature in DIIMS. See the [DIIMS Records Classifier Guide](#) for more information on how to make a request using DIIMS.
- 3.2 Items that have been approved for final disposition should be requested from the records centre as a **permanent return**.
- 3.3 If the records centre administrator has not yet been advised by Enterprise Records Management (ERM) that the boxes or file folders (volumes) being requested are ready for disposal, the retrieval request will be handled by the records centre administrator as a

---

<sup>1</sup> Agencies that are unable to use DIIMS due to network access issues may request an entire box by filling out a **Request for Records** form and e-mailing the form to the records centre that houses the records.

routine retrieval request. **It is up to the department requesting the file to identify the retrieval as a permanent return.**

- 3.4 If the records centre administrator has been advised by ERM that the boxes or file folders (volumes) being requested are ready for disposal and has been provided with disposition labels for boxes that were in semi-active storage in the records centre, the retrieval request will be handled as a permanent return.
- 3.5 Departments and agencies are responsible for picking up their items from the records centre. The records centres do not deliver retrieved items. Instead, departments can:
  - Send a courier to pick up the item.
  - Pick up the item in person.
  - Ask the records centre administrator to put the item in internal mail. Internal mail is not recommended for items that contain confidential or personal information because the chain of custody is not tracked.
- 3.5 The records centres do not ship items to another community. Instead, the person who made the request must arrange to have the item picked up and delivered to the other community.
- 3.6 The records centres do not have research or “reading room” facilities and are not able to accommodate requests to review records on site.

#### **4. Procedures – Retrieving Items using DIIMS**

The following procedures apply to all requests for items that are listed in DIIMS.

- 4.1 Search or browse DIIMS to find the item that you would like to request.
- 4.2 Follow the procedures for requesting physical items in the [DIIMS Records Classifier Guide](#).
- 4.3 The records centre administrator will receive your request, print a request slip, and retrieve the item.
- 4.4 The records centre administrator will contact you when the item is ready to be picked up.
- 4.5 Permanent return request and any requests for items that have been moved to a pallet in preparation for disposal will be forwarded to ERM. An ERM records analyst will update the disposition record and DIIMS to show that the item was permanently returned to the department or agency.

#### **5. Procedures – Retrieving Items using the Request for Records Form**

The following procedures apply to all requests for paper file folders (volumes) that are not listed in DIIMS. These procedures may also be used to request entire boxes by agencies that do not have access to DIIMS.

- 5.1 Review Box Inventory Forms and Box Location Status Lists to find the item that you would like to request. Double-check the location of the box in DIIMS, as the box may have been

removed from its records centre shelf location and placed on a pallet. Pallet locations appear in DIIMS using the following format: Records Centre Facility Code / Area / Pallet number (e.g. RC-YKHLD / PAL / 01)

- 5.2 Follow the [Request for Records Form Procedures](#) and fill out a [Request for Records](#) Form.
- 5.3 E-mail the completed **Request for Records** Form to the records centre that has the records. See *4002 Records Centre Contact Information* for the records centre e-mail addresses.
- 5.4 The records centre administrator will receive your request, print a request slip, and retrieve the item.
- 5.5 The records centre administrator will contact you when the item is ready to be picked up.
- 5.6 Permanent return request and any requests for items that have been moved to a pallet in preparation for disposal will be forwarded to ERM. An ERM records analyst will update the disposition record to show that the item was permanently returned to the department or agency.

## 4310 Returning Files and Boxes

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The GNWT records centres provide storage and retrieval services for semi-active records belonging to government departments and some agencies. Records placed in storage may be retrieved by the department that owns them at any time prior to final disposition.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Items that were charged out as regular 90-day retrievals can be returned. Items must be returned to the records centre that they were originally stored in or retrieved from.
- 3.2 Permanently returned items cannot be returned to the records centre as part of their original transfer. Instead, they must be added to a new transfer.
- 3.3 Items must have the original **Request for Records Form** attached to them. This is to make sure that the items are returned to the correct locations.
- 3.4 Items must not be bundled together with elastic bands.
- 3.5 Items must be delivered to the records centres. Do not deliver items to the Department of Infrastructure's main regional office locations.  
  
In Łíídlı́ Kúé, Tthebacha, Xát'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik), contact the records centre administrator to schedule a delivery time and ensure that someone will be at the records centre to receive your items. Do not leave the items outside by the front door of the records centre.
- 3.6 Items may be delivered in person or by courier. Internal mail is not recommended for confidential or personal information because the chain of custody is not tracked.
- 3.7 The following service standard applies:
  - Returned items will be returned to the records centre shelves and charge out information will be updated in DIIMS within 24 hours of receipt of the items or as soon as possible.

#### **4. Procedures**

- 4.1 In Sòmbak'è (Yellowknife), send charged-out file items to the Records Centre, GNWT Central Warehouse, 415 Byrne Road.
- 4.2 In Łíídlı Kúé, Tthebacha, Xátł'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik), call the records centre administrator to schedule the delivery.
- 4.3 The records centre administrator will update DIIMS (if applicable). They will then put the item back on the shelf in the records centre.
- 4.4 The records centre administrator will contact you if an item cannot be returned to its original location for some reason. For example, you will be contacted if documents have been added to a paper file folder (volume) and it no longer fits inside its box.

## 4320 Permanent Returns

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

The GNWT records centres provide storage and retrieval services for semi-active records belonging to government departments and some agencies. Records placed in storage may be retrieved by the department that owns them at any time prior to final disposition.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 A permanent return happens when someone retrieves an item from the records centre and plans to keep it. Permanent returns are also called reactivations.
- 3.2 Items that are permanently returned will not be taken back into the records centre as part of their original transfer. They must be added to a new transfer. The reason for this is that the items may have changed, and the original retention and disposition dates may no longer be correct.
- 3.3 Departments and agencies are responsible for picking up their items from the records centre. The records centres do not deliver retrieved items. Instead, departments can:
  - Send a courier to pick up the item.
  - Pick up the item in person.
  - Ask the records centre administrator to put the item in internal mail. Internal mail is not recommended for items that contain confidential or personal information because the chain of custody is not tracked.
- 3.4 The records centres do not ship items to another community. Instead, the person who made the request must arrange to have the item picked up and delivered to the other community.
- 3.5 Departments and agencies may put restrictions on who can retrieve items from the records centres. Department Records Management Teams must give the records centres a list of employees who are authorized to retrieve items. If no list is provided, the records centres will accept retrieval requests from any employee in that department.
- 3.6 No one can request records belonging to a department or agency other than the one for which they are employed.

- 3.7 Departments and agencies are responsible for keeping track of the items that they retrieved.
- 3.8 If an item is accidentally requested as a permanent return, when it was supposed to be a regular 90-day retrieval, the department has 90 days from the date of the request to contact Enterprise Records Management (ERM) to reverse the request.
- 3.9 The following service standard applies:
- Permanently returned items will be updated in DIIMS within five business days.

#### 4. Procedures

- 4.1 For items listed in DIIMS, such as boxes and file folders (volumes), follow the procedures for requesting physical items in the [DIIMS Records Classifier Guide](#). Select Permanent Return as the Request Type.
- 4.2 For file folders (volumes) that have not been entered into DIIMS, follow the [Request for Records Form Procedures](#) and fill out a [Request for Records](#) Form. Select Permanent Return in the Return By section of the form.
- 4.3 The records centre administrator will receive your request, print a request slip, and retrieve the item. They will also cancel the retrieval request in DIIMS.
- 4.4 The records centre administrator will contact you when the item is ready to be picked up.
- 4.5 The records centre administrator will forward the Request for Records e-mail to the Enterprise Records Management e-mail account.
- 4.6 For items entered in DIIMS, an ERM records analyst will update the following:
- Permissions will be changed so that Department Records Management Team can modify and move the item.
  - Location will be updated to Department (DEP).
  - Status will be updated to Active (ACT).
  - Status Date will be updated to the date that the item was permanently returned.
  - File folders (volumes) will be removed from their box.
  - Boxes will be removed from their shelves.
- 4.6 For items not entered in DIIMS, an ERM records analyst will update ERM's PDF copy of the Box Inventory Forms to show that the item was permanently returned.
- 4.7 ERM recommends that Department Records Management Teams update their master Box Inventory Forms to show that the item was permanently returned.
- 4.8 To permanently return an item that was retrieved as regular 90-day retrieval, send an e-mail to the records centre e-mail address and explain that you want to permanently return the item.

- Attach the completed **Request for Records** Form to your e-mail message, or
- For requests made through DIIMS, provide the transfer ID, temp box # or DIIMS Box ID, and the full file number, volume number, and file title.

4.9 To reverse a permanently return on an item that was supposed to be retrieved as regular 90-day retrieval but was accidentally submitted as a permanent return, send an e-mail to the Enterprise Records Management e-mail address, [Corporate\\_Records@gov.nt.ca](mailto:Corporate_Records@gov.nt.ca), and explain that you want to reverse the permanent return. This request must be received within 90 days after the original retrieval request was sent.

- Attach the completed **Request for Records** Form to your e-mail message, or
- For requests made through DIIMS, provide the transfer ID, temp box # or DIIMS Box ID, and the full file number, volume number, and file title.

## 4321 Permanent Returns Following a Records Centre Program Review

<b>Issued:</b>	November 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Enterprise Records Management (ERM) unit conducts annual reviews of the regional records centre programs. The program reviews include taking an inventory of the records centre's holdings. Very often the inventories find that boxes have been charged out of the records centre for several months. ERM permanently returns these boxes to their department or agency. This is done for two reasons:

- The contents of the boxes may have changed while they are charged out, which makes box inventories and box retention and final disposition dates inaccurate.
- ERM is responsible for managing the space in the records centres. Shelf space must be maximized to allow for transfers of new records into storage.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Items that have been retrieved as regular 90-day retrievals are considered overdue if they have not been returned at the end of the 90 day period (90 calendar days).
- 3.2 ERM will permanently return any boxes identified as overdue during a records centre program review.

### 4. Procedures

- 4.1 One month before a scheduled records centre program review, the ERM records analyst assigned to the program review will notify Department Records Management Teams that a program review is going to take place.
- 4.2 Department Records Management Teams should review boxes that are charged out from the records centre. The Department Records Management Teams should respond to the ERM records analyst's notice and advise the records analyst on what they are planning to do with each box. This notice should be sent to the ERM records analyst at least one week before the scheduled program review start date.

Boxes that have been charged out for more than 90 days should be returned to the records centre or the Department Records Management Team can request to have the box marked as a permanent return.

If there are unusual circumstances that require an extension to the borrowing period, the Department Records Management Team should contact the ERM records analyst and request an extension. The ERM records analyst will review the request and, in consultation with the Manager, ERM, accept or deny the request.

- 4.3 Records centre inventories are conducted by ERM records analysts with assistance from records centre administrators.
- 4.4 The contents of each shelf in the records centre are compared against an inventory list printed from DIIMS. The inventory is printed the week before the scheduled program review start date.
- 4.5 If an Out Card is found on a shelf, the ERM records analyst will check the retrieval date of the box. If the box is overdue and ERM has not approved a request to extend the charge-out period, the ERM records analyst will remove the Out Card from the shelf.
- 4.6 The ERM records analyst will notify the Department Records Management Team that Out Cards for overdue boxes were found in the records centre. The box may be returned to the records centre or a request made to ERM to have the box permanently returned to the department.
- 4.7 If the Department Records Management Team does not provide direction on how to handle the box, or if a request is made to have the item permanently returned to the department, the ERM records analyst will update the following information in DIIMS:
  - Permissions will be changed so that the Department Records Management Team can modify and move the item.
  - Location will be updated to Department (DEP).
  - Status will be updated to Active (ACT).
  - Status Date will be updated to the date that the item was permanently returned.
  - Boxes will be removed from their shelves.
- 4.8 The ERM records analyst will notify the Department Records Management Team that the item has been permanently returned.
- 4.9 ERM recommends that Department Records Management Teams update their master Box Inventory Forms to show that the item was permanently returned

## 4330 Missing Files and Boxes

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	December 2021

### 1. Introduction

The GNWT records centres provide storage and retrieval services for semi-active records belonging to government departments and some agencies. The Department of Infrastructure takes precautions to ensure that records transferred to the records centres are accounted for at all times. However, sometimes items go missing.

Missing file folders (volumes) are usually identified by the records centre administrators when attempting to complete a retrieval request.

Missing boxes are usually identified either by the records centre administrator while attempting to complete a retrieval request or by a records analyst from Enterprise Records Management (ERM) while conducting an inventory of the records centre.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 File folders (volumes) and boxes will only be identified as missing if the Department Records Management Team for the department that owns the item provides written instruction to Enterprise Records Management to change the item's status.
- 3.2 Boxes that have been found may be returned to the records centre as long as they are in the semi-active stage of their life cycle. Boxes that have reached their final disposition phase cannot be returned to the records centre for storage.
- 3.3 File folders (volumes) that have been found may be returned to the records centre as long as the box is still in storage in the records centre and has not been approved for final disposition or disposed of.

### 4. Procedures – Missing Items

- 4.1 The records centre administrator or ERM records analyst is unable to locate an item in the records centre.

- 4.2 The records centre administrator or ERM records analyst will send an e-mail to the Department Records Management Team for the department that owns the item and advise that the item appears to be missing from the records centre.
- 4.3 If the Department Records Management Team confirms in writing that the item is missing, Enterprise Records Management will update its information on the item.
- 4.3.1 For boxes and file folders (volumes) entered into DIIMS:
- The status will be changed to missing (MIS).
  - The description field will be updated with a note indicating that the item has been declared missing.
  - File folders (volumes) will be removed from their boxes.
  - Boxes will be removed from their shelf location.
  - Permissions will be updated so that the Department Records Management Team has full rights to manage the item if it is located.
- 4.3.2 For file folders that have not been entered into DIIMS, the ERM records analyst will update ERM's copy of the Box Inventory Forms to show that the item is missing.

## 5. Procedures – Found Items

- 5.1 The Department Records Management Team sends an e-mail to the Enterprise Records Management e-mail account indicating that a missing item has been found.
- 5.2 For file folders (volumes), an ERM records analyst will do the following:
- Confirm that the original box is still in storage in the records centre.
  - If the box is still in storage, the ERM records analyst will,
    - Reassign the volume to its original box.
    - Update the permissions for the file folder.
    - Update the status to semi-active (SA) and update the description to indicate that the item has been located.
    - Update Box Inventory Forms, if applicable.
    - Advise the records centre administrator that the item is going to be returned to the records centre.
    - Tell the Department Records Management Team to send the item to the records centre.
  - If the box has been disposed of or is no longer in storage, the ERM records analyst will,
    - Tell the Department Records Management Team that the file folder cannot be returned to the records centre and that it will be permanently returned to the department.

- Update the status of the item to Active (ACT) and update the description to indicate that the item has been located and permanently returned to the department.
- Update Box Inventory Forms to show that the item has been permanently returned to the department, if applicable.

5.3 For boxes, an ERM records analyst will do the following:

- Update the permissions for the box.
- Update the status to semi-active (SA) and update the description to indicate that the item has been located.
- Update Box Inventory Forms, if applicable.
- Advise the records centre administrator that the item is going to be returned to the records centre.
- Tell the Department Records Management Team to send the item to the records centre.

5.4 For file folders (volumes) the Department Records Management Team fills out and prints a [Request for Records Form](#) and attaches it to the volume so that the records centre administrator can easily return the item to its original box.

5.5 For boxes, the Department Records Management Team should confirm that the contents of the box still match the original box inventory forms or DIIMS inventory. Then, the Department Records Management Team will fill out a [Records Transfer Slip](#) (DIIMS link) and send it to the Enterprise Records Management e-mail account. The ERM records analyst will forward the Records Transfer Slip to the records centre administrator.

In Sòmbak'è (Yellowknife), the boxes will be picked up and delivered to the records centre on the next scheduled pick-up day.

In Łíídlı Kúé, Tthebacha, Xátł'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik), the Department Records Management Team will make arrangements to have the box delivered to the records centre and schedule the delivery with the records centre administrator.

## 4400 Records Disposition

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	July 2021

### 1. Introduction

The disposal of records is part of the ordinary and normal business of government. Almost all government records will eventually outlive their usefulness to the department or agency that created them and keeping records longer than necessary is a liability to the government.

Records occupy physical and network storage space and there is a cost to maintain them. Keeping large volumes of out-of-date records also increases the time, resources, and risks associated with searching for information, responding to Access to Information requests, and responding to legal actions.

At the same time, failure to keep records and failure to dispose of records in accordance with the GNWT's accepted business practices exposes the GNWT to risks. There is a risk that information will not be available when required. There is also a risk that the government will not be able to adequately explain what happened to information when responding to a question from the Legislative Assembly, an Access to Information request, an audit, an investigation, or a legal action.

The length of time that records should be kept by a government department or agency is identified in records disposition authorities (RDAs). RDAs also identify the mode of final disposition. The Territorial Archivist reviews and authorizes the disposal of records in accordance with the retention schedules and final dispositions outlined in the records disposition authorities.

Disposing of records without the authorization of the Territorial Archivist is a violation of the *Archives Act*. Anyone who damages or mutilates a record, removes a record from a government office, or destroys a record without authorization from the Territorial Archivist is guilty of an offence and is liable on summary conviction to a fine not exceeding \$5,000, or to imprisonment for a term not exceeding one year, or to both.

### 2. References

Agreement on records between the Government of the Northwest Territories and the Interim Commissioner of Nunavut, dated March 29, 1999.

Archives Act, R.S.N.W.T 1998, c.A-6

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

Information and documentation – Records management – Part 1: Concepts and principles, International Organization for Standardization, ISO 15489-1:2016.

### 3. Guidelines

- 3.1 Records must not be disposed of except in accordance with the retention and disposition set out in an approved RDA, such as the Administrative Records Classification System (ARCS) (RDA 1995-32), an Operational Records Classification System (ORCS), or a One-Time Schedule, or the Transitory Records Schedule (RDA 1997-02).
- 3.2 Records must not be disposed of unless they have reached the final disposition phase of their life cycles as identified in an approved RDA. Final disposition usually takes the form of transfer to the Northwest Territories Archives or destruction.
- 3.3 As per the *Agreement on records with the Government of Nunavut*, where the GNWT proposes to destroy substantive records that were created before April 1, 1999, the GNWT will provide the Government of Nunavut (GN) with a written notice of the records to be destroyed. The GN will review the records and may determine that it wishes to retain some of the records. Enterprise Records Management will coordinate the offer of records to the GN and the transfer of any records that the GN wishes to retain. There is no requirement to notify the GN about the disposal of transitory records.
- 3.4 Records relating to pending or current litigation, legal actions, investigations, audits, or Access to Information requests should not be disposed of while that activity is underway or anticipated.
- 3.5 The Department of Infrastructure provides records disposal services to the GNWT for records that have been classified and scheduled in the ARCS, an ORCS, or a One-Time Records Disposition Authority, as an extension of its records centre services for paper records and electronic records stored in DIIMS.
- 3.6 Actions relating to disposition of records must be documented. The department that created or maintained the records is responsible for maintaining a record of records disposition. Records documenting the disposition of records may be classified and scheduled in ARCS.
- 3.7 Transitory records may be disposed of by government employees, providing that they meet the requirements of the *Transitory Records Schedule* (RDA 1997-02). Transitory records may contain sensitive confidential and personal information. Disposal of transitory records must be handled with care to avoid disclosure of the information. There is no requirement to document the disposal of transitory records.

## 4410 Disposition of Physical Records

<b>Issued:</b>	July 2018
<b>Last Updated:</b>	December 2021

### 1. Introduction

The GNWT Records Centres provide records disposal services for substantive government records that are in a physical format, primarily paper. This procedure does not apply to transitory records.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 In order to be processed by a GNWT records centre for disposal arrangements, files in each box must be closed (i.e. no additional paper will be added to them), have reached the final disposition stage in their life cycle, and be scheduled by the GNWT Administrative Records Classification System (ARCS), an Operational Records Classification System (ORCS), or a One-Time Schedule.
- 3.2 To be accepted for disposal, the boxes must meet the records centre requirements. See *4100 Requirements for Accessing Records Centre Services*.
- 3.3 Unscheduled records (records that are not classified and scheduled by an approved RDA) and transitory records will not be accepted for disposal in the records centre.
- 3.5 The following service standards apply:
  - **Sòmbak'è (Yellowknife):**
    - Boxes will be picked up every second Wednesday by a moving contractor hired by the Department of Infrastructure's North Slave Regional Office. Contact [Corporate\\_Records@gov.nt.ca](mailto:Corporate_Records@gov.nt.ca) for a copy of the schedule. If there is a priority move of surplus furniture, then the pick-up date will be moved to Thursday.
    - Requests must be received by the Wednesday before the pick-up date to ensure that Enterprise Records Management (ERM) has time to review and process the requests.

- **All Records Centres**
  - Boxes will be received, and box location information will be uploaded to DIIMS within 24 hours of receipt of the boxes or as soon as possible.
  - Boxes will be shredded within 24 hours from the time that ERM authorizes the shredding or as soon as possible. Shredding for the Sòmbak'è (Yellowknife) Records Centre is contracted out and shredding frequency varies depending on the number of boxes to be shredded.

#### 4. Procedures – Disposition from Department

Sometimes records reach the final disposition stage of their life cycle while they are still located in a government office.

The following procedure describes the steps involved in transferring boxes to the records centre to dispose of them immediately.

- 4.1 Pack files into boxes. Make sure that the boxes comply with the records centre requirements.
- 4.2 Enter the boxes into DIIMS and assign them to a collection. Instructions on how to enter boxes and create collections are available in the [DIIMS Records Classifier Guide](#).
- 4.3 Assign the volumes to the boxes in DIIMS or complete and save **Excel Box Inventory Forms**.
  - Use a single method for inventorying all the boxes in a transfer.
  - Do not mix boxes in the same transfer that were inventoried using the Box Inventory Forms with boxes that have volumes assigned to them in DIIMS.

Instructions on how to enter volumes and assign them to boxes are available in the *DIIMS Records Classifier Guide*.
- 4.4 Fill out and save a **Records Transfer Slip** (DIIMS link).
- 4.5 Forward the DIIMS box and collection information, the **Records Transfer Slip** and any **Box Inventory Forms** to the Department Records Management Team.
  - Box inventory forms are not required if the volumes have been entered into DIIMS and assigned to boxes.
- 4.6 The Department Records Management Team will review the boxes for errors or missing information and may ask for changes.
- 4.7 The Department Records Management Team assigns the boxes to a transfer in DIIMS. Only team members who have Records Coordinator access permissions in DIIMS can assign boxes to transfers. See the *DIIMS Records Classifier Guide* for information on how to assign boxes to a transfer.

- 4.8 The Department Records Management Team obtains a **Disposition Authorization Letter** from the director or regional superintendent responsible for the records. The Disposition Authorization Letter must include the Records Disposition Authority number (RDA number) that applies to the records that are being disposed of and the number of boxes being disposed of. This authorization letter approves the disposal of records that have met their eligible disposition date while in the custody and control of the program that own the records. It is also used by ERM to accept the records for disposal arrangements managed by a GNWT's records centre facility.

The director or regional superintendent should review the **Box Inventory Forms** or a **Box Inventory Report** generated from DIIMS prior to approving the disposal of the records. The reason for this review is to identify any records that should not be destroyed because they are required to respond to litigation, a legal action, an investigation, an audit, or an Access to Information request. Records that are subject to one of these actions must be kept by the department until the matter is resolved.

ERM and the records centres are not responsible for identifying records that should be retained for legal, audit, Access to Information, or other reasons.

- 4.9 Print **GNWT Box Labels** from the [DIIMS Records Classifier Reports](#). These labels display the transfer ID, the temporary box ID, and the DIIMS box ID. Place the labels on the boxes. Make sure that the correct label goes on the correct box. Placing the wrong label on the wrong box could lead to premature or incorrect disposal of the records.

Instructions for printing the labels are available in the *DIIMS Records Classifier Guide*. See *4100 Requirements for Accessing Records Centre Services* and *Appendix A* for the correct placement of the labels

- 4.10 The Department Records Management Team updates the **Records Transfer Slip** and any **Box Inventory Forms** with the transfer ID number and then submits them along with the **Disposition Authorization Letter** to ERM (Corporate\_Records@gov.nt.ca).

ERM prefers to receive one transfer request per e-mail message.

Box Inventory Forms are not required if the volumes have been entered into DIIMS and assigned to boxes.

- 4.11 ERM will review the transfer for errors or missing information. If there are no errors or missing information ERM will accept the transfer for disposition.
- 4.12 ERM will open a disposition file and assign a disposition file number to the boxes in DIIMS. ERM will send **disposition labels** to the Department Records Management Team.
- 4.13 The Department Records Management Team will have the **disposition labels** printed and placed on the boxes. They will notify ERM when the boxes have been labeled. Disposition labels show the same transfer, temporary box ID number, and DIIMS box ID that is shown on the GNWT Box Labels. Departments must take care to ensure that the correct label is placed on the corresponding box. Placing the wrong label on the wrong box could lead to incorrect disposal of the records.

- 4.14 In Sòmbak'è (Yellowknife), ERM will arrange with the Department of Infrastructure's Central Warehouse to have the boxes picked up by a moving contractor. Boxes are usually picked up every second Wednesday. ERM can provide the schedule.
- 4.15 In Łíídlı Kúé, Tthebacha, Xátł'odehchee, and Inuvik (Fort Simpson, Fort Smith, Hay River, and Inuvik), departments are responsible for hiring a moving contractor and for scheduling a delivery time with the records centre administrator.
- Boxes must be dropped off at the records centre. They will not be accepted if delivered to Department of Infrastructure's main regional office location.
  - Boxes must not be dropped off at the records centre outside of scheduled times. The records centre administrator must be on hand to receive the boxes.
- 4.16 Records should be shipped to the records centre soon after they have been accepted by ERM for transfer to a records centre for disposal.
- ERM may cancel a transfer that is not shipped within one month of acceptance. The risk increases when not submitted within a month, for the contents of the boxes to have changed while they sit in government office space. Files may have been removed and new ones added. These changes may impact the retention and disposition of a box. They may also result in missing or misplaced files.
- 4.17 Records shipped from a community that does not have a records centre are the responsibility of the originating department until they are received by the records centre.
- ERM and the records centres are not responsible for any damage that may occur in transit.
  - ERM may request photographs of the boxes before they are accepted into a records centre to ensure that the boxes are in good shape before they leave the originating office.
- 4.18 The records centre administrator will visually inspect the boxes on arrival at the records centre to make sure that the boxes comply with the records centre requirements.
- 4.19 If the records centre administrator does not identify any concerns with the boxes, the boxes will be received in DIIMS and processed for disposition.
- Boxes that have a final disposition of Destroy (D) will be shredded.
  - Boxes that have a final disposition of Archival Selection (AS/D) will be offered by ERM to the NWT Archives.
    - The NWT Archives personnel will review the records and may select all, some, or none of the records for permanent preservation in the Archives.
    - Records not selected for inclusion in the NWT Archives will be destroyed.

- Records that are to be destroyed and that were created before April 1, 1999 will be offered by ERM to the Government of Nunavut (GN) prior to being shredded.
  - If the GN requests records, then ERM will notify the Department Records Management Team that a request has been made.
  - The Department Records Management Team will consult with appropriate personnel within the department to determine if the records are eligible for release to the GN and will inform ERM of the decision to release the records to the GN or not.
  - ERM will arrange shipment of the records to the GN. Records not requested by GN or not authorized for transfer will be destroyed.

4.20 ERM will notify the Department Records Management Team when all the boxes in a transfer have been disposed of.

## 5. Procedures – Disposition from Storage

In most cases, paper records reach the final disposition stage of their life cycle while they are in storage in one of the GNWT's records centres. The following procedure describes the steps involved disposing of records from storage in a records centre.

- 5.1 Once per year, Enterprise Information Management (EIM) initiates a Disposition Approval Workflow in DIIMS. This workflow identifies records which are ready for disposition according to the retention and disposition schedules assigned to the records in DIIMS.
- 5.2 Each department's Records Management Team will be asked to assist in the verification of the list of senior managers for each department.
- 5.3 An e-mail is sent from EIM's Enterprise Records Management unit (ERM) to the senior manager for each division.<sup>1</sup> The e-mail will include a link to a workflow status page. Departmental Records Management Teams will be copied on these e-mails.
- 5.4 From the workflow status page, the senior manager will be able to review a report of records centre boxes which are ready for disposition. An electronic record of their review activities will be generated by DIIMS and kept by EIM.<sup>2</sup> The department records management team will receive a notification from DIIMS when the review activity is complete.

The senior manager will also be able to indicate if any of the boxes need to be kept for another year due to a current legal matter, audit, or access to information request.

---

<sup>1</sup> In agencies which are not within the GNWT's data network, and which consequently have limited access to DIIMS, this e-mail will be sent to the agency's records management team.

<sup>2</sup> In agencies which are not within the GNWT's data network, and which consequently have limited access to DIIMS, the agency's records management team should review the disposition report with the appropriate members of the senior management team and obtain their written acceptance (by wet signature, digital signature, or by e-mail) for the disposition. The records management team can then approve the disposition in DIIMS on the behalf of their organization. A copy of the written acceptance should be sent by e-mail to Corporate\_Records@gov.nt.ca.

- 5.5 ERM will begin the process of disposing of the records when they receive notification from DIIMS that the review activity is complete.
- 5.6 If the senior manager does not complete the review of the records by the end of the 90-calendar day review period, they will be deemed to have agreed to the disposition, and ERM will begin the process of disposing of the records.
- 5.7 ERM coordinates with each records centre administrator to arrange the disposition of the records.
- Boxes that have a final disposition of Destroy (D) will be shredded.
  - Boxes that have a final disposition of Archival Selection (AS/D) will be offered to the NWT Archives.
    - The NWT Archives will review the records and may select all, some, or none of the records for permanent preservation in the Archives.
    - Records not selected by the NWT Archives will be destroyed.
  - Records that are to be destroyed and that were created before April 1, 1999 will be offered by ERM to the Government of Nunavut (GN) prior to being shredded.
    - If the GN requests records, then ERM will notify the Department Records Management Team that a request has been made.
    - The Department Records Management Team will consult with appropriate personnel within the department to determine if the records are eligible for release to the GN and will inform ERM of the decision to release the records to the GN or not.
    - ERM will arrange shipment of the records to the GN.
    - Records not requested by the GN or not authorized for transfer will be destroyed.
- 5.8 The Department Records Management Team will be notified when all the records have been disposed of.

## 4420 Disposal of Transitory Records in Paper and Other Media

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

The [Transitory Records Schedule](#) (Records Disposition Authority 1997-02) provides authorization to GNWT departments and agencies to dispose of transitory records in compliance with the *Archives Act*.

The Transitory Records Schedule identifies six record types that can be disposed of as transitory records:

- Advertising material.
- Blank information media.
- Draft documents and working materials that were used to create a final document, and which are not required to show the various stages in the development of the final document or to record decisions.
- Duplicate documents.
- Non-GNWT Publications.
- Temporary information that is not required to document actions or decisions or to demonstrate that an activity took place or that information was received.

The Transitory Records Schedule applies to records in all formats, including electronic records.

### 2. References

Archives Act, R.S.N.W.T 1988, c.A-6

Financial Administration Act: Disposal of Public Property Regulations, R-047-93

Infrastructure Establishment Policy, Executive Council Policy 31.00

Disposal of Goods Policy, Executive Council Policy 31.03

Recorded Information Management Policy, IMT Policy Manual

RDA 1997-02 Transitory Records Schedule

Disposal of Surplus Goods Guidelines

### 3. Guidelines

- 3.1 Government employees may identify and dispose of transitory records themselves.

- 3.2 Transitory records do not have to be inventoried prior to disposal.
- 3.3 Transitory paper records do not have to be sent to a GNWT records centre for disposal.
- 3.4 Transitory records must be protected and securely disposed of in order to maintain security, confidentiality, protect personal privacy, and prevent security breaches.
- 3.5 Transitory paper records should be placed in a secure document destruction bin and subsequently shredded and recycled by a document destruction company contracted by the government to provide this service.

Where a document destruction contractor is not available, transitory records may be shredded in government offices using government-owned shredders.

Where a government department or agency decides to purchase a shredder, the shredder should be a cross-cut shredder that produces shredded paper no larger than 2mm x 15mm.<sup>1</sup>

Shredded paper should be sent to a paper recycling facility if possible or disposed of at the municipal solid waste facility in order to ensure that the disposal is compliant with public health, environmental, and other regulations. Shredded government records should not be repurposed for personal, education, or industrial use, such as bedding for animals, craft or packing material, theatrical props, or fuel for campfires or wood stoves.

- 3.6 Transitory paper records should not be burned. It is difficult to completely burn records. Incomplete burning may lead to the accidental disclosure of confidential or personal information. In addition, burning releases smoke and may release toxins into the air, which may have health and environmental consequences.
- 3.7 Information media, such as hard drives, USB devices (external hard drives, flash drives, thumb drives, etc.), memory cards (SD, miniSD, microSD, CF, MMC, etc.), optical storage disks (DVDs and CDs), 5.25" and 3.5" floppy disks, audio tapes, video tapes, and data tapes, should be erased or have their contents deleted. The media should then be sanitized using specialized data erasure software, degaussed, or physically destroyed to prevent the unauthorized recovery of information that was previously stored. Physical destruction may be done by shredding in a specialized shredder, disintegrating, pulverizing, or otherwise destroying the information bearing medium so that it cannot be reconstructed and played. File deletion or reformatting alone is not sufficient to destroy the information stored on the media.
- 3.8 Print publications can be declared surplus and disposed of through the GNWT's surplus goods program.

---

<sup>1</sup> 2mm x 15mm (shredder type IIIA – regular office use) is the Royal Canadian Mounted Police Security Shredding Standard for Government of Canada Protected B records. Protected B records are information where unauthorized disclosure could cause serious injury to an individual, organization, or government. It is reasonable to apply this Federal standard to the GNWT's transitory records, as they may contain information that could cause injury to another party.

## 4430 Disposition Holds for Records Stored in the Records Centres

<b>Issued:</b>	April 2019
<b>Last Updated:</b>	July 2021

### 1. Introduction

A disposition hold is a hold or halt placed on the scheduled disposal of records due to foreseeable or pending litigation, investigation, audit, access to information request, or other special requirements.

Records that pertain to pending or potential litigation, audits, investigations, and access to information requests should not be destroyed. It is recommended that these records are marked or sequestered in some way to ensure that they are neither disposed of nor tampered with.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

3.1 Disposition holds may be put in place for one or more of the following reasons:

- A legal matter, such as an investigation or lawsuit. Ideally, a request for a legal disposition hold will be supported by a litigation hold notice from the Department of Justice.
- An internal or external audit.
- A request made under the *Access to Information and Protection of Privacy Act* or the *Health Information Act*.
- The Operational Records Classification System (ORCS) is under review or being revised due to changes to policy, procedures, or legislation which may impact the retention and final disposition of the records.

3.2 Records that are already in semi-active storage in a GNWT records centre when a disposition hold is issued will continue to be held by the records centre until the disposition hold is lifted, providing that the records centre has sufficient excess capacity.

If a GNWT records centre reaches full capacity, records that are subject to a disposition hold may be returned to their originating department or agency.

3.3 The disposition of records that have been approved for final disposition and not yet disposed of may be put on hold. Boxes that were previously in storage in the records centre

(disposition from storage) will be put back into storage. Boxes that were previously in a GNWT office (destruction from department) will be returned to the originating department or agency.

- 3.3 Records that have reached their final disposition while located in a department's office space cannot be transferred to a GNWT records centre after they have been subject to a disposition hold. Instead, the records must remain in the department's office space until the hold is lifted and the records can be transferred to the records centre for final disposition.
- 3.4 When a disposition hold is lifted, the original retention and disposition will be applied to the records. If the records have reached the end of their original retention period as identified in ARCS, ORCS, or a One-Time Schedule, the boxes will be listed on the next annual Box Disposition Report.

#### **4. Procedures – Boxes Listed on Records Disposition Report**

- 4.1 Once a year, Enterprise Information Management initiates a records disposition workflow process in DIIMS, which includes reports which are distributed to departments. These reports list all the boxes stored in GNWT records centres which are eligible to be destroyed or transferred to the NWT Archives. Departments have 90 days to review the reports and identify records to be kept.

See *Section 4410* for more information on the disposition from storage process.

- 4.2 If a disposition hold is required due to a legal matter, audit, or access to information request, senior managers may use the DIIMS workflow to identify boxes which should be kept for another year.
- 4.3 The Department Records Management Team can send a request to Enterprise Records Management to place the boxes in a formal disposition hold, which will prevent the boxes from appearing in the disposition workflow until the hold is removed.

#### **5. Procedures – Boxes Approved for Final Disposition**

- 5.1 If a disposition hold is required for boxes that have already been approved for Final Disposition, the Department Records Management Team should send an e-mail to Enterprise Records Management explaining that a disposition halt has been put in place, identifying the boxes affected by the disposition halt, and requesting a status update on the boxes to determine if they have already been destroyed or transferred to the NWT Archives.
- 5.2 An ERM records analyst will review the status of the boxes and provide the Department Records Management Team with a status update. The ERM records analyst will tell the records centre administrator to stop any disposal activities and await further instructions.
- 5.3 If the boxes have not already been destroyed or transferred to the NWT Archives, the Department Records Management Team will obtain a letter from the Director or Regional Superintendent responsible for the records advising that records must be halted.

5.4 The Department Records Management Team will forward the letter to Enterprise Records Management.

5.5 On receipt of the letter, the ERM records analyst will inform the records centre administrator that the disposition has been cancelled.

5.5.1 If the boxes were originally in storage in the records centre (disposition from storage), the ERM records analyst will tell the records centre administrator that the boxes should be returned to the records centre shelves and that the disposition labels should be removed.

The records centre administrator will return the boxes to any free shelf location in the records centre.

The ERM records analyst will remove the boxes from the disposition and add them to a disposition hold in DIIMS. If all of the boxes in the disposition have been halted, the ERM records analyst will cancel the disposition.

5.5.2 If the boxes were originally stored in the originating department's office space (disposition from department), the ERM records analyst will ask the Department Records Management Team to make arrangements to return the boxes to the originating department. The Department of Infrastructure is not responsible for arranging delivery of the boxes.

Once the boxes have been returned to the department, remove the disposition labels from the boxes or black the labels out if they cannot be removed.

It is recommended that departments seal and sequester any returned boxes and place labels on them indicating that they are subject to a disposition hold in order to discourage tampering with the boxes.

## **6. Procedures – Boxes In Storage and Not Yet Ready for Final Disposition**

6.1 Disposition holds can be placed on boxes that are in storage in a records centre and that have not yet reached the final disposition phase of the life cycle.

6.2 The Department Records Management Team obtains a letter from the Director or Regional Superintendent responsible for the records advising that records must be halted.

6.3 The Department Records Management Team forwards the letter to Enterprise Records Management.

6.4 An ERM records analyst will add the boxes to a disposition hold in DIIMS.

## **7. Procedures – Lifting a Disposition Hold**

7.1 Disposition holds may be in place for many years. However, it is important for space management within the GNWT records centres that disposition holds are lifted as soon as possible.

- 7.2 From time to time, the Manager, Enterprise Records Management, may provide Department Records Management Teams with a list of boxes in storage in the records centres that are in a disposition hold. The Manager will ask the Department Records Management Teams to review the list and provide written confirmation as to whether the disposition hold still applies or not.
- 7.2.1 If the disposition hold is still in place, an e-mail message from the Department Records Management Team confirming that the hold is in place provides sufficient documentation for ERM's purposes.
- 7.2.2 If the disposition hold can be lifted, the Department Records Management Team obtains a letter from the Director or Regional Superintendent responsible for the records advising that the disposition hold may be lifted.
- 7.2.3 The Department Records Management Team forwards the letter and a list of the boxes to which the letter applies to Enterprise Records Management.
- 7.2.4 An ERM records analyst will remove the boxes from the disposition hold in DIIMS.
- 7.3 If the boxes are ready for final disposition when the disposition hold is lifted, the Department Records Management Team must submit a new request for disposition to Enterprise Records Management, with a new disposition authorization letter signed by the Director or Regional Superintendent.

## **Vital Records and Emergency Management**

## 5001 About Vital or Essential Records

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Vital records, also called essential records, are records which either:

- Contain information essential for the continuation of key GNWT programs, services, or operations during and immediately after an emergency; or
- Contain information essential for the re-establishment of the primary legal, financial, and functional responsibilities of the GNWT following a disaster.

Only a portion of the GNWT's records are vital or essential to the government's core responsibilities over natural resources, education, health care, social services, policing and the administration of justice, and other matters of a local or private nature in the territory. Vital records also include records which are needed to recreate the GNWT's legal and financial position, and protect its obligations to the public, employees, and contractors. Vital records are records the GNWT absolutely cannot do without.

Vital records are:

- Irreplaceable,
- Required to operate a department or agency's most significant programs and services; or
- Have an intrinsic uniqueness.

The NWT Emergency Plan, departmental emergency plans, and essential services lists are good sources of information for identifying the programs and the related records which are considered critical to fundamental government and departmental operations.

The term "vital records" should not be confused with "Vital Statistics Records" which are records of births, marriages, deaths, and other life events.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, ICT Policy 6003.00.18

[A Guide to Business Continuity Planning](#), Office of Critical Infrastructure Protection and Emergency Preparedness, Government of Canada.

[The Preservation of Essential Records: A guide for governments, organizations, institutions, and businesses](#), Emergency Preparedness Canada, 1996 (out of print).

Emergency Management for Records and Information Programs, 2<sup>nd</sup> edition, Virginia A. Jones and Darlene Barber, ARMA International, 2011.

Vital Records, TR 29-2017, ARMA International.

### **3. Guidelines**

- 3.1 It is recommended that GNWT departments and agencies establish vital records programs as part of their overall records management programs, emergency management programs, or business continuity programs. Vital records programs support the information governance principle of protection.

### **4. Procedures**

- 4.1 Obtain senior management approval to develop a vital records plan.
- 4.2 Identify and prioritize the business operations which are critical during and immediately after an emergency or disaster.
- 4.3 Prepare an information map and use it to identify the vital records which support the critical business operations. Assess the following:
- Locations and formats of the records.
  - Identify existing backups or duplicates, such as network backups, or business process that duplicate information between a regional office and headquarters. Determine if the duplicates and backups are complete.
- 4.4 Identify potential risks to the information, such as fire, water damage, pest damage, theft, cyberattacks, etc., and complete a risk assessment and business impact assessment for each possible hazard.
- 4.5 Identify mitigation steps to reduce the loss risk and determine the mitigation costs. These costs are usually associated with the creation and maintenance of backup copies of vital records in an alternate location.
- 4.6 Write the vital records plan and obtain senior management approval to implement the plan.
- 4.7 Implement risk mitigation steps.
- 4.8 Routinely monitor, test, and update the plan.

## 5501 About Emergency Management Planning for Records

<b>Issued:</b>	December 2021
<b>Last Updated:</b>	December 2021

### 1. Introduction

Accidents, emergencies, and disasters are part of life. While the focus in any event is the health and safety of employees and the public, consideration should be given to the protection and remediation of records which may be vulnerable to or damaged by natural and human caused events.

Emergency management planning is a component of a well-rounded records and information management program. Records remediation is an unfortunate consequence of accidents, emergencies, and disasters.

Paper records and records in other physical media are vulnerable to damage from many sources, such as fire, water, dust and mold, pests, and more. Electronic records are also vulnerable to damage, particularly if they are stored locally on computer hard drives or on removable media, such as a flash drive, external hard drive, or DVD.

The NWT Archives and Enterprise Information Management (EIM) provide advice to GNWT departments and agencies on emergency management planning and recovery of damaged records. EIM also has a reference collection of records-related to emergency planning and response publications which is available for consultation.

Please see Appendix D for an example of a flow chart for salvage and recovery of damaged records.

### 2. References

NWT Archives, *Are Your Records Safe? The Emergency Management Continuum*, presentation to the 2020 Records and Information Management Symposium. Available as an [online module](#) on the My HR Learning and Development site.

Enterprise Information Management, *Disaster and Emergency Response Handbook for Government Records*, draft under development.

Alberta, Public Works, Supply and Services, *Disaster Planning for Government of Alberta Records*, PWSS 149, 1987.

Betty Walsh, *Salvage Operations for Water Damaged Archival Collections; A Second Glance*, Preservation Committee, Canadian Council of Archives, 2003.

Canada, Office of Critical Infrastructure and Emergency Preparedness, *A Guide to Business Continuity Planning*, 2003.

Canadian Conservation Institute, *Emergency and Disaster Preparedness for Cultural Institutions*, no date.

Institute for Inspection Cleaning and Restoration Certification, *Reference Guide for Professional Mold Remediation*, 3<sup>rd</sup> edition, 2015.

Institute for Inspection Cleaning and Restoration Certification, *Standard and Reference Guide for Professional Water Damage Restoration*, 4<sup>th</sup> edition, 2015

Institute for Inspection Cleaning and Restoration, *Standard for Professional Mold Remediation*, 3<sup>rd</sup> edition, 2015.

Johanna Wellheiser, Jude Scott and John Barton, *An ounce of prevention: Integrated disaster planning for archives, libraries, and records centers*, 2<sup>nd</sup> edition, 2002.

Rosalie Stremple and Michael F. Martone, *Disasters Come in All Sizes*, InfoPro, 2000.

State Archives and Records Authority of New South Wales, *Counter disaster reaction and recovery plan*, 2019.

Virginia A. Jones and Darlene Barber, *Emergency Management for Records and Information Programs*, 2<sup>nd</sup> edition, ARMA International, 2011.

## **Electronic Records**

## 6001 About Electronic Records

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

An electronic record is a record stored in an electronic or digital format which can only be processed by a computer or another digital device. Some examples of electronic records include, but are not limited to:

- MS Word documents
- MS Excel spreadsheets
- E-mail messages
- Digital photographs and other digital images
- CAD files
- PDF documents
- Digital sound or video recordings
- Other computer files that store information.

Electronic records can also come from paper documents and analogue audio-visual materials which were digitized. Databases, information systems, and GIS systems are not usually considered by the GNWT to be records, but the reports and other documents they generate may be records which need to be saved external to the system.

Most records created and used by GNWT departments are born digital – meaning that they were created as an electronic record rather than as a paper document. Electronic records document the GNWT’s business activities, and are affected by the same legal, audit, and other requirements as paper records:

- They may be presented as evidence in an investigation or court proceedings.
- They may be requested as part of an access to information request.
- Laws that require records to be kept apply equally to paper and electronic records.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Management of Electronic Information Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Every government department and agency is responsible and accountable for the management of its electronic records. Electronic records which document government actions, transactions, and decisions should be saved into DIIMS, where available. In departments which have not implemented DIIMS electronic documents should be saved on GNWT network file shares.

Agencies, boards, commissions, and crown corporations may have their own document management systems which is the preferred method for storing and managing their electronic records.

- 3.2 Electronic records should not be stored locally on computer hard drives, tablets, smartphones, or on external hard drives because these storage locations are vulnerable to security and privacy breaches. In addition, computer hard drives and mobile devices are not included in GWNT network backups and so records saved on them may be lost if the hard drive or device fails or becomes corrupted.
- 3.3 Processes for managing electronic records should be put in place to ensure records are reliable, secure, and compliant with legal, business, and other requirements, comprehensive, and created, captured, and managed systematically.
- 3.4 In consultation with the Department Records Management Team, each government program area should decide if its official or master records will be kept as electronic records, paper records, or in other media. This decision should be documented and saved with other documentation about the records and information management program in order to promote consistency in employee practices and to support the authenticity and reliability of the records (e.g. ARCS V10 6215-00, Records Management - Policies and Procedures).

Program related legislation should be reviewed to determine if the legislation specifies a format in which records must be kept. Obtain a legal opinion if the legislative requirements are unclear.

- 3.5 In consultation with the Department Records Management Team, each government program should develop procedures for managing electronic records. Procedures should address appropriate storage and organization of electronic records and naming conventions.
- 3.6 In consultation with the Department Records Management Team, supervisors are responsible for ensuring employees receive training on the creation, capture, storage, use, distribution and tracking, closing, retention, and disposition of the electronic records which they create, receive, and use while carrying out their work.
- 3.7 In consultation with the Department Records Management Team, supervisors are responsible for regularly monitoring and evaluating compliance with the program area's

records and information management procedures. Corrective actions should be taken to address any failures to comply with the procedures.

- 3.8 Department Records Management Teams may choose to consult with Enterprise Records Management on the development of procedures and methods for monitoring and evaluating compliance.

## 6100 Managing Electronic Records Using DIIMS

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

DIIMS, the Digital Integrated Information Management System, also known as OpenText Content Server, is the preferred electronic content management system (ECMS) for GNWT departments, the NWT Housing Corporation, and the Legislative Assembly.

The purpose of DIIMS is to do the following:

- Enhance the productivity of the GNWT's employees.
- Facilitate collaboration and sharing of information.
- Provide a tool for the effective management of e-mail messages.
- Reduce storage costs associated with maintaining information in electronic formats.
- Effectively manage the government's electronic records in compliance with the *Archives Act* by providing a mechanism for classifying and scheduling electronic records in accordance with the Administrative and Operational Records Classification Systems (ARCS and ORCS).

During the 2009-2010 IM-IS-IT Capital Planning cycle, the Government Chief Information Officer received approval from the Informatics Policy Council (IPC) to issue a Request for Proposal for an electronic content management system for all GNWT departments, the Legislative Assembly, and the NWT Housing Corporation. The contract was awarded to OpenText Content Server and the system was successfully piloted in the Department of Public Works and Services in 2012. Subsequent to the pilot, IPC approved the continued implementation of the system across the government.

DIIMS is supported by the Enterprise Content Management (ECM) section of Enterprise Information Management. ECM works with Department Records Management Teams to support the management of departmental electronic records.

### 2. References

Management of Electronic Information Policy, IMT Policy Manual

DIIMS End User Guide

### 3. Guidelines

- 3.1 DIIMS should be used to store non-transitory e-mail messages and draft and final versions of electronic documents relating to government business.

- 3.2 DIIMS is organized into a hierarchy of digital folders. The folder structure is based on the file classification hierarchy found in the Administrative and Operational Records Classification System (ARCS and ORCS). When electronic documents are saved into an ARCS or ORCS folder in DIIMS, they inherit the ARCS or ORCS classification and retention schedules.

Because the upper level folders in the DIIMS folder structure are tied to an approved ARCS or ORCS classification structure, they cannot be added to, deleted, or modified unless the underlying ARCS or ORCS is amended. DIIMS users may have the ability to add and modify the folder structure at lower levels in the DIIMS folder hierarchy depending on their system permissions. Contact the Departmental Records Management Team for assistance with using the ARCS and ORCS. Online ARCS and ORCS training is also available from Enterprise Information Management through the HR Training Calendar.

Security and access restrictions are assigned to the ARCS and ORCS folders. Some folders are available to all employees in a program area, or even to an entire department. Other folders have been restricted to protect personal or confidential information. Contact the Department Records Management Team or the DIIMS Help Desk before saving personal or confidential information to make sure that the information is being saved into a folder which has the appropriate security settings.

- 3.3 Documents and folders are easier to locate if consistent file naming conventions or rules are followed. Program areas should consult with the Department Records Management Team to determine if the department already has file naming conventions or to establish naming conventions if none already exist. File naming conventions for DIIMS should be documented in departmental records and information management procedures manuals.
- 3.4 Managers and supervisors are responsible for ensuring employees have received training on the use of DIIMS. They are also responsible for monitoring DIIMS usage to ensure it is being used in compliance with GNWT-wide and departmental procedures.
- 3.5 DIIMS allows multiple users to collaborate on documents within and between departments. This ensures there is a single, authoritative, version of a record by reducing the duplication of records across the government. Management approval should be obtained before sharing documents with employees in different program areas and caution should be exercised at all times to prevent the release of private and confidential information.
- 3.6 Many routine business processes are supported by DIIMS workflows. In addition to streamlining and automating tasks, workflows ensure that electronic documents are saved into the most appropriate location in DIIMS, where they can be managed according to ARCS and ORCS. They also provide opportunities for increasing oversight of processes through reporting and auditing.

## 6200 Managing Electronic Records on Network File Shares

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

GNWT departments which have not implemented DIIMS usually use network file shares (shared drives) as the primary repository for their electronic records. Electronic records are public records and must be managed in compliance with the *Archives Act* and GNWT policies. Network file shares need to have records and information management controls applied to them to make the information easier to find and use, comply with legal and other requirements for managing records, and reduce storage costs. Effective use of network file shares for managing electronic records requires training, monitoring, and clear procedures.

DIIMS is the preferred GNWT solution for managing the government's electronic records. Network file shares lack some important recordkeeping features which are found in DIIMS. These features include strong search capabilities, audit trails, and the ability to automate retention and disposition rules.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Management of Electronic Information Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Department Records Management Teams should have access to all departmental network file shares so they can effectively manage the content of the network file shares through their life cycle.
- 3.2 In departments which have not implemented DIIMS, network file shares should be used to store non-transitory e-mail messages and draft and final versions of electronic documents.
- 3.3 Folders in network file shares should be organized into a folder hierarchy based on the classification structure of the Administrative and Operational Records Classification Systems (ARCS and ORCS). For example:

- 📁 Divisional ORCS
- 📁 Administration
  - 📁 1000 Administration – General
  - 📁 1015 Departmental Meetings
    - 📁 1015-25 Meetings
      - 📁 Staff Meetings 2019-2020
      - 📁 Staff Meetings 2020-2021
  - 📁 1025 Planning and Organization
- 📁 Buildings and Properties
- 📁 Equipment and Supplies
- 📁 Finance
- 📁 Human Resources
- 📁 Information Management and Services

Using ARCS and ORCS to organize electronic records on network file shares helps match up the paper filing system to the electronic one, which encourages better searching and retrieval of information. It also facilitates the response to access to information requests, legal actions and investigations, and audits by encouraging consistency in the management of departmental information across locations and document formats. It also helps prepare the department for eventual implementation of DIIMS.

- 3.4 Using password protections and other user managed tools for preventing access to information may render the information unusable to the GNWT if the person who set up the restrictions is unavailable, or the password is forgotten. Consult with the Technology Service Centre (TSC) for options to secure records stored on network shared drives.
- 3.5 Documents and folders are easier to locate if consistent file naming conventions or rules are followed. Program areas should consult with the Department Records Management Team to determine if the department already has file naming conventions or to establish naming conventions if none already exist. File naming conventions for network shared drives should be documented in departmental records and information management procedures manuals.
- 3.6 Managers and supervisors are responsible for ensuring employees have received training on the use of network shared drives. They are also responsible for monitoring network file share usage to ensure it is being used in compliance with GNWT-wide and departmental procedures.
- 3.7 Duplication of information is a concern for network shared drives. Departments should encourage the consistent use of the ARCS and ORCS folder structure to reduce duplication, encourage the creation of a single, authoritative, electronic record, and reduce network storage chargeback costs.
- 3.8 Deleting records from a shared drive is a form of disposal and must only occur in compliance with the *Archives Act* and approved records disposition authorities. Substantive,

or non-transitory, records should not be deleted. Instead they should be retained on the network file share until they can be imported into DIIMS. The GNWT does not have a policy or procedure governing the disposal of substantive electronic records outside of DIIMS, so the disposal of these records is not advisable. Employees may delete transitory records.

- 3.9 Personal network drives – usually the G:/ drive – should not be used as the final repository for GNWT business-related records.

## 6400 Disposal of Electronic Records

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Electronic records are subject to the same records retention and disposition requirements as their paper counterparts. The disposal of records is part of the ordinary and normal business of government. Almost all government records will eventually outlive their usefulness to the department or agency that created them and keeping records longer than necessary is a liability to the government.

The length of time that records should be kept by a government department or agency is identified in records disposition authorities (RDAs). RDAs also identify the mode of final disposition. The Territorial Archivist reviews and authorizes the disposal of records in accordance with the retention schedules and final dispositions outlined in the records disposition authorities.

Disposing of records without the authorization of the Territorial Archivist is a violation of the *Archives Act*. Anyone who damages or mutilates a record, removes a record from a government office, or destroys a record without authorization from the Territorial Archivist is guilty of an offence and is liable on summary conviction to a fine not exceeding \$5,000, or to imprisonment for a term not exceeding one year, or to both.

### 2. References

Archives Act, R.S.N.W.T 1998, c.A-6

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Management of Electronic Information Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

Information and documentation – Records management – Part 1: Concepts and principles, International Organization for Standardization, ISO 15489-1:2016.

### 3. Guidelines

- 3.1 The GNWT does not have a procedure addressing the disposal of electronic records stored on network shared drives. Disposal of electronic records in the absence of a standard procedure is not advisable because it is not part of the government's normal and ordinary

course of business and consequently could lead to questions concerning the validity of the disposal actions.

Departments which are not using DIIMS to manage electronic records should keep all substantive electronic records on their shared drives until the retention and disposition of the records can be managed through DIIMS.

3.2 The GNWT has procedures for the disposal of electronic records stored in DIIMS. The procedures meet the GNWT's requirements for the retention and disposal of records under the *Archives Act*. These requirements are:

- Electronic records must not be disposed of except in accordance with the retention and disposition set out in an approved RDA.
- Electronic records must not be disposed of unless they have reached the final disposition phase of their life cycles as identified in an approved RDA.
- Substantive and transitory records relating to pending or current litigation, legal actions, investigations, audits, or Access to Information requests should not be disposed of while that activity is underway or anticipated.
- All actions relating to disposition of substantive records must be documented.

3.3 The NWT Archives is not acquiring electronic records at this time. Electronic records with a final disposition of Archival Selection (AS/D) must remain in departmental custody and control until such time as the NWT Archives is able to acquire the records.

3.4 Transitory electronic records may be disposed of (deleted) by government employees who created or received them, providing that the electronic records meet the requirements of the *Transitory Records Schedule* (RDA 1997-02) and are not required to document their actions, transactions, or decisions.

#### **4. Procedures – Disposition from DIIMS**

4.1 Once per year, Enterprise Information Management (EIM) initiates a Disposition Approval Workflow in DIIMS. This workflow identifies records which are ready for disposition according to the retention and disposition schedules assigned to the records in DIIMS.

4.2 Each department's Records Management Team will be asked to assist in the verification of the list of senior managers for each department.

4.3 An e-mail is sent from EIM's Enterprise Records Management unit (ERM) to the senior manager for each division. The e-mail will include a link to a workflow status page. Departmental Records Management Teams will be copied on these e-mails.

4.4 From the workflow status page, the senior manager will be able to review a report of records stored in DIIMS which are ready for disposition. An electronic record of their review activities will be generated by DIIMS and kept by EIM. The department records management team will receive a notification from DIIMS when the review activity is complete.

The senior manager will also be able to indicate if any of the boxes need to be kept for another year due to a current legal matter, audit, or access to information request.

- 4.5 EIM's Electronic Content Management (ECM) unit will begin the process of disposing of the records from DIIMS when they receive notification from DIIMS that the review activity is complete.
- 4.6 If the senior manager does not complete the review of the records by the end of the 90-calendar day review period, they will be deemed to have approved the disposition, and ECM will begin the process of disposing of the records.
- 4.7 The Department Records Management Team will be notified when all the records have been disposed of.

## 6430 Disposal of Transitory Electronic Records

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

The [Transitory Records Schedule](#) (Records Disposition Authority 1997-02) provides authorization to GNWT departments and agencies to dispose of transitory records in compliance with the *Archives Act*.

The Transitory Records Schedule identifies six record types that can be disposed of as transitory records:

- Advertising material.
- Blank information media.
- Draft documents and working materials that were used to create a final document, and which are not required to show the various stages in the development of the final document or to record decisions.
- Duplicate documents.
- Non-GNWT Publications.
- Temporary information that is not required to document actions or decisions or to demonstrate that an activity took place or that information was received.

The Transitory Records Schedule applies to records in all formats, including electronic records.

Save electronic records which are not transitory into the department's recordkeeping system (DIIMS, a network file share, or a paper file) as an original, master record.

### 2. References

Archives Act, R.S.N.W.T 1988, c.A-6

Financial Administration Act: Disposal of Public Property Regulations, R-047-93

Infrastructure Establishment Policy, Executive Council Policy 31.00

Disposal of Goods Policy, Executive Council Policy 31.03

Recorded Information Management Policy, IMT Policy Manual

Management of Electronic Information Policy, IMT Policy Manual

Scheduling and Disposition of Electronic Mail Messages Directive

## RDA 1997-02 Transitory Records Schedule

### Disposal of Surplus Goods Guidelines

#### 3. Guidelines

- 3.1 Government employees may identify and dispose of electronic transitory records themselves.
- 3.2 Transitory electronic records do not have to be inventoried prior to disposal.
- 3.3 Transitory electronic records must be protected and securely disposed of to maintain security, confidentiality, protect personal privacy, and prevent information security breaches.
- 3.4 Transitory electronic records should be deleted from hard drives, network file shares, Outlook e-mail accounts, and any other location where they have been stored on a regular basis, such as weekly or monthly.

Ideally, transitory records are deleted as soon as it is determined they have no further use. For example, junk e-mail should be deleted immediately. In another example, a convenience or reference copy of a new procedure can be deleted after it has been read and understood because the master copy of the procedure is available in DIIMS or on the network file share.

- 3.5 Hard drive recycling bins should be emptied on a regular basis, such as once a month.
- 3.6 Outlook should be set to automatically delete items in the Deleted Items folder on a set schedule, such as when Outlook is closed or after a certain number of weeks or months have passed. Deleted items should not be retained for more than 12 months.
- 3.7 Outlook has a Recovered Deleted Items from the Server option. Items emptied out of your Deleted Items folder are moved to a separate location where they are stored for a period of time according to Technology Service Centre (TSC) policy.

Do not permanently delete items from the Recovered Deleted Items location unless instructed to do so by the TSC to control a malicious e-mail.

Deleting items from the Recovered Deleted Items location is known as “Triple Delete.” The practice of Triple Delete has exposed other governments to negative publicity and individual employees working for those governments have been fined and faced legal charges due to the destruction of evidence or the destruction of information required in response to an access to information request.

The GNWT is best served by allowing network storage and deletion policies to operate as designed.

- 3.8 For departments implemented on e-mail management, e-mails will be automatically “stubbed” and archived in the DIIMS e-mail archive.

E-mail messages which do not contain transitory information should be saved into the appropriate folder in DIIMS' Enterprise Workspace. DIIMS will save the entire e-mail message, not just the stubbed e-mail.

Stubbed e-mails will be automatically deleted from the e-mail archive as transitory records in compliance with timeframes established in the *Scheduling and Disposition of Electronic Mail Management Directive*.

Contact your Departmental Records Management Team or the DIIMS Help Desk to find out if your department has implemented e-mail management.

- 3.9 Information media, such as hard drives, USB devices (external hard drives, flash drives, thumb drives, etc.), memory cards (SD, miniSD, microSD, CF, MMC, etc.), optical storage disks (DVDs and CDs), 5.25” and 3.5” floppy disks, audio tapes, video tapes, and data tapes, should be erased or have their contents deleted. The media should then be sanitized using specialized data erasure software, degaussed, or physically destroyed to prevent the unauthorized recovery of information that was previously stored. Physical destruction may be done by shredding in a specialized shredder, disintegrating, pulverizing, or otherwise destroying the information bearing medium so that it cannot be reconstructed and played. File deletion or reformatting alone is not sufficient to destroy the information stored on the media.

## **Paper Records and Other Media**

## 7001 About Paper Records and Other Media

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

This guidance is not intended to replace existing departmental records and information management rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

#### 1.1 Paper records

Paper records are public records which are created, received, and kept in a paper format. Typically, they consist of documents printed or written on letter or legal sized paper, are placed in file folders, or occasionally binders, and are kept in office filing cabinets. They might also be bound into a ledger or register. They are “traditional” records and are closely associated with the government’s formal records management policies and procedures.

Modern paper records are usually “born digital”, or created on a computer, and then printed for storage purposes or so they can be signed. Some paper records begin their life as a paper document. These “born analogue” records include hand written documents, forms that were filled out by hand or using a typewriter and printed documents received in the mail.

If a person prints a document because it is easier to read and use on a printed page, but their office has decided the master or official record is the electronic record stored in DIIMS or on a shared drive, then they have created a “convenience copy.” A convenience copy is not considered to be an official government record. Convenience copies are transitory records and should be placed in an office document disposal bin or shredded using a cross-cut office shredder.

#### 1.2 Other media

Other media refers to records which are not electronic (digital) records and which are stored on physical media other than letter or legal sized paper documents. Some examples of other media include photographs, photographic film and slides, printed maps and blueprints, images stored on microfilm or microfiche, and audio-visual materials stored on audio tape, video tape, or film.

### 2. References

Archives Act, R.S.N.W.T. 1998, c.A-6

### 3. Guidelines

- 3.1 Each government department and agency is responsible and accountable for the management of its paper records and records in other media. Processes for managing paper records and records in other media should be put in place to ensure records are reliable, secure, and compliant with legal, business, and other requirements, comprehensive, and created, captured, and managed systematically.

Enterprise Information Management recommends using DIIMS to automate and support the control and management of the records from the time they are created through to final disposition.

- 3.1 In consultation with the Department Records Management Team, each government program area should decide if its official or master records will be kept as paper records, in other media, or in an electronic format. This decision should be documented and saved with other documentation about the records and information management program in order to promote consistency in employee practices and to support the authenticity and reliability of the records (e.g. ARCS V10 6215-00, Records Management - Policies and Procedures).

Program related legislation should be reviewed to determine if the legislation specifies a format in which records must be kept. Obtain a legal opinion if the legislative requirements are unclear.

- 3.2 In consultation with the Department Records Management Team, each government program should identify the storage area or areas where official paper records and records in other media will be kept. This decision should be documented and saved with other documentation about the record and information management program in order to promote consistency in employee practices and to support future communication and training for employees.

- 3.3 In consultation with the Department Records Management Team, each government program should develop procedures for managing paper records and records in other media. It may be useful to support these procedures with checklists. These procedures and checklists may form part of a departmental records and information management procedures manual. Procedures should address the following:

- Designation of responsibilities for managing paper records and records in other media. This includes identifying the employee positions which interact with the records and have responsibilities for their creation, capture, distribution and tracking, and life cycle management.
- How new paper files will be created and officially opened, including creation of new volumes of existing files.

- Enterprise Information Management recommends using DIIMS to open files and volumes because it allows departments to keep track of all records as assets and improves one's ability to search for and locate files. DIIMS reports can be used to create lists of all files and volumes belonging to a department.
  - Some DIIMS workflow applications automatically create files, volumes, and file labels for new paper files.
  - If DIIMS is not used to manage paper files and records in other media, they should be listed on a manual file list.
- How records in other media will be created.
  - Naming conventions for paper files and records in other media.
  - Labeling requirements, including use of DIIMS file labels.
  - Tracking procedures, such as procedures to charge files in and out of the filing system, to ensure the chain of custody is maintained.
  - Sharing of records between offices and regions, including identifying the location of the master record.
  - Volume and file closing procedures.
- 3.4 In consultation with the Department Records Management Team, supervisors are responsible for ensuring employees receive training on the creation, capture, storage, use, distribution and tracking, closing, retention, and disposition of the paper records and records in other media which they create, receive, and use while carrying out their work.
- 3.5 In consultation with the Department Records Management Team, supervisors are responsible for regularly monitoring and evaluating compliance with the program area's records and information management procedures. Corrective actions should be taken to address any failures to comply with the procedures.
- 3.6 Department Records Management Teams may choose to consult with Enterprise Records Management on the development of procedures and methods for monitoring and evaluating compliance.

## 7100 Active Filing of Paper Records

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Filing paper records is not difficult. It must be done regularly to prevent backlogs from piling up. Consistent filing and management of paper records ensures the records are readily available to those who need them.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T. 1988, c.A-6

Recorded Information Management Policy, IMT Policy Manual

RDA 1997-02, Transitory Records Schedule

### 3. Guidelines

3.1 Before beginning to file paper government records, the Department Records Management Team should be contacted to discuss any questions about the Administrative Records Classification System (ARCS), the department's Operational Records Classification System (ORCS), the file classification numbers used by the program area, or departmental filing procedures.

3.2 All paper records should be listed or registered to manage them as a government asset.

Most government departments use DIIMS to list and keep track of their paper files. Using DIIMS to manage paper files from the moment the file is created greatly enhances the government's ability to manage paper records through their life cycle. Some departments may be using a Word document or spreadsheet to list their paper files instead of using DIIMS.

DIIMS and file lists are important tools for managing paper records. They help the GNWT ensure that records are created and captured in a way that supports legal and business requirements to keep evidence of the government's business activities. They help manage records as valuable government assets. They also help support actions which keep records secure from unauthorized disclosure or disposal, searchable and available to authorized

personnel, maintained in compliance with the *Archives Act*, and securely disposed of at the end of their life cycle.

DIIMS and file lists capture metadata about the records which describes their context, content, and structure. Metadata is an important component of records as it supports retrieval and understanding and verifies the authenticity and integrity of the records over time.

File lists of paper records should, at minimum, do the following:

- Assign unique identifiers to the file, such as the file number, volume number, and file title.
- Identify the date the file was created/opened and the date it was closed.
- Create relationships to other records, by classifying the record into ARCS and ORCS.
- Identify the location where the file is stored.

DIIMS captures all the necessary metadata to support the management of the paper records.

## 4. Procedures

4.1 Before filing paper records, sort them to identify the official or substantive records (master) which must be kept as documentation of the government program's policies, procedures, actions, transactions, interactions with others, and decisions.

Separate out and securely dispose of transitory records, such as duplicate copies, handwritten notes which were transcribed into a final document, etc. Refer to the [Transitory Records Schedule](#) for assistance in identifying records which are considered transitory.

4.2 To file individual paper records:

- Look over each record and identify its purpose.
- Look through DIIMS or the file list to find out if a physical file already exists for each record. If a file exists, write the file number on the upper right hand corner of the first page of each record. Place the records in the file in reverse chronological order, so that the most recent record is on top and will be the first document seen when the file folder is opened.
  - If the existing file is full, you will need to close off the first volume and create a second volume of the same file. Update DIIMS or the file list with the closed date for the volume, then enter a new volume with the same file number and file title, the new volume number, and the new date range. Create a new label for the new volume.

- It is important that each volume of a file is inventoried separately in DIIMS or on file lists. Otherwise, volumes may go missing and important information may be lost.
- If a file does not already exist, look up the file classification number in ARCS or ORCS. Write that number on the upper right hand corner of the first page of the document. Add the file to DIIMS and use DIIMS to print a barcoded label for the new file, or add the file to the file list. Place the records in the file in reverse chronological order, so that the most recent record is on top and will be the first record seen when the file folder is opened.

4.3 You may have a record that could be filed into more than one file folder. One solution to this problem is to cross-reference the files. Write all of the possible file numbers in the upper right hand corner of the record. Place an “X” in front of the file numbers that contain related information.

Example:           1145-30-01  
                       X 0549-02-03  
                       X 0549-02-10

The record is filed in the first file folder. A cross-reference sheet is put in the other file folders to tell you to look in the first folder for the record. This is similar to using shortcuts to link electronic records together in DIIMS or on a network shared drive.

4.4 Establish a file charge-out system to keep track of the location of files and maintain a chain of custody. Every paper file should have a home location where it is usually stored. A file’s home may be a central filing area, central registry, or individual offices, depending on the filing procedures for each department.

A file charge-out system involves making a charge-out record every time a file is removed from its home location. The charge-out record should keep track of which file was taken, who took it, and the date on which it was removed. The charge-out record should be updated every time the file moves from one person to another. This way the chain of custody is maintained and the file can be located.

Different types of charge-out systems include the following:

- Charge-out guides are available from office supply stores. Cardboard guides usually have a space on them to write the file number, file title, and the name of the person who took the file. Plastic guides usually have a clear pocket to place a paper charge-out slip. After filling out the guide or the slip, place the guide in the filing cabinet in place of the file which was removed. The guide is removed from the filing cabinet when the file is returned.

- Sign-out sheets may be handwritten or stored in a Word document or spreadsheet. They are filled out every time a file is removed from the filing cabinet and updated when the file is returned.

## 7110 Filing Equipment and Supplies

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

The GNWT does not have specific standards for filing equipment and supplies. There are benefits, however, to standardizing filing equipment and supplies within an office or a department, such as cost savings from bulk purchases of supplies and the ability to reuse surplus equipment.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T. 1988, c.A-6

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines - Filing Supplies

- 3.1 Departmental standards for filing supplies should be identified in departmental records and information management procedure manuals.
- 3.2 Choose the size of file folder to be used in the office. The size of file folder may be dictated by the office furniture and filing cabinets available in the workplace. Most offices in the GNWT use legal size file folders (9½" x 14⅝" or 241mm x 371mm exclusive of tabs). Legal sized files are slightly more expensive than letter sized files and take up a little more floor space, but documents are less likely to fall out and it is not necessary to fold legal sized documents.
- 3.3 Consider the weight of the file folders. File folders are made from different weights of paper. Choose heavier weight file folders for files that are used frequently or will hold a large volume of material. Lighter weight file folders can be used for files which are not used as frequently.
- 3.4 Consider using archival quality acid-free file folders for files which have a long retention period (over 20 years). Using acid-free folders will help prolong the life of the records.
- 3.5 Consider using pocket or accordion style folders when you have large volumes of material which cannot be split up easily into volumes of regular file folders. Pocket folders are also

useful when you want to file small pieces of paper which might fall out of a regular file folder.

- 3.6 Consider using multi-part or classification folders for case files which contain many different types of documents which need to be referenced quickly. Multi-part folders have dividers in them to separate them into different sections. Each section can be used for each type of document.
- 3.7 Use suspension or hanging folders in drawer style filing cabinets. Suspension files have little hooks on them to hang in the filing cabinets and hold regular file folders. They can be re-used when the files are removed. Suspension files should not be used in place of a regular file folder because the hooks get caught on things and do not fit well in records centre boxes. The plastic or metal tabs must be removed before the folders can be shredded and recycled.
- 3.8 Consider whether your filing equipment is designed for top tab or end tab file folders. Tabs are the part of the folder that extends beyond the edge of the folder to provide a place for a label. Top tab file folders have a tab along one long edge of the folder. End tab file folders have a tab along one short side of the folder. Tabs come in different sizes. Choose a tab size wide enough to display your file label properly. Choose top tab folders for drawer-style filing cabinets and end tab folders for open style filing equipment.
- 3.9 Choose manila, buff, natural, or white file folders. File folders in other bright colours are more expensive, harder to recycle, and the colour may bleed and damage the papers inside the folders if they get wet or are stored in humid conditions. If using coloured file folders, use the colours to identify a specific group or category of files or to separate files into different fiscal years.
- 3.10 Be aware that Mylar reinforced file folders may be difficult to recycle because of the polyester coating.
- 3.11 Single or two prong fasteners can be used to hold documents in place and prevent documents from spilling out of file folders.
- 3.12 DIIMS prints folder labels on 3¼" x 4" or 82.5mm x 101.6mm laser printer labels (e.g. Avery 5164 or equivalent).

#### **4. Guidelines - Filing equipment**

- 4.1 Departmental standards for filing equipment should be identified in departmental records and information management procedure manuals.
- 4.2 There are four commonly used types of filing cabinets. Each type of system has good and bad points. If you choose your filing cabinets carefully you will increase the efficiency and cost effectiveness of your department's records management program.

- **Vertical Filing Cabinets:** files are placed or hung in a drawer and are arranged from front to back with the top tabs facing the front of the drawer.
- **Lateral Filing Cabinets:** files are placed sideways in the drawer and are usually read from left to right. The top tabs face the left side of the drawer.
- **Open Shelf:** files are stored on shelves, similar to a bookcase, or in boxes which are attached to a rack or frame. They come in open and locking models. For security, open models should only be used in filing areas which are secured behind locked doors with no public access. Open shelf systems use end tab file folders and are read from left to right, with the tab usually facing the left end of the shelf or row.
- **Mobile Filing Systems:** mobile filing systems are designed to maximize storage space and minimize retrieval times. Usually they feature open shelf filing mounted on a track, which allows more shelves to be placed in a given area. The systems have significant weight and may require reinforcements to the floor. Consult with the Department of Infrastructure before installing mobile systems.

4.3 There are a number of things to consider when buying filing cabinets and other records storage equipment such as map cabinets, microfilm cabinets, and fireproof vaults.

- **Space Restrictions:** office space is expensive so choose filing cabinets which make the best use of the office space. When measuring for filing cabinets, remember to include the width and depth of the cabinet, the space that you need to pull out a drawer (for vertical and lateral cabinets), and the space you need to stand in front of the cabinet. Consult with the Department of Infrastructure regarding the height of the cabinets as they must not be too close to ceiling sprinkler heads.
- **Safety:** look for filing equipment which incorporates safety features. Filing equipment should be arranged to avoid reaching, extending, and bending. Step stools and ladders should be provided if required to help with access to the equipment. Take appropriate precautions, such as providing gloves, to prevent papercuts. Dust masks and gloves may be needed for handling older, dusty records. Carts may be required to help with transporting and carrying large numbers of files or heavy boxes full of files. Employees should be trained to have only one drawer in a vertical or lateral filing cabinet open at one time, to reduce the risk of tipping the cabinet forward.
- **Storage Requirements:** to figure out how much storage space you need, first inventory your active records and determine how many linear metres you have for each category of file. Then figure out your future needs by looking at how fast the volume of files grows each year and how long you need to keep the files on site in the office before sending them to a GNWT records centre for storage. For example, if you expect that the number of active files will grow by 10 percent per year and you need

to keep them on site for five years, you will need 50 percent more storage space than you have now. It is a good idea to include an extra 15 percent more storage space for contingencies.

- **Security Requirements:** all government records should be stored in areas which are secured from public access. Records requiring a higher degree of security should be stored in locking cabinets. You may want to store vital or essential records in equipment that has a high fire rating. Secure and fire safe cabinets are more expensive so they should only be purchased to meet a specific need.
- **Floor Load:** filing equipment has significant weight, especially when full, and may exceed floor load capacity. Consult with the facilities and properties division about the floor load before installing filing equipment. Mobile filing equipment and fireproof vaults are particularly heavy.
- **Equipment Cost:** determine what your requirements are for storage, space, and security before looking at how much the equipment will cost. Different types of cabinets have different storage capacities. When you compare prices, adjust the figures so that you are comparing costs for equal amounts of file storage space. Check with the GNWT's central warehouse services to determine if there are suitable surplus filing cabinets available before purchasing new.
- **Operational Cost:** the main ongoing cost is for filing supplies. Legal and letter sized file folders do not cost the same amount. Likewise, top tab and end tab file folders have different prices.
- **Physical Aspects of the Records:** the physical format of the records may make your purchasing decisions for you. Special media, such as maps, drawing and blueprints, film, magnetic audio and video tapes, and CDs and DVDs, may require special storage equipment.
- **Retrieval Efficiency:** consider how many people are using the filing equipment at the same time and how they will retrieve records from it. Open shelf filing systems let a larger number of people access the files at the same time. Vertical and lateral filing cabinets and mobile filing equipment work best if only one or two people are accessing the files at the same time. Consider physical abilities as well. Short people and people with limited mobility may not be able to reach files which are in the top drawer of a tall cabinet. Someone who uses a mobility aid may have difficulty working in tight spaces.

## 7111 File Labels

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

The GNWT does not have specific standards for how files are labeled. Departments using DIIMS have a variety of label formats available to manage paper records. Departments which manage their paper records using manual processes should set their own standards for labeling paper files. There are benefits to standardizing how file labels, particularly colour coded labels, are used. These include improving retrieval times because it is easier to find file numbers and titles if they are always located in the same position and the possibility of reducing costs through bulk label purchases. Labels printed from DIIMS have the added benefit of using barcode technology which reduces data entry time when boxing and preparing files for transfer to a records centre.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Departments that use DIIMS to manage paper files should use one of DIIMS' barcoded label formats. DIIMS uses 3¼" x 4" or 82.5mm x 101.6mm laser printer labels (e.g. Avery 5164 or equivalent) for file folder/volume labels.
- 3.2 Departments that do not use DIIMS to manage paper records should create standard formats for file labels. These standards should be documented in departmental records and information management procedures. For improved clarity, file labels should be typed rather than hand written. At minimum, file labels should contain the following information:
  - The ARCS or ORCS classification number (i.e. the file number).
  - The volume number.
  - The file name or title.
  - The open and closed dates of the file and the S/O date for files that have a superseded/obsolete (S/O) retention trigger.

It can be helpful if the retention schedule is also listed on the label.

- 3.3 Colour coded labels can be useful for retrieving files quickly and reducing misfiles. The human eye can read colours and colour sequences faster than it reads numbers. Colour coding files takes more time initially but can pay off by increasing retrieval times. They can be purchased from office supply stores or ordered from companies which specialize in filing supplies. Once you have chosen a certain brand of colour labels it is best to stick with the same brand to make sure that the colour sequence remains consistent over time.

Colour coded labels should be used in addition to a standard file label described in the preceding paragraphs.

Colour coding works best in large numeric filing systems with large numbers of case files and high levels of retrieval.

It is not necessary to colour code the full primary-secondary-tertiary file number from ARCS or ORCS. Instead, a guide can be used to indicate where each primary and secondary starts in the filing cabinet and only the unique tertiary level numbers need to be colour coded. For example, in a set of client files, use a guide to indicate where the client files begin in the filing cabinet, and then use colour coded labels for the unique client ID number.

Colour coded labels are available for both end tab and top tab file folders. Alphabetic, numeric, and date labels can be purchased:

- **Alphabetic or Numeric Labels:** coloured labels represent the numbers 0 through 9 or the letters of the alphabet. A strip of labels is added to each file, creating a colour representation of the file number. When the files are placed in the filing cabinet, bands of colour form across the file folders. This makes it easy to spot misfiles.
- **Date Labels:** coloured labels which represent dates. The most commonly used date labels are the yearly labels, which typically show the last two digits of each year (e.g. “21” for the year 2021). Monthly colour coded labels are also available. Colour coded date labels are used as a visual aid for identifying files that have date based file opening and closing criteria or where knowing the date the file or volume opened is important for retrieving the file. They are less useful for multi-year files. When using date labels for files that open and close on a fiscal year basis (April through March), use colour coded date labels to indicate the *beginning* of the fiscal year. For example, if a file was opened during the 2020-2021 fiscal year, a colour coded 2020 label would be used.

## 7200 Closing Paper Files

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Closing a physical file refers to the process of deciding that paper records will no longer be added to a file folder and discontinuing the use of the file folder. File folders are usually closed off under one of the following circumstances:

- When they become more than 2.5cm (1 inch) thick. In these cases, the usual process is to close off the first volume of the file and then open a second volume with the same file number and title.
- On a certain date, such as the end of the fiscal year.
- When a certain event happens. These events are usually indicated by the code “S/O” in the retention schedules in the Administrative and Operational Records Classification Systems (ARCS and ORCS). S/O is an abbreviation for Superseded/Obsolete, which indicates that something has to happen which either replaces the record or makes it obsolete. ARCS and ORCS include descriptions of the S/O event triggers.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 The opened date of a file is usually, but not always, the date of the first or earliest record in the file. Financial records are sometimes backdated to the beginning of the fiscal year.
- 3.2 The closed date of a file is usually, but not always, the date of the last or most recent record in the file.

In some cases, the closed date may not be the same as the date of the last record in the file. In particular, files with S/O event triggers may have a closed date which differs from the date of the last record on the file.

For example, a new policy was approved in April 2005 and remained in effect until January 2020 when it was replaced by a new policy. The date of the last record on the file is April 2005. However, the policy was in effect for 15 years without having any new records added to the file. In most cases, policy files close when the policy is replaced or cancelled. So, the closed date for our example file is January 2020, the date the policy was replaced instead of the date of the last record on the file. In this example, using the date of the last record as the closed date would result in the disposal of the records many years too soon.

Similarly, financial records are often closed on the last day of the fiscal year, regardless of the actual dates of the documents contained in the file.

- 3.3 If a single file contains several volumes, each volume may have its own open and closed dates. For case files, which are usually files about a specific person, client, employee, or project, the overall closed date for the entire file is usually the closed date of the last volume.
- 3.4 Active files should be reviewed at least once a year to close off the ones which are completed.
- Many, but not all, financial records can be closed automatically at the end of the fiscal year.
    - Contracts, agreements, grants and contributions, signing authorities, and some other categories of financial records, are open for multiple years and have S/O closure criteria. They need to be reviewed to determine if the appropriate event has occurred to close the file.
  - Files for programs that run on a fiscal year basis usually can be closed off automatically at the end of the year.
  - Case files and other files which do not clearly close at the end of the fiscal year should be reviewed by employees who are knowledgeable about the records. The employees should be asked to identify the files whose activity has ceased and confirm the files have met the S/O event trigger criteria.

## 4. Procedures

- 4.1 Create a file listing report from DIIMS, if paper files have been entered into DIIMS. See the [DIIMS Records Classifier Guide](#) for more information on how to create reports.
- 4.2 Review the DIIMS file listing report with co-workers and identify files which can be closed. If DIIMS is not being used to manage active paper records, review any existing file lists, or check each file in the filing equipment.
- 4.3 Write or stamp the closed date on the file label.
- 4.4 Write or stamp the word “Closed” on the outside of the file folder where it can be clearly seen.

- 4.5 Put a “Closed Volume” or “Closed File” sheet on top of the last record in the file. This will alert people to stop adding new material to the file.
- 4.6 Update the closed date for each volume entered in DIIMS or on other file lists.<sup>1</sup> Update the S/O date for files which have an S/O event trigger for their retention schedules. Contact your Department Records Management Team for assistance with batch updating dates on volumes entered in DIIMS.

---

<sup>1</sup> The ability to update the metadata for volumes entered into DIIMS is restricted to employees who have been assigned Records Classifier or Records Coordinator access permissions.

## 7300 Managing Legacy Paper Records (Backlogs)

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Legacy paper records refers to a group of older paper records, often called backlog records, which have not been classified or filed using the Administrative or Operational Records Classification Systems (ARCS or ORCS) and managed through their life cycle in accordance with the retention and disposition schedules in ARCS and ORCS.

Legacy paper records are not unusual. Most government departments have collections of records waiting for someone to take the actions necessary to manage them.

Legacy paper records often suffer from an out-of-sight-and-out-of-mind problem. Government departments would benefit from including an effort to clean up legacy paper records as part of their overall planning for their records management programs. Legacy records are a liability to the government. For example:

- Information required for making decisions may not be available or complete.
- It may be necessary to recreate records which already exist, but which cannot be located because they are hidden in the legacy records.
- Information required in response to a legal matter, an investigation, an audit, or an access to information request may not be discovered.
- The storage locations may not be appropriately secure, leading to the possibility of an information security or privacy breach.
- The storage locations may not be appropriately protected from damage from water, fire, pests, and other hazards.
- The records may be taking up costly office space, storage space, or warehouse space which could be put to better use or which the government might not need to rent if the records were scheduled.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T. 1988, c.A-6

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

Administrative Records Standard, IMT Policy Manual

Operational Records Standard, IMT Policy Manual

### **3. Guidelines**

- 3.1 Legacy paper records are public records and cannot be legally disposed of without the approval of the Territorial Archivist. This approval is obtained by using approved Records Disposition Authorities (RDA), such as ARCS, ORCS, or a One-Time Records Disposition Authority to schedule the retention and disposal of the records.
- 3.2 In most cases, legacy records can and should be classified to the most recent version of an RDA. However, there may be situations where the RDA has been amended since the records were created, and the most recent version no longer has a classification which is appropriate for classifying and scheduling the records. In those cases, it may be possible to use a previous version of the RDA to classify and schedule the records, providing that the open and/or closed dates of the records fall into the same time frame that the earlier version of the RDA was in effect. Contact Enterprise Records Management and the NWT Archives to confirm the applicable date ranges for different versions of RDAs and for additional case-by-case guidance.

### **4. Procedures**

- 4.1 Determine if there is an approved RDA for the legacy records.

The Department Records Management Team may be required to develop a One-Time RDA to schedule and authorize the disposal of records which cannot be classified to the current or previous versions of ARCS or ORCS. A One-Time RDA is a retention schedule which applies to a specific number of files and which is intended support legacy record clean-up projects by scheduling records from government offices and programs which no longer exist. Contact Enterprise Records Management and the NWT Archives for assistance in determining if a One-Time RDA is required.

- 4.2 Create a project plan for the legacy records project. The project team should ideally include the Department Records Management Team, employees who are knowledgeable about the legacy records and who can provide insight into how the records were created and used, and employees to work on processing the records. A member of the Department Records Management Team usually acts as the project manager, while the director or superintendent responsible for the program area is the project owner/sponsor.
- 4.3 The Department Records Management Team trains the project team on how to classify and inventory the records, pack them into records centre boxes, and look for information the Department Records Management Team may need to create a new One-Time Records Disposition Authority, if required.

- 4.4 Inventory the records. It may be necessary to inventory the records using the Excel Box Inventory Form rather than DIIMS. Contact Enterprise Records Management to discuss the use of the Excel Box Inventory Form versus DIIMS with a legacy records project. Guidance will be provided on a case-by-case basis.

If the original file labels use file numbers from an older filing system, record the old number in the volume name or comments fields. It is important to keep track of the old numbers to link the old filing system to the ARCS, ORCS, or One-Time RDA.

- 4.5 Create new labels containing the new file classification number or generate new labels from DIIMS. Relabel all records which are going to be integrated into the department's active filing system and records which are going to be transferred to a GNWT records centre for storage. The new labels will assist with records retrieval.
- 4.6 Organize the scheduled records into transfers and submit the transfers to Enterprise Records Management following the procedures outlined in sections 4100 and 4200 of this handbook.

## **Records and Information Management Related Topics**

## 8100 Government Reorganization

<b>Issued:</b>	July 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

The organization of the GNWT's departments and agencies changes from time to time. These organizational changes have implications for the GNWT's records and information assets as well as its human resources, financial assets, physical assets, and more.

Reorganization of government programs can impact the ownership of government records. Government records are usually owned by the department or agency which has the records in its custody or under its control. Government reorganization changes the custody and control of public records and needs to be addressed through the records management program.

Reorganization impacts not only the departments and agencies involved, but also other government organizations, such as the Technology Services Centre (TSC), Enterprise Information Management, and the NWT Archives. Consideration needs to be given to contractual obligations, legal requirements to retain information such as those outlined in the *Archives Act* as well as other legislation, current or pending litigation, current or pending audits, current access to information requests, and information privacy and confidentiality requirements.

Preparing records for a reorganization, transferring records to another department or agency, and integrating transferred records into the new department or agency takes planning, time, and adequate resources, particularly human resources, in order to ensure needed information is available to program areas and clients during and immediately after the reorganization takes effect.

### 2. References

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

## 8110 Division or Program Renamed

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Changing a division's name is more than just rebranding. It reflects a change in the mandate and goals of the organization, and for records and information management purposes represents a change in custody and control of the information.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, ICT Policy Manual

Records Scheduling Policy, ICT Policy Manual

### 3. Guidelines

3.1 Changes in the ownership of records should be reflected in an amendment to all applicable ORCS as soon as possible. Ideally, ORCS should be amended within a year after the division's name is changed. At the very least, ownership should be updated when the ORCS is reviewed as per the *Records Scheduling Policy* requirement to review ORCS every five years.

3.2 Changes in the ownership of records should be reflected in DIIMS folder structures, as soon as possible after the change has been made.

### 4. Procedures

4.1 To update the name of a division or prefix in DIIMS, the Department Records Management Team should e-mail a change of name request to the DIIMS Service Desk.

4.2 To amend an ORCS to reflect current ownership, the Department Records Management Team should contact Enterprise Records Management and the NWT Archives and initiate an ORCS amendment project.

## 8120 Division or Program Moving to a New Department

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Moving a division or program to a new department or agency requires planning. Moving programs to a new department or agency reflects a change in the mandate and goals of the organization, and for records and information management purposes represents a change in custody and control of the information. There are a number of issues around ownership and storage of records to be resolved when a program moves.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

### 3. Guidelines

3.1 Changes in the ownership of records should be reflected in an amendment to all applicable ORCS as soon as possible. Ideally, ORCS should be amended within a year after the reorganization. At the very least, ownership should be updated when the ORCS is reviewed as per the *Records Scheduling Policy* requirement to review ORCS every five years.

3.2 Changes in the ownership of records should be reflected in DIIMS folder structures, as soon as possible after the change has been made.

### 4. Procedures – Originating Department

4.1 Meet with the program area as soon as possible after the reorganization is known and establish a team to work on the transfer of records. Make sure the team includes representatives of the Departmental Records Management Teams from both the originating and the receiving departments. Other parties, such as the TSC, ISSS, the DIIMS Service Desk, and Enterprise Records Management, should be brought in as necessary to ensure a smooth transfer of records stored in shared drives, e-mail accounts, DIIMS, and the Records Centres.

4.2 Make lists to identify:

- All of the functions and programs which are being transferred to the new department or agency.
- The employees who are moving to the new department or agency.

- The categories of records which will be transferred, such as project files, case files, financial records.
  - It is helpful to identify the current location(s) and custodian of the records, as well as the future location and custodian of the records. The custodian is the person responsible for looking after the records and making sure they are organized properly.
  - Include records in all media and locations, i.e. electronic records on network shared drives, electronic records stored in DIIMS, electronic records stored in collaborating sites, electronic records stored on external hard drives or on local computer hard drives, e-mail records, documents on GNWT websites, analogue and digital audio and video recordings, maps, plans, digital photographs, traditional photographs, photographic negatives, photograph slides, microfilm and microfiche, paper records stored in individual workstations, in shared filing cabinets, in storerooms, and in the GNWT records centres.
  - Identify related active and semi-active records which are held by other divisions and which could create custody and control issues later, such as records held in the directorate, policy, and communications divisions.
- Any information systems and related data.

4.3 Identify any Records Disposition Authorities, file lists and filing procedures associated with the records and provide them to the receiving department or agency. The receiving department or agency will need these in order to effectively use, maintain, access, and dispose of the records.

4.4 Identify the scope of the records to be transferred. In most cases, all records in all locations and all stages of their life cycle will be transferred to the new department or agency. In rare cases, the receiving department or agency may want to receive only the current, open, records. The originating department or agency will have to determine which division will take custody and control of any records which are not transferred to the new organization, and ensure they are classified and disposed of in compliance with the appropriate records disposition authority.

4.5 Identify any ongoing or pending litigation, audits, investigations, or access to information requests and make decisions regarding which department will be responsible for these matters going forward.

4.6 Contact the GNWT Central Warehouse to acquire records storage boxes for any records which are physically moving from one office location to another. The Central Warehouse's inventory fluctuates, so it is best to order the boxes early to make sure there are enough boxes available for the move.

4.7 Develop a work plan to identify the work that needs to be done, who is responsible to carry it out, when the tasks need to be completed, and who is responsible for any associated costs. For example:

	Task	Assigned To	Deadline
1	Organizing network shared drives so that the information can be easily transferred.	Originating Department	
2	Moving electronic records from one department's shared drives to another.	TSC	
3	Moving e-mail accounts and changing network permissions for individual employees.	TSC	
4	Moving electronic records in DIIMS from one department's folders to another.	DIIMS Service Desk	
5	Copying/moving electronic records stored in other locations.	Originating Department	
5	Reassigning ownership of records stored in records centres.	Enterprise Records Management	
6	Copying records from SharePoint and Web Sites for transfer to new department.	Originating Department	
7	Receiving paper files and setting them up in new office space.	Receiving Department	
8	Prepare high level inventories of the records to be transferred and provide the inventories to the receiving department.	Originating Department	
9	Send letter acknowledging transfer of custody and control of the records.	Originating Department Deputy Head	
10	Send letter accepting receipt of custody and control of the records.	Receiving Department Deputy Head	

- 4.8 Save all documentation relating to the project in ARCS v10, 6215-55 Records Management Projects. File lists should be updated and saved in 6215-05 File Lists. Information relating to records stored in the GNWT records centres should be filed in 6215-70 Transfers and Dispositions. Information about Records Disposition Authorities should be filed in 6215-65 Records Disposition Authorities.

## 5. Procedures – Receiving Department

- 5.1 Meet with records management tea, and program area from the originating department or agency in order to gain an understanding of what functions and records are being transferred.
- 5.2 Determine which records are required for use immediately in order to ensure continuity of business programs. Work with the originating department or agency to ensure these records are handled with care and will be available to the program area. Prioritize the other records to be received based on their importance to the program area.
- 5.3 Plan where the records will be housed when they are received. Consider requirements for:
- Physical records stored in workstations and central filing areas.

- Physical records stored in the GNWT records centres.
  - Electronic records stored on network shared drives.
  - Electronic records stored in DIIMS.
  - Electronic records stored in SharePoint or other collaboration sites.
  - Electronic records available on GNWT web sites.
- 5.4 Notify the TSC and DIIMS Service Desk of requirements for storing electronic records.
- 5.5 Notify Enterprise Records Management of requirements for storing paper records in GNWT records centres.
- 5.6 When the records are transferred, verify that all of the records were received.
- 5.7 Follow up with the program area to identify any records which were missed in the original transfer. Work with the originating department to acquire any records which were missed.
- 5.8 Update any files lists and procedures.
- 5.9 In consultation with Enterprise Records Management and the NWT Archives, amend any existing ORCS with the correct custody and control information or develop new ORCS if necessary.
- 5.10 If records are reorganized, reclassified, renamed, or consolidated, create and maintain an index documenting the original order and showing where the information went. Maintaining a record of the chain of custody is essential for routine retrieval purposes, to allow a full response to an access to information request, audit, or legal matter, and eventually may be valuable to the NWT Archives to document the evolution of a government program.

It is advisable to consult with the NWT Archives regarding the handling of records having a final disposition of Archival Selection (AS/D).

- 5.11 Save all documentation relating to the project in ARCS v10, 6215-55 Records Management Projects. File lists should be updated and saved in 6215-05 File Lists. Information relating to records stored in the GNWT records centres should be filed in 6215-70 Transfers and Dispositions. Information about Records Disposition Authorities should be filed in 6215-65 Records Disposition Authorities.

## **6. Procedure – Transferring Programs to Nunavut or an Indigenous Government**

- 6.1 Transfers of active and semi-active records to the Government of Nunavut are governed by and should be done in accordance with the *Nunavut Act (Canada)* and Sections 3 and 4 of the agreement on records between the governments of Nunavut and the Northwest Territories.
- 6.2 Transfers of active and semi-active records to indigenous governments are governed by and should be done in accordance with the relevant legislation and agreements.

- 7. Procedure – Transferring Programs to the Government of Canada, a Provincial Government, the Government of the Yukon, or a non-government body.**
- 7.1 Transfer of custody and control of records to organizations other than Government of Nunavut or an Indigenous Government requires the authorization of the Territorial Archivist, under section 9 of the *Archives Act*, unless the transfer is occurring in compliance with an act of the Parliament of Canada, in which case the federal legislation has priority over the *Archives Act*.

## 8130 Departments Amalgamating or Merging

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Careful planning is required when two or more departments merge and form a new government department to ensure that the records and information required by the new department's programs are available and that there is minimal interruption to public services.

Departmental mergers change the custody and control of records. There are a number of issues around ownership, storage, and disposal of records to be resolved when departments merge.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Records management needs to be considered early in the planning stages of any departmental mergers. Records management project teams with representation from the target departments should be established early to address the transfer of records and information. Other parties, such as the TSC, ISSS, the DIIMS Service Desk, and Enterprise Records Management, should be brought in as necessary to ensure a smooth transfer of records stored in shared drives, e-mail accounts, DIIMS, and the Records Centres. Enterprise Information Management has experience with departmental moves and mergers and can provide examples of project planning documentation.
- 3.2 Changes in the ownership of records should be reflected in an amendment to all applicable ORCS as soon as possible. Ideally, ORCS should be amended within a year after the reorganization. At the very least, ownership should be updated when the ORCS is reviewed as per the *Records Scheduling Policy* requirement to review ORCS every five years.
- 3.3 Changes in the ownership of records should be reflected in DIIMS folder structures, as soon as possible after the change has been made.

## 4. Procedures

- 4.1 Establish a team to work on the transfer of records. Make sure the team includes representatives from the Department Records Management Teams from both departments. Other parties, such as the TSC, the DIIMS Service Desk, and Enterprise Records Management, should be brought in to ensure a smooth transfer of records stored in shared drives, e-mail accounts, DIIMS, and the Records Centres.
- 4.2 If possible, obtain a summary of the Record of Decision or other documents that authorize the creation of the new department and save this with the project documentation as evidence of the change of ownership of the records.
- 4.3 Develop a project plan and implement using project management methodology. Enterprise Information Management can provide examples of project plans and lessons learned from previous departmental mergers.
- 4.4 Develop a detailed task list, assigning responsibilities for the following areas:
  - Project planning and oversight.
  - Project employee records management training.
  - Project communications and reporting.
  - Review current state of records management programs in each department, including:
    - Current, draft, and obsolete Records Disposition Authorities.
    - Procedures and guidelines.
    - Filing practices and methodologies.
    - DIIMS usage.
    - Network file server usage.
    - Extent of ARCS and ORCS implementation with electronic and paper files.
    - Use of GNWT records centres and other records storage locations, such as storerooms and warehouses.
    - IS systems.
  - Space changes and office moves.
  - Inventory or data map of all records in all media.
    - This is a key document which will identify where information is currently located and who is responsible for it. It will be used to determine where the information will reside and who will be responsible for it in the new department.
    - Include records in all media and locations, i.e. electronic records on network shared drives, electronic records stored in DIIMS, electronic records stored in collaborating sites like SharePoint, electronic records stored on external hard

drives or on local computer hard drives, e-mail records, documents on GNWT websites, analogue and digital audio and video recordings, maps, plans, digital photographs, traditional photographs, photographic negatives, photograph slides, microfilm and microfiche, paper records stored in individual workstations, in shared filing cabinets, in storerooms, and in the GNWT records centres.

- Identification of program essential records which must be available both immediately before and immediately after the merger.
- Design of the new folder structure and permissions in DIIMS.
- Design of new folder structures for network shared drives.
- Pre-merger shared drive clean-up.
- Pre-merger transfer of semi-active records to the records centres.
- Pre-merger disposal of physical records and electronic records stored in DIIMS.
- Data migration.
- Identify and carry-out business process re-alignments, including changes to filing systems and procedures, locations for storing forms and templates, changes to existing DIIMS workflows.
- ORCS development or revision for new department.
- ARCS/ORCS implementation for new department.
- Records management and DIIMS training for all employees.
- Ongoing or pending litigation, audits, investigations, or access to information requests.

4.5 If records are reorganized, reclassified, renamed, or consolidated, create and maintain an index documenting the original order and showing where the information went. Maintaining a record of the chain of custody is essential for routine retrieval purposes, to allow a full response to an access to information request, audit, or legal matter, and eventually may be valuable to the NWT Archives to document the evolution of a government program.

It is advisable to consult with the NWT Archives regarding the handling of records having a final disposition of Archival Selection (AS/D).

- 4.6 Save all documentation relating to the project in ARCS v10, 6215-55 Records Management Projects. File lists should be updated and saved in 6215-05 File Lists. Information relating to records stored in the GNWT records centres should be filed in 6215-70 Transfers and Dispositions. Information about Records Disposition Authorities should be filed in 6215-65 Records Disposition Authorities.

## 8140 Departments Disbanded

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

Careful planning is required when a single government department is disbanded to form two or more new government departments. Planning is required to ensure that the records and information required by each program is available and that there is minimal interruption to public services.

Breaking up a department changes the custody and control of the records previously owned by the department. There are a number of issues around ownership, storage, and disposal of records to be resolved when departments disband.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

Records Scheduling Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Records management needs to be considered early in the planning stages of any departmental reorganization. Records management project teams with representation from the new departments should be established early to address the transfer of records and information. Other parties, such as the TSC, ISSS, the DIIMS Service Desk, and Enterprise Records Management, should be brought to ensure a smooth transfer of records stored in shared drives, e-mail accounts, DIIMS, and the Records Centres.
- 3.2 Special consideration needs to be given to records from the directorate, policy, communications, finance and administration divisions, and regional offices. These divisions often have records which combine records relating to each of the new departments. Ideally, the records relating to each of the new departments would be split up and provided to the new departments, but this is not always possible. Careful planning will be required regarding the future ownership of these records so as not to create long term problems with access to and classification, retention, and disposition of these records. It is best to try to avoid situations where multiple departments have to approve the disposal of records.
- 3.3 Changes in the ownership of records should be reflected in an amendment to all applicable ORCS as soon as possible. Ideally, ORCS should be amended within a year after the

reorganization. At the very least, ownership should be updated when the ORCS is reviewed as per the *Records Scheduling Policy* requirement to review ORCS every five years.

- 3.4 Changes in the ownership of records should be reflected in DIIMS folder structures, as soon as possible after the change has been made. It may be possible to move records to the custody of the new departments in advance.

#### 4. Procedures

- 4.1 Establish a team to work on the transfer of records. Make sure the team includes representatives from the Department Records Management Team and representatives from each of the new departments. Other parties, such as the TSC, the DIIMS Service Desk, and Enterprise Records Management, should be brought to ensure a smooth transfer of records stored in shared drives, e-mail accounts, DIIMS, and the Records Centres.
- 4.2 If possible, obtain a summary of the Record of Decision or other documentation that authorizes the creation of the new departments and save this with the project documentation as evidence of the change of ownership of the records.
- 4.3 Develop a project plan and implement using project management methodology.
- 4.4 Develop a detailed task list, assigning responsibilities for the following areas:
- Project planning and oversight.
  - Project employee records management training.
  - Project communications and reporting.
  - Review current state of the records management program, including:
    - Current, draft, and obsolete Records Disposition Authorities.
    - Procedures and guidelines.
    - Filing practices and methodologies.
    - DIIMS usage.
    - Network file server usage.
    - Extent of ARCS and ORCS implementation with electronic and paper files.
    - Use of GNWT records centres and other records storage locations, such as storerooms and warehouses.
    - IS systems.
  - Space changes and office moves.
  - Inventory or data map of all records in all media.
    - This is a key document which will identify where information is currently located and who is responsible for it. It will be used to determine where the

information will reside and who will be responsible for it in the new departments.

- Include records in all media and locations, i.e. electronic records on network shared drives, electronic records stored in DIIMS, electronic records stored in collaborating sites like SharePoint, electronic records stored on external hard drives or on local computer hard drives, e-mail records, documents on GNWT websites, analogue and digital audio and video recordings, maps, plans, digital photographs, traditional photographs, photographic negatives, photograph slides, microfilm and microfiche, paper records stored in individual workstations, in shared filing cabinets, in storerooms, and in the GNWT records centres.
- Identification of program essential records which must be available both immediately before and immediately after the new departments come into existence.
- Design of the new folder structure and permissions in DIIMS.
- Design of new folder structures for network shared drives.
- Shared drive clean-up.
- Transfer of semi-active records to the records centres.
- Disposal of physical records and electronic records stored in DIIMS.
- Data migration.
- Identify and carry-out business process re-alignments, including changes to filing systems and procedures, locations for storing forms and templates, changes to existing DIIMS workflows.
- ORCS development or revision for new departments.
- ARCS/ORCS implementation for new departments.
- Records management and DIIMS training for all employees.
- Ongoing or pending litigation, audits, investigations, or access to information requests.

4.5 If records are reorganized, reclassified, renamed, or consolidated, create and maintain an index documenting the original order and showing where the information went. Maintaining a record of the chain of custody is essential for routine retrieval purposes, to allow a full response to an access to information request, audit, or legal matter, and

eventually may be valuable to the NWT Archives to document the evolution of a government program.

It is advisable to consult with the NWT Archives regarding the handling of records having a final disposition of Archival Selection (AS/D).

- 4.6 Save all documentation relating to the project in ARCS v10, 6215-55 Records Management Projects. File lists should be updated and saved in 6215-05 File Lists. Information relating to records stored in the GNWT records centres should be filed in 6215-70 Transfers and Dispositions. Information about Records Disposition Authorities should be filed in 6215-65 Records Disposition Authorities.

## 8200 Ministers Records

<b>Issued:</b>	January 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

The Office of the Cabinet Secretariat issues guidelines for the handling of records by ministers' offices. These guidelines address the ownership of records held by a minister's office and the handling of the records when a minister leaves office.

The purpose of these guidelines is to provide additional guidance to departments who receive records from their minister's office.

### 2. References

Ministers' Offices Records Guidelines

### 3. Guidelines

- 3.1 Paper and electronic files received by a department or agency from the ministers' office should be kept as a complete set. They should be clearly separated from the records held by the directorate or policy divisions. Although this may result in duplication of records it is best to keep, classify, schedule, and dispose of both the departmental copy and the minister's copy as separate, master records, because each set of records may contain documentation that is missing from the other.

### 4. Procedures

- 4.1 On receiving records from a minister's office, classify them using the Administrative Records Classification System (ARCS).<sup>1</sup> The most likely classifications to be used, from ARCS v10, include:

- 1275-20 Ministerial Chronos
- 1275-25 Briefings
- 1275-37 Issues files
- 1275-40 Speeches and Statements
- 1290-20 Cabinet Submissions
- 1290-30 Cabinet Committees
- 1290-35 Decision Papers and Options Papers
- 1310-35 Standing Committees

---

<sup>1</sup> The Cabinet Secretariat and Financial Management Board Secretariat should file Executive Council or Financial Management Board records received from ministers' offices in the appropriate Operational Records Classification Systems (ORCS).

- 1310-70 Oral and Written Questions
- 1310-75 Session Preparation
- 4325-20 Financial Management Board Submissions

4.2 In DIIMS, create a sub-folder (tertiary level folder) under the appropriate secondary for the Minister's records. It is recommended to title the folder using the date range of the minister's time in office and the minister's name. Use this folder to save electronic records and to create volumes to manage paper records.

4.3 Contact the DIIMS Service Desk for assistance with copying electronic records received on a CD, DVD, or external hard drive or flash drive into the appropriate folders DIIMS. Verify that all records were copied into DIIMS.

Once you have confirmed that the records in DIIMS are complete, destroy the CD, DVD, or external hard drive or flash drive which contained the records. External hard drives and flash drives can also be wiped. Contact the TSC for information on how to securely wipe an external hard drive or flash drive so that the information that was stored on it cannot be recovered.

4.4 Paper records can be inventoried using DIIMS. Volumes can be entered into the appropriate sub folder (tertiary level folder). The name of the minister should be included in the volume name or description fields.

## 8300 Managing Government Records When Working Remotely

<b>Issued:</b>	April 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

From time to time it is necessary for employees to work remotely from the office, such as in the field or at a work site, while on duty travel, or occasionally from home. The purpose of this guidance is to support decision making by management and employees to ensure the safeguarding of personal information and/or confidential government records regardless of the medium used to produce the records (i.e. electronic and paper-based),

This guidance is not intended to replace department specific instructions for employees currently working remotely on a routine basis, where established procedures or protocols have been created. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T 1988, c.A-6.

Access to Information and Protection of Privacy Act, S.N.W.T 1994, c.20

Health Information Act, S.N.W.T 2014, c.2

[GNWT Code of Conduct](#)

[GNWT Protection of Privacy Policy](#)

Email Use Policy, IMT Policy

Recorded Information Management Policy, IMT Policy Manual

Electronic Information Security Policy, IMT Policy Manual

Electronic Information Security Standard, IMT Policy Manual

Threat-Risk Analysis Guideline, IMT Policy Manual

[Message from the Northwest Territories Information and Privacy Commissioner on Protecting Privacy while Working from Home](#)

RDA 1997-02, Transitory Records Schedule

### 3. Guidelines

Precautions should be taken to ensure that government information remains secure and confidential while working remotely. Even while working remotely, GNWT employees are bound by the government's Code of Conduct and Oath of Office and Secrecy, information security policies, the *Archives Act*, the *Access to Information and Protection of Privacy Act (ATIPPA)*, and the *Health Information Act (HIA)*.

- 3.1 Employees should understand the sensitivity of the government records and information they create and use.
- 3.2 Only government approved electronic devices should be used for conducting government business (this applies to both government-issued devices and personal devices). The devices should be appropriately protected and updated (i.e. privacy screen filter, encrypted government issues laptops, USB flash sticks, home computers and mobile phones, etc.).
  - Electronic devices should not be left unattended in a public place.
  - Electronic devices should be locked when not in use.
  - Electronic devices should not be shared with others. (If using a shared personal computer, ensure all windows have been closed and all programs shut down before allowing someone else to use the computer.)
  - Electronic devices should be positioned so others cannot see the screen.
- 3.3 Paper records that contain personal and confidential information should not be removed from government offices (i.e. client files, paper documents, etc.). Removing records from government offices without authorization may be a violation of the *Archives Act*.
- 3.4 If it is deemed essential for operations, the removal of paper records must be discussed with and approved (signed off) by the supervisor. The employee must ensure they are the only person who will be able to access or view the confidential or personal information.
- 3.5 Protected protocols for transporting confidential and/or personal paper records from government offices must ensure:
  - The least amount of information is removed as possible.
  - Their removal is documented (i.e., create an email or worksheet describing and listing specific files, date range of material, etc.). Provide a copy to your supervisor.
  - They are secured in a container, such as a records centre box or a briefcase, for transport and are marked confidential.
  - Transfer is point-to-point with no stops in between.

- Steps are taken to prevent the unauthorized access, use, disclosure, loss, destruction, or theft of the information.
  - Records are returned to the government offices secure storage location as soon as no longer required for work purposes and any copies are securely destroyed (i.e. shredded).
- 3.6 All government records should be appropriately safeguarded when in use and not in use (i.e. records should not be left unattended on worktables and in public places where others can view, keep in locked drawer of filing cabinet or desk drawer to which the employee has sole access, computers password protected, etc.)
- 3.7 Storage of electronic records must be in a secure government repository (i.e. DIIMS) or a network space designated as the government office's recordkeeping system so access is available to co-workers authorized to have access, and the records are backed up (i.e. do not save records in locations that are only available to one person, such as the desktop or email account).
- 3.8 Personal e-mail accounts should not be used as a means to conduct government business and to transfer records containing personal information for work purposes.
- 3.9 Employees should avoid saving documents onto portable electronic devices, such as a laptop or tablet hard drive, smartphone, or a portable hard drive.
- As soon as possible after an employee has finished creating or using a document on a portable device, they should connect to DIIMS or the GNWT network shared drives and upload the document to the appropriate location in DIIMS or on the network. This may require a VPN connection to be successful.
  - Verify that the upload was a success and then permanently remove (delete) the local copy (transitory copy) ensuring it has been deleted from the device's recycle/trash bin.
- 3.10 Transitory records may be deleted as per the [\*Transitory Records Schedule\*](#).
- Transitory records relating to pending or current litigation, legal actions, investigations, audits, or ATIPP requests should not be disposed of while that activity is underway or anticipated.
  - Transitory records must be protected and securely disposed of to maintain security, confidentiality, protect personal privacy, and prevent information security breaches. See section *4420 Disposal of Transitory Records in Paper and Other Media* for more information.

- Transitory paper records should be secured and returned to the government office as soon as no longer required to conduct business and placed in the approved secure document destruction bin or shredded using the office's cross-cut shredder
- 3.11 Employees should remember that a public record is a public record and belongs to the GNWT, regardless of where it is created or what format it is in. A record is a public record if it contains information that was created and used in order to carry out government business.
- 3.12 Even if employees are using non-standard procedures and equipment to carry out government business, appropriate information must still be captured, and appropriate records created and maintained.
- Employees should make sure that information about government decision-making is captured and saved as records. Employees should ask themselves:
    - Could someone else who is not familiar with the situation understand what happened?
    - Are the records I create and maintain available to others who may have a need to use them, especially if I am unavailable?
    - Am I creating and maintaining records which are complete, accurate, reliable, and trustworthy?
  - If instant messaging systems or text messages are being used to communicate with colleagues, supervisors, or clients and contacts, any information concerning government business and decision making should be transcribed and saved into DIIMS or a GNWT network shared drive.
  - Consider making e-mail the method of choice for communicating government business between colleagues, supervisors, and clients and contacts. E-mail messages can be uploaded to DIIMS or exported from Outlook and saved as a record on GNWT network shared drives.
- 3.13 Make sure you understand the GNWT's protocols for reporting information and privacy breaches.

## Records and Information Management Working Remotely Checklist

	Yes	No	N/A
<b>General</b>			
Have you been authorized to work remotely or from home?			
Do you have an authorized GNWT computer/laptop or other devices to work with when working remotely? If using personal computing equipment, has your supervisor authorized you to use it?			
Are you able to secure your GNWT computer/laptop or other devices when they are not in use?			
Do you have external access to DIIMS or VPN access to the GNWT's network?			
Can you protect your work from unauthorized access, use, disclosure, loss, destruction, or theft of the information, including by members of your household?			
Do you understand your responsibilities under the <i>Archives Act</i> , the <i>Access to Information and Protection of Privacy Act</i> , and, if applicable, the <i>Health Information Act</i> ?			
Do you understand how to report an information or privacy breach?			
<b>Electronic Records</b>			
Do you understand that personal email accounts should not be used to conduct government business?			
Do you understand that government records should be created and stored on the hard drives of computers and laptops and other devices only while they are being worked on, and should be saved and copied back to DIIMS or the GNWT network shared drives as soon as you have finished working on them, in order to ensure the records are available to your colleagues and that they are backed up?			

	Yes	No	N/A
Do you understand how to delete local copies of government records stored on computers, laptops and other devices after they have been saved into DIIMS or the GNWT network shared drives?			
Do you understand which folders you should use to save electronic documents in DIIMS or the GNWT network shared drives?			
Do you understand how to transcribe government business conducted by text messaging or instant messaging and save it into DIIMS or on the GNWT network shared drives?			
If you print copy records at home for ease of use, do you have a plan for returning the paper records to the office for secure destruction as soon as no longer required?			
<b>Paper Records</b>			
Do you have your supervisor's permission to remove paper records from the office?			
Have you identified the smallest number of records you need to deliver your program or service?			
Do you understand the importance of protecting the privacy and confidentiality of paper records?			
Are you able to securely transport the records from the office to your home?			
Are you able to securely store the records at home and prevent unauthorized access, use, disclosure, loss, destruction, or theft of the information, including by members of you household?			
Have you made a list of the records you are removing from the office and have you shared that list with your supervisor?			
Do you have a plan for the return of the paper records/physical files to the office as soon as no longer required?			

## 8310 Using Online Chat and Collaboration Tools

<b>Issued:</b>	April 2020
<b>Last Updated:</b>	July 2021

### 1. Introduction

The purpose of this guidance is to support decision making by management and employees when using collaboration, text, chat, meeting and conferencing, and instant messaging tools (e.g. Telemerge, GoToMeeting, WebEx, Zoom, Microsoft Teams, Slack, etc.).

This guidance is not intended to replace department specific instructions for employees working remotely on a routine basis or where established procedures or protocols have been created. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T 1988, c.A-6.

Access to Information and Protection of Privacy Act, S.N.W.T 1994, c.20

Health Information Act, S.N.W.T 2014, c.2

[GNWT Code of Conduct](#)

[GNWT Protection of Privacy Policy](#)

Email Use Policy, IMT Policy Manual

Recorded Information Management Policy, IMT Policy Manual

Electronic Information Security Policy, IMT Policy Manual

Electronic Information Security Standard, IMT Policy Manual

Threat-Risk Analysis Guideline, IMT Policy Manual

[Message from the Northwest Territories Information and Privacy Commissioner on Protecting Privacy while Working from Home](#)

RDA 1997-02, Transitory Records Schedule

### 3. Guidelines

3.1 Use of collaboration, text, chat, meeting and conferencing, and instant messaging tools should be approved by the program director. The collaboration tool should be one of the approved tools which meet the government's security requirements. Contact the IS Service Desk for assistance in selecting an approved collaboration tool.

3.2 Before making decisions for using collaboration, text, chat, meeting and conferencing, and instant messaging tools, set expectations for how the tools will be used. Clearly explain when it is appropriate to use the collaboration tool (e.g. staff meetings, coordinating tasks, etc.) and when it is inappropriate to use the collaboration tool (e.g. supervisor-employee discussions, discussions relating to a specific client, sharing of personal information, etc.). Monitor the use of the tool and ensure employees comply with the expectations.

Create written instructions or procedures concerning the appropriate use of collaboration, text, chat, meeting and conferencing, and instant messaging tools by employees. Written instructions or procedures for each government program are recommended to support the use of these tools should questions arise concerning their use.

Assume that the information shared on collaboration tools could become public. Never use these platforms to share sensitive information which would make our information systems and networks vulnerable to attack or which would impact the privacy of others, such as:

- Personally identifiable information, including name, address, date of birth, social security number, gender, race, grades, and other personal information, as well as financial information such as salary, banking information, and payroll deductions.
- Login Credentials/Passwords
- Secure or confidential information. This information is better communicated with a phone call or by GNWT e-mail.

3.3 Remember that everything shared on collaboration, text, chat, meeting and conferencing, and instant messaging tools is subject to discovery for access to information requests, audits, investigations, and legal matters. It is best to use courteous, professional, and inclusive language when using these tools.

3.4 Government employees have a responsibility to the public and the Legislative Assembly to keep records documenting their activities. Good and thorough recordkeeping by government bodies is a cornerstone of public accountability and Canadian democracy. Information about government actions, transactions, and decisions should be documented.

Government employees should be documenting the following activities and saving them into their office's record keeping system in DIIMS or on network shared drives:

- Online meetings should be documented in minutes or notes.

- Discussions, advice, and decisions relating to government business should be copied from text, chat, and instant messaging services. It may be possible to export data from the chat or messaging system and save it as a record. If the system does not have that capability, the discussions, advice, and decisions should be transcribed and saved.
- Changes to government programs and services should be documented.
- Information should be kept documenting legal or financial rights or obligations for the government, members of the public, businesses, and other organizations.
- Decisions relating to development or interpretation of legislation, policy, programs, human resources, budget and financial decisions, and procurement must be documented.

Documentation should clearly show who was included in the discussions and who was responsible for making decisions.

Monitor the use of collaboration, text, chat, meeting and conferencing, and instant messaging tools to ensure appropriate documentation is being kept in the office's recordkeeping system.

3.5 Most, but not all messages transmitted on text, chat, and instant messaging services will be transitory. Transitory records are records needed for only a short period of time to complete a routine action or prepare a final document. Transitory records may be deleted as per the [Transitory Records Schedule](#).

- Information stored in text, chat, and information management systems is discoverable and there may be a requirement to produce it. Transitory records relating to pending or current litigation, legal actions, investigations, audits, or access to information requests should not be disposed of while that activity is underway or anticipated. Do not abuse the edit function to effectively delete a message by replacing it with new information.
- Text, chat, and instant messaging tools should be set to auto-delete transitory messages unless the information is responsive to current litigation, legal actions, investigations, audits, or access to information request. Transitory messages should be kept for no longer than 365 days, but may be set to a shorter period of time. Auto-delete settings should be documented in the written instructions or procedures for using the tools.

3.6 The use of collaboration, text, chat, meeting and conferencing, and instant messaging tools should be included in employee onboarding and offboarding procedures. New employees should be added to the platform and provided with training on the appropriate use of the collaboration tool. When an employee terminates or moves to another position in the government their access to the collaboration tool should be removed.

## 8311 Considerations for Online Meetings

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Video conferencing allows GNWT employees to meet with each other and with individuals outside the GNWT from a distance. Just like face-to-face meetings, records should be kept documenting the discussions of an online meeting.

The purpose of this guidance is to support decision making by management and employees when holding online meetings using MS Teams or other video conferencing tools.

This guidance is not intended to replace department specific instructions for employees currently working remotely on a routine basis, where established procedures or protocols have been created. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Archives Act, R.S.N.W.T 1988, c.A-6.

Access to Information and Protection of Privacy Act, S.N.W.T 1994, c.20

Health Information Act, S.N.W.T 2014, c.2

GNWT Code of Conduct

GNWT Protection of Privacy Policy

Recorded Information Management Policy, IMT Policy 6003.00.18

Privacy Impact Assessment – Preliminary Privacy Screening Tool

Privacy Impact Assessment – Module 1 – Preliminary Risk Assessment

Privacy Impact Assessment – Module 2 – Privacy Analysis

GNWT Administrative Records Classification System, Version 10 (2018)

### 3. Guidelines – Creating and Saving Meeting Records

- 3.1 Employees are responsible for creating and keeping records which document their work. For online meetings, departments and agencies should keep the same kinds of records that would be created and kept for an in-person meeting.

- 3.2 The onus for keeping records is on the organizer of a meeting. The organizer of a meeting should usually keep or delegate someone to keep the following:
- Agendas
  - Written minutes, notes, or records of decision, and
  - Copies of presentation slide decks and other documents distributed or shared at the meeting.
- 3.3 Employees are responsible for making sure records of meetings are saved into the department or agency's recordkeeping system. This may mean saving documents into the appropriate folder in DIIMS, on a network shared drive, or paper filing system.
- 3.4 Video conferencing and online collaboration tools are not recordkeeping systems and must not be used as the sole repository for GNWT meeting records.

#### 4. Guidelines - Classification and Retention for Meeting Records

- 4.1 In most cases, records relating to meetings can be classified and organized using the GNWT Administrative Records Classification System (ARCS). ARCS version 10 contains two primary-level classifications for meeting records:
- Primary 1015 is used for meetings in which *all* participants work for the same department or agency, such as staff meetings or senior management team meetings. These records are kept for 7-10 years and some will be transferred to the NWT Archives for permanent preservation.
  - Primary 1145 is used for meetings in which *some* of the participants work for other GNWT departments or agencies, other governments, or other external organizations. These records are kept for 12 years and some will be transferred to the NWT Archives for permanent preservation.

Contact the Department Records Management Team for assistance in determining the appropriate place to save records of online meetings.

#### 5. Guidelines – Recording Online Meetings

Video conferencing tools may have the ability to record online meetings. There are several issues with recording meetings which should be taken into consideration by meeting organizers before deciding to make a recording.

- 5.1 In general, there should be no need to record an online meeting which would not be recorded if it were held face to face or over the phone. Meetings should only be recorded if there is a compelling reason to do so.

There are situations where recording an online meeting may be beneficial to the GNWT, such as testimony at a hearing or inquiry, interviews conducted for a legal matter, and training sessions and presentations which can be used later or which cannot be captured in another way.

- 5.2 Recording a meeting does not replace the requirement to keep written records of the meeting.
- 5.3 Recordings of online meetings are records and must be exported or downloaded from the video conferencing tool and saved in the department or agency's recordkeeping system.
- 5.4 Recordings of online meetings can be large. For example, the size of a recording of a one-hour meeting can range from 200 MB to over one GB in size, depending on the video conferencing system being used and the recording settings. Downloading recordings from the video conferencing tool and then uploading them to DIIMS or the GNWT network may cause bandwidth issues for recordings over 250 MB. The size of the recordings will impact network storage capacity. It will also impact personal data usage if this is being done while working from home.

DIIMS can accommodate records under 2 GB (2000 MB) in size. Contact the TSC for information about maximum size for records stored on network shared drives. Avoid storing records on computer hard drives (C: drive) or external storage devices.

- 5.5 Recordings of online meetings are usually saved in an MP4 format or a format specific to the video conferencing service. These formats may not be appropriate for long term (more than 10 years) or archival preservation. It may be necessary to convert the recordings to a preservation format before saving them into DIIMS or the network shared drive. Converting the videos to a different format may impact file size.

Contact the NWT Archives for guidance with respect to preservation quality video recording formats.

- 5.6 Recordings of online meetings may capture personal information which would not be captured in other types of meeting records. Recordings may capture the images and voices of the participants, information about their locations, and any information or opinions they share during the meeting. Recordings may also capture personal information of non-participants in the background, such as images of or information about family members. It may not be appropriate for this information to be kept as a government record.

Government departments and agencies should consult with their departmental access and privacy coordinator or the Department of Justice's Access and Privacy Office before recording meetings. It may be necessary to conduct a privacy impact assessment to determine if it is appropriate to record meetings.

- 5.7 To comply with territorial, national, and international laws, meeting participants, both internal and external to the GNWT, should be informed in advance of the meeting that it will be recorded. Review the text of the recording disclaimer with the departmental access and privacy coordinator or with the Department of Justice's Access and Privacy Office.

The following is an example of a recording disclaimer. Text in blue brackets should be replaced with the department's information.

*This meeting will be recorded.*

*Your personal information, including (as applicable) your image, voice, name, opinions, and any other personal information disclosed by you during the online meeting, will be collected in accordance with section 40(c) of the Access to Information and Protection of Privacy Act and/or section 29 of the Health Information Act by the [insert name of department or agency] for the purpose of documenting your participation in the meeting. If you have any questions about the collection of your personal information, please contact: [title, business address and business telephone number].*

*The recording of this meeting may be disclosed in the future in response to an access to information request, audit, investigation, or other legal matter.*

*If you do not wish your personal information to be collected, please do not join the meeting.*

Meeting participants have the option to turn off their cameras so that their image will not be captured in the video, which will reduce the intrusion on their privacy.

- 5.8 Departments and agencies may be required to release recordings of online meetings in response to an access to information request, legal matter, audit, or investigation.

Before releasing the recordings, it may be necessary to redact them to prevent the disclosure of information which is protected under the *Access to Information and Protection of Privacy Act* or the *Health Information Act*. Recordings can be difficult and time consuming to redact, and this may impact the government's ability to respond to a request in compliance with legislated timeframes. Redacting recordings also typically requires the purchase of specialized software.

## 8400 Naming Conventions and Titling Files

<b>Issued:</b>	July 2021
<b>Last Updated:</b>	July 2021

### 1. Introduction

Naming conventions are rules for how electronic folders, electronic records, and paper records will be named or titled. The GNWT does not have a standard for naming conventions. Instead, departments can establish their own naming conventions.

Naming conventions are important components in the development of electronic and paper recordkeeping systems. They introduce consistency in the naming of titling of records, which makes for better and faster searching and retrieval of information.

This guidance is not intended to replace existing departmental filing rules and procedures. Instead, it may be used to confirm that current practices are consistent with the recommendations of the Enterprise Information Management Division.

### 2. References

Infrastructure Establishment Policy, Executive Council Policy 31.00

Recorded Information Management Policy, IMT Policy Manual

### 3. Guidelines

- 3.1 Naming conventions should be set up in consultation with the employees who create and use the records. Different program areas may have different naming requirements. Naming conventions should be documented in the departmental records and information management procedures manual.
- 3.2 Determine the naming elements which need to be included in the name or title of a record. The order in which the elements appear should be identified in the naming conventions. Some common elements include:
  - **Title** – this element should be short but meaningful and clearly describe the content or subject matter of the record.
    - If using personal names, the last name usually comes first followed by the first initial or first name.
    - Abbreviations should generally be avoided because the meaning of the abbreviation may be lost over time. If names of organizations or programs are abbreviated, a list of standard abbreviations should be created.

- **Case, project, or client ID numbers** – this element is usually a unique, system generated identifier which uniquely identifies the case, project, or client.
- **Version number** – use two-digit version numbers to keep electronic records in numerical order. This element is not necessary for electronic records stored in DIIMS because DIIMS manages versions.
- **Volume number** - this element applies to paper file folders and helps distinguish different volumes of a file.
- **Record type** – this element helps distinguish different records which might otherwise have the same title, such as an agenda and minutes for a meeting. Other examples of record type include letter, memo, briefing note, plan, report, etc.
- **Date** – this is a date which is relevant to the record, such as the date of a meeting, or the fiscal year to which the record relates. It is not necessarily the date on which the record was written or saved.
  - To improve sorting use numbers to represent months rather than the names of months.
  - The GNWT standard date format is yyyy-mm-dd (e.g. 2020-04-24).
  - When referring to a fiscal year, use a standard method to identify the fiscal year, such as 2020-2021 or 2020-21. Using different methods to write out the fiscal year affects searching and sorting of electronic records. Use a hyphen to separate the date elements.
- **Author or creator** – this information may be useful to identify who worked on a record or a version of a record. Like names, the format is usually the last name followed by the first initial or first name.

3.3 Avoid using symbols and punctuation, except for apostrophes, hyphens (dashes), underscores, and commas, as they may be difficult for computers to process. Hyphens and underscores can be used to separate words or elements of the name. Spaces between words in a file name can also cause problems if an electronic record is posted to the internet.

3.4 Be aware of the length of the name. Very long folder and file names can create problems when saving and retrieving computer files, particularly on the network shared drives. For paper files, very long file names may not fit on the file labels.

## **Appendices**

## Appendix A Records Centre Label Placement

<p><b>Sòmbak'è</b> (Yellowknife)</p>	 <p>Storage Label</p>	
<p><b>Tthebacha and Xát'odehchee</b> (Fort Smith and Hay River)</p>	 <p>Disposition Label</p> <p>Storage Label</p>	

**Łııdlı Kúę and  
Inuvik (Fort  
Simpson and  
Inuvik)**

Disposition Label



Storage Label



**Map Tubes**

Storage Label



Document Label



## Appendix B Examples of Vital or Essential Records

The following is a list of records that may be considered as vital records.<sup>1</sup> This list is not comprehensive. On reviewing their functions, government bodies may decide that some of the records listed below are not vital and that some records not listed are.

In most cases, it is the most current, up to date information which is considered vital or essential.

### Emergency response plans

- Hospital disaster plans
- Rescue resources and plans

### Lists of key personnel and delegations of authority

- Lines of succession
- Staff designated to perform during emergencies
- Staff with specialized training
- Signing authorities

### Lists, composite drawings, and/or master drawings, maps, and charts

Showing location and essential information on emergency facilities

- Hospitals and health centres
- Oil wells and natural gas reserves, oil and natural gas pipeline cut-off valves
- Gas plants and their capacities
- Shelter accommodations
- Food and clothing stockpiles
- Welfare centres and institutions
- Power supplies including facilities and transmission lines
- Water supplies, treatment plants, main aqueducts, pumping stations, deep wells
- Communications systems, including telephone and radio networks
- Major bridge infrastructures
- Highway profiles, highway crossings of oil and gas pipeline, gravel pits
- Data on public transportation resources

### Lists of key equipment and supplies, including operating instructions

- Medical equipment and supplies
- Fire apparatus
- Communications equipment
- Rescue equipment
- Heavy machinery
- Highway maintenance
- Construction equipment
- Emergency welfare manuals on feeding, clothing, and providing shelter to people displaced by an emergency

---

<sup>1</sup> This list was derived in part from [The Preservation of Essential Records: a guide for governments, organizations, institutions, and businesses](#), Emergency Preparedness Canada, 1996.

- Locations and quantities of stocks of materials required to restore basic services to the public
- Supplier listings

### **Records vital to public order, safety, and public health**

- Police
- Fire
- Medical resources

### **Information relating to the establishment of the organization**

- Acts and regulations
- Orders-in-council
- Executive Council minutes
- FMB minutes
- Records of Decision
- Organization charts
- Procedures manuals
- NWT Gazette
- Current annual reports and business plans
- Policy decisions
- Forms (one copy of each form)

### **Court documents and legal records**

- Wills that have not been probated
- Adoption records
- Administration of estates
- Appointment registers for justices-of-the-peace, notaries, and public officers
- Legal change of name records
- Intergovernmental agreements
- MOUs with other organizations and governments
- Licenses and permits
- Legal documents, such as contracts, agreements, land files, leases

### **Education**

- Debenture agreements for school construction
- Student records (high school)
- College student and graduate records
- Professional and trade examination records
- Teachers record of service

### **Financial records**

- Estimates
- Records of loans
- Records of special funds
- Sales records and guarantees
- Listings of bonds, debentures, insurance records, securities, investment records
- Bank deposit records and previous month's monthly statement
- Appropriations
- Revenues

- Financial records of boards and agencies
- Public accounts for the last two years
- General ledgers and journals
- Accounts payable and receivable

### Land titles documents

- Maps of municipal boundaries, tax rolls, lease account rolls, legal description of all communities
- Legal survey plans, town site plans
- Mineral claims, water resource rights
- Public land registers
- Records about the purchase of and payment for public land
- Listings and surveys of lands, forests, agriculture, mines

### Personnel and human resources records

- Union agreements
- Personnel files, pay files, pension records, attendance records

### Health and welfare records

- Records concerning recipients of assistance programs
- Records concerning wards of the government
- Data on notifiable diseases
- Data on health hazards and prevention measures

### Other records

- Vital statistics records (births, marriages, deaths, adoptions, change of name)
- Computer programs
- Production formulae
- Specifications on specialized projects
- Lists of regional, area, and community offices and facilities available
- Lists of vital records and their storage locations
- Lists of records available at regional, area, and community offices
- Capital asset lists and lists of property holdings
- Research and technical data, such as maps, plans, charts, of an important or irreplaceable nature
- Topographic and demographic data
- Climatological data

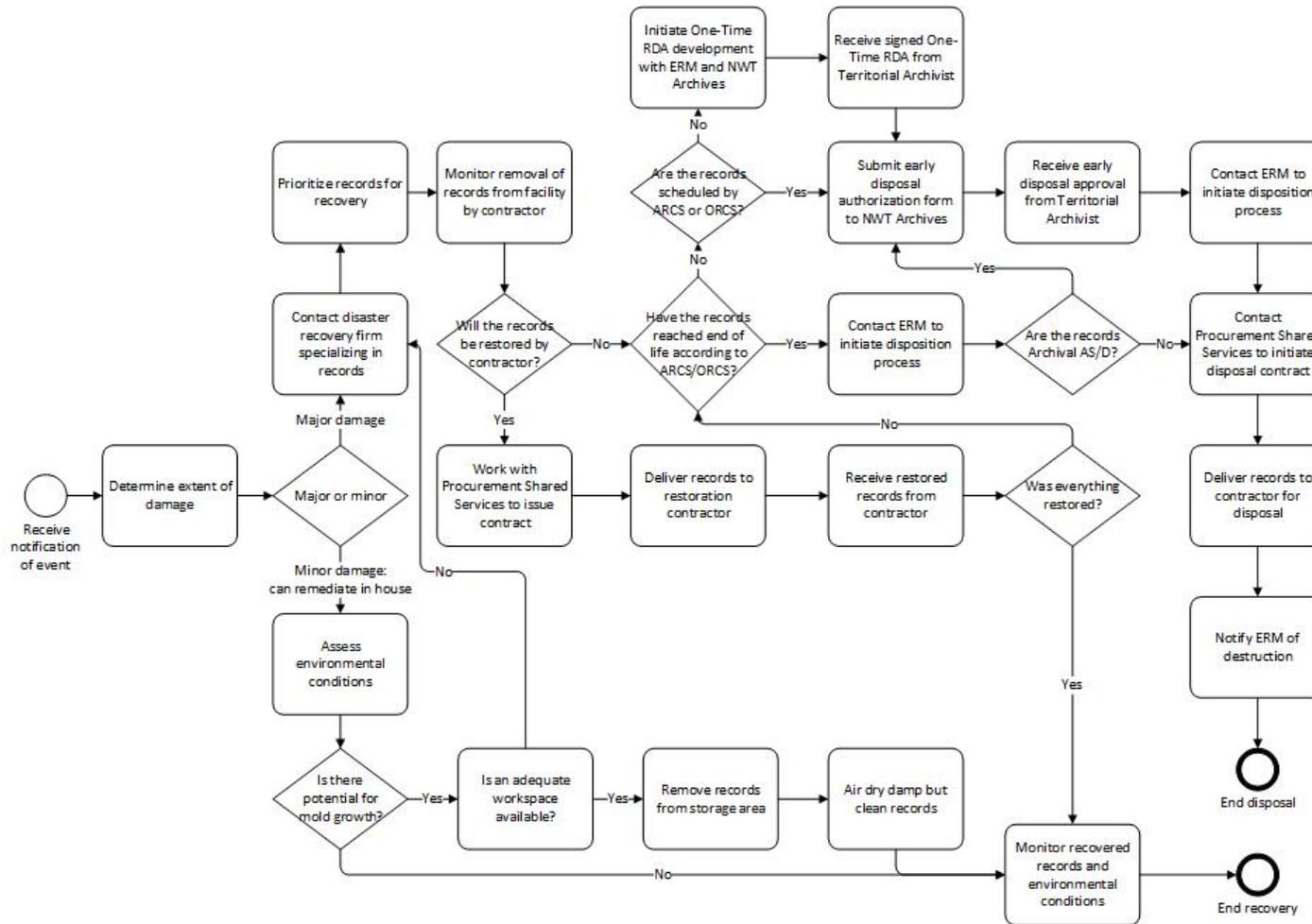
## Appendix C Examples of Substantive and Transitory Records

This is not an exhaustive list. Contact the Department Records Management Team for assistance in identifying substantive and transitory records.

<b>Substantive Records</b> Create and keep as official records	<b>Transitory Records</b> Non-records. Destroy when no longer needed unless subject to a disposition hold.
<ul style="list-style-type: none"> <li>• Advice, recommendations, and decisions, as well as background material.</li> <li>• All financial transactions as well as supporting documentation.</li> <li>• All information showing how information systems have been maintained.</li> <li>• All records showing that services have been provided or obligations have been incurred.</li> <li>• Approvals and authorizations.</li> <li>• Asset inventory and control records.</li> <li>• Audits and evaluations, as well as all background material.</li> <li>• Contracts and other legal agreements, as well as background material.</li> <li>• Important telephone, e-mail, and face-to-face discussions.</li> <li>• Planning and budget records, as well as all background material.</li> <li>• Policies and procedures, as well as background and interpretive material.</li> <li>• Proposed legislation and regulations, as well as background material.</li> <li>• Records of contact or correspondence with clients, consultants, vendors, partners, agents, indigenous groups, and the public.</li> <li>• Records relating to the issuance of licenses, permits, and leases.</li> <li>• Records showing the planning, approval, and execution, and results of projects.</li> <li>• Work done by consultants and others.</li> </ul>	<ul style="list-style-type: none"> <li>• Blank information media, such as unused forms, removable hard drives, erased audio and video tapes, CDs, and DVDs. <b>Note:</b> accountable forms must be logged before they are destroyed. Digital and magnetic media must be degaussed, wiped, or physically destroyed to ensure the data is not recoverable.</li> <li>• Duplicate copies of a substantive record which do not have comments written on them.</li> <li>• Junk mail and spam.</li> <li>• Mass distribution notices and e-mail messages which do not affect your duties.</li> <li>• Notes and rough drafts of letters, memos, reports, minutes, etc, which were transcribed into a final record. <b>Note:</b> this information should be kept as a substantive record if it contains major revisions or helps to show how the final document was created. It should also be kept if it helps account for official decisions. Draft legislation, budgets, policies, standards, guidelines, and other legal documents should be kept as substantive records.</li> <li>• Publications from outside your office, such as supply catalogues, equipment manuals, textbooks, brochures, and newsletters.</li> <li>• Temporary information, such as simple messages, routing slips, and post-it notes which do not require follow-up. <b>Note:</b> this information should be kept as a substantive record if it helps to show how a department reached a decision.</li> </ul>

## Appendix D Example Disaster Salvage and Recovery Workflow

<b>Issued:</b>	December 2021
<b>Last Updated:</b>	December 2021



## Appendix E Glossary

**Access** refers to the right, opportunity, or means of finding, viewing, using, or retrieving information.

**Access to Information and Protection of Privacy Act (ATIPP Act)** refers to legislation which gives the public the right to request access to information held by Northwest Territories public bodies as well as the right to request a correction to personal information. The legislation also sets out when a public body may collect, use, and disclose personal information. The ATIPP Act further provides for an independent review by the NWT Information and Privacy Commissioner of the decisions made under the Act.

**Access to Information Coordinator** refers to the employee within a public body who has been designated as an access and privacy coordinator as per the *Access to Information and Protection of Privacy Act*.

**Access to information request** refers to a written request for information made under the *Access to Information and Protection of Privacy Act*.

**Accountability** refers to the Generally Accepted Recordkeeping Principle: a senior executive (or a person of comparable authority) shall oversee the information governance program and delegate responsibility for records and information management to appropriate individuals. The organization adopts policies and procedures to guide personnel and ensure that the program can be audited.

**Active** refers to the initial phase of the records life cycle where records are required on a regular basis.

**Active records** are readily accessible records related to current, ongoing, or in-process activities and are referred to on a regular basis to respond to day-to-day business requirements. (ARMA International)

**Administrative records** are records documenting common management processes, activities, and functions including planning and organization, committee participation, drafting of agreements and contracts, legal matters, and communications. Administrative records support “housekeeping” functions such as the management of facilities, property, material, finances, personnel, and information systems. Administrative records are common to all offices and are distinct from operational records.

**Administrative Records Classification System (ARCS)** is the government-wide standard for identifying, describing, organizing, classifying, managing, and disposing of all types of administrative (housekeeping) records. Administrative records support “housekeeping” functions such as the management of facilities, property, material, finances, personnel and information systems. Administrative records also relate to common management processes including

committees, agreements, contracts, information services, legal opinions, and other similar functions.

**Analogue records** refer to physical records of various media types (text, photographic, film, microfilm, blueprints, maps, audio, et cetera) that does not require a computer to view embedded information.

**Archival records** are records selected for permanent preservation and held by the NWT Archives.

**Archival selection** refers to the process whereby the NWT Archives determines which government records will be retained permanently to document the history and operations of the GNWT. Government records which are not selected by the NWT Archives are destroyed.

**Archives** (1) *see NWT Archives.* (2)

**Archives Act** refers to legislation which establishes the position of the Territorial Archivist the institution of the NWT Archives. The *Archives Act* defines GNWT records and stipulates that they must be transferred to the Territorial Archivist within 30 years of their creation unless legally disposed of according to an approved records disposition authority.

**ARCS** *see Administrative Records Classification System.*

**AS/D** *see Archival Selection.*

**Asset** refers to something having value, such as a possession or property, that is owned by a person, business, or organization.

**ATIPP** *see Access to Information and Protection of Privacy Act.*

**Authentic** means that the record is what it purports to be and that it is free from tampering or corruption.

**Authenticity** refers to the sum of the qualities of a record that establishes the origin, reliability, trustworthiness, and correctness of its content.

**Authoritative** refers to something which contains complete and accurate information and is therefore respected.

**Availability** refers to the Generally Accepted Recordkeeping Principle: an organization shall maintain its information assets in a manner that ensures their timely, efficient, and accurate retrieval when needed.

**Backlog** *see Legacy records.*

**Box** (noun) refers to (1) a rectangular container with stiff sides and sometimes a lid; or (2) a box and its contents, or just the contents of a box.

**Box** (verb) refers to the act of putting something in a box.

**Box Inventory Form** refers to a form used to create a records location system to assist departments in retrieving their inactive records from the records centre. A box inventory form lists records, file by file, that are located within each records centre box.

**Box Inventory Report** refers to a DIIMS report used to create a records location system to assist departments in retrieving their inactive records from the records centre. A box inventory report lists records, file by file, that are located within each records centre box.

**Classification** refers to the organization of materials into categories according to a scheme that identifies, distinguishes, and relates the categories. Classification may involve physically arranging the materials or the use of a class code to index and retrieve documents stored in a different order. For electronic documents, classification may involve assigning a class code used to index and retrieve the document.

**Classification system** refers to a systematic arrangement of records into functional or subject groups using numbers or letters for identification.

**Classify** refers to the act of assigning the appropriate filing code to records according to the established records classification system.

**Close** means (1) to cause something to change from being open to not being open; or (2) to cause something to end.

**Closed file** refers to a file on which action has been completed and to which electronic or physical documents are unlikely to be added. The file may be closed because the activity or event to which it relates has ended or due to system design procedures (e.g. the specification that all records are to be closed at the end of a fiscal or calendar year).

**Closed volume** refers to a volume of a file that has been cut-off at a definite time period or due to the file exceeding 2.5 cm (1 inch) in thickness.

**Closure criteria** (plural of closure criterion) refers to the standard by which a judgement or decision may be made to close a file. In the GNWT, file closure criteria are identified in records disposition authorities.

**Colour coding** refers to the use of colour in a paper filing system to identify file folders or records with certain characteristics to improve speed of access and to reduce the chance of misfiles. (ARMA International)

**Compliance** refers to the Generally Accepted Recordkeeping Principle: an information governance program shall be constructed to comply with applicable laws, other binding authorities, and the organization's policies.

**Confidential information** refers to information whose disclosure is prohibited by law, regulation, or court decision, or has the potential to harm the privacy of individuals or the security of the entity.

**Confidential records** are records containing certain information that requires protection against unauthorized access or disclosure.

**Convenience copies** refer to duplicate copies (either in digital or analog format) of master records created for ease of access and use. Convenience copies are not substitutes or replacements for master records and cannot be relied upon as a record of actions, transactions, or decisions. See also Transitory Record.

**Conversion** refers to the process of changing documents and records from one storage medium, application, and/or system to another.

**Copy file** refers to a record that is a copy of and is maintained in addition to the master file. A copy file is kept for reference purposes and is not used or relied upon as the government body's official record of its actions, business transactions, decisions, policies, and approvals.

**Creation** refers to the act of creating, making, or producing something, such as a document or record.

**Custody** means safekeeping or care.

**Cut-off** refers to the time at which a file should be declared closed. This is usually at the termination of an event or project or at the end of a calendar or fiscal year.

**D** *see Destroy.*

**Data** is the smallest meaningful units of recorded information.

**Database** refers to (1) a set of structured data elements consisting of at least one file, or a group of integrated files, usually stored in one location and made available to multiple users simultaneously; and (2) a database management system, which is a software system used to record, access, and retrieve data stored in a database.

**Department Records Management Team** refers to the business unit designated by a government body to be responsible for the development and overall administration of the government body's records and information management program.

**Destroy** means to damage something so badly that it cannot be used or no longer exists.

**Destruction** *See Final disposition.*

**Devolution** refers to the moving of power or responsibility from a main organization to a lower level, or from a central government to a local government. In the GNWT, Devolution usually refers to the devolution of responsibility over land and resources from the Government of Canada to the GNWT in 2014 as per the *Northwest Territories Devolution Act* and the *Northwest Territories Land and Resources Devolution Agreement* but may refer to earlier transfers of responsibility from the federal government to the territorial government.

**Digital** is any data or recorded information that exists as binary code (zeros and ones).

**Digital Integrated Information Management System (DIIMS)** is an enterprise GNWT-wide solution that enables the GNWT to gain better access and control of its electronic information throughout the organization. It is a content lifecycle management system that provides organizations with the tools to manage and share corporate information through its lifecycle from a single repository.

**Digitization** is the process of converting records from analogue (physical) formats to digital formats.

**Digitized record** is a record that has been converted from an analogue record to a digital record format.

**Digitize** means (1) to convert something to a digital form; or (2) to put information into the form of a series of the numbers 0 and 1, usually so that it can be understood and used by a computer.

**DIIMS** *see Digital Integrated Information Management System.*

**DIIMS Records Classifier Reports** refers to an internal web page containing reporting tools for monitoring the use of the DIIMS system and for performing records management tasks.

**Directive** refers to formal instruction that obliges departments to take or avoid specific action.

**Disclosure** refers (1) to the act of making something known or the fact that is made known; or (2) something that was not previously known or the act of giving such information to the public.

**Disposal** refers to the act of getting rid of something.

**Disposition** refers to the final action taken per the retention schedule, concluding with the destruction, transfer, or permanent preservation of a record.

**Disposition halt** *see Disposition hold.*

**Disposition hold** refers to the suspension of the scheduled destruction of records due to foreseeable or pending litigation, investigation, audit, or special organizational requirements.

Division in the GNWT refers to the separation of the Northwest Territories into the Territory of Nunavut and the Western Arctic, which retained the name of Northwest Territories, in 1999, as per the *Nunavut Act* and the *Nunavut Land Claims Agreement*.

**Document** (noun) refers to (1) any written or printed work; or (2) information or data fixed in some media. *See also Record.*

**Document** (verb) means to record the details of an event, a process, etc.

**Electronic information** refers to information that is recorded and stored in an electronic format.

**Electronic record** is an analogue or digital record that is carried by an electrical conductor and requires the use of electronic equipment to be intelligible by a person.

**Enterprise Information Management** refers to the division in the Department of Infrastructure with responsibility for the enterprise, GNWT-wide, records and information management program.

**Essential records** *see Vital records*

**File** refers to a group of documents related by use, topic, or case, housed together in an electronic or paper folder or group of folders, and arranged in a logical sequence.

**File closure** Criteria *see Closure criteria*.

**File folder** refers to a paper folder in which papers and documents are collected and organized for retrieval. *See also Folder*.

**File list** refers to a comprehensive list of all of the files associated with a particular storage location or organization. Also called a register, it provides evidence that a record has been created or captured in a recordkeeping system and facilitates retrieval. It records descriptive information about the record and assigns a unique identifier to the record.

**File naming convention** is a convention or generally agreed scheme for naming files. Well-chosen naming conventions aid in navigating and searching for information.

**Final disposition** is the final action taken with regard to a group of records after their inactive phase has ended. It may be either destruction or transfer to the NWT Archives.

**Folder** refers to (1) a directory structure that organizes electronic files into groups (a directory or sub-directory); or (2) a sheet of cardboard or heavy paper stock that is used as a loose cover to keep documents and other flat materials together, especially for purposes of filing.

**Format** refers to the material onto which information or data has been recorded and may subsequently be used (i.e. paper, microfilm, electronic).

**Generally Accepted Recordkeeping Principles** (the Principles) refers to a framework of definitive principles for governing an organization's information as a strategic asset. These information governance principles support organizational goals, facilitate compliance with regulatory, legislative, and information management requirements, and limit risks.

**Geographic information system** (GIS) refers to a combination of hardware, software, and rules that supports complex analysis of geospatial and temporal information and that often uses static or dynamic maps for reports.

**GIS** *see Geographic information system*

**GNWT Data Network** refers to the GNWT communications network that transmits data. (The Free Dictionary)

**Government body** means (a) a department, branch or office of the Government of the Northwest Territories, (b) an agency, board, commission, corporation, office or other body designated in the regulations to the *Archives Act*, or (c) the office of a member of the Executive Council.

**Government records** *see Public records.*

**Guideline** means a document providing guidance, advice or explanation to managers or functional area specialists.

**Halt** *see Disposition hold*

**Health Information Act (HIA)** refers to legislation which protects people's privacy by governing the collection, use, sharing, and storage of their personal health information. The Act recognizes both individuals' rights to access their own information and the needs of health service providers to collect, use, and share patient information in order to provide best care.

**HIA** *see Health Information Act*

**Hold** *see Disposition hold*

**Inactive records** refer to records which are not required for regular use, but which have not yet reached the time for final disposition. *See also Semi-active records.*

**Information** refers to data that has been given value through analysis, interpretation, or compilation into a meaningful form.

**Information systems** store and provide access to information or data.

**Integrity** refers to the record being complete and unaltered in all essential respects.

**Inventory** (noun) refers to (1) a detailed listing that includes the types, locations, dates, volumes, equipment, classification system, and usage data of an organization's records.

**Inventory** (verb) refers to the process of identifying all records of an organization.

**Label** refers to a tag, piece of paper, or other material with identifying information attached to the thing identified.

**Legacy records** refer to set of older records which need to be organized, classified, and scheduled in accordance with a records disposition authority. In the GNWT legacy records are frequently referred to as "backlog records."

**Legislation** refers to a law or set of laws made official by a parliament or legislature.

**Life cycle** or **Lifecycle** means the span or time from the creation or receipt of a record through its useful life to its final disposition.

**Maintenance** refers to the work needed to keep something in good condition.

**Master record** is a record that is considered the official record and is considered a true and valid record by both the creator and for legal purposes. Also referred to as a substantive or authoritative record.

**Metadata** refers to data describing content, structure, and context of records and their management through time. Metadata can be divided into one of three categories:

- Descriptive metadata describes a resource for purposes such as discovery and identification. Metadata in this area can include such elements as author, title, and description.
- Structural metadata indicates how compound objects are put together. It identifies data format, media format, or the type of data representation and file types, hardware and software needed to render the data, and the compression method and encryption algorithms used, if any.
- Administrative metadata provides information to help manage a resource, such as when and how it was created, and who can access it.

**Migration** refers to the process of moving recorded information from one information system configuration to another or from one storage medium to another without making changes to format.

**Monitor** (verb) means to watch or check a situation carefully for a period of time in order to discover something about it.

**MOV** (Apple Quicktime Movie) is a file format used to store video, audio, time code, and text tracks.

**Naming convention** *see File naming convention.*

**Nil** in a records disposition authority means zero years or no retention period assigned.

**Non-record** *see Transitory record.*

**NWT Archives** refers to all public records and other documentary material under the care, custody, and control of the Territorial Archivist. This term is commonly used to refer to the organization that is managed by the Territorial Archivist and which looks after the NWT Archives. It is also commonly used to refer to the facilities in the Prince of Wales Northern Heritage Centre that house the NWT Archives.

**Official record** *see Master record.*

**One-Time Records Disposition Authority** refers to a records disposition authority used to authorize and process the disposition of a specific group of records, such as the records of a discontinued program or service.

**Operational records** refers to records that are related to the operations and services provided by a government body in carrying out the functions for which it is responsible according to statute, mandate, or policy. Operational records are distinct from administrative records and are unique to each government body.

**Operational Records Classification System (ORCS)** is the government-wide standardized system for the classification, filing, retrieval, retention and disposition of operational records. Each

government body will have one or more ORCS. Operational records are those records which relate to the operations and services provided by a government body in carrying out the functions for which it is responsible according to statute, mandate, or policy. Operational records are distinct from administrative records and are unique to each government organization.

**ORCS** *see Operational Records Classification System.*

**Original** *see Master record.*

**Out card** or **outcard** refers to a device used to replace material that has been removed from a file and indicate what was taken, by whom, and when.

**Ownership** refers to the state or fact of owning something.

**PDF** (Portable Document Format) refers to a file format that captures formatting information from a variety of applications and makes it possible to transmit and display records in an identical way, independent of the platform. PDF is an ISO standard, ISO 32000-1:2008 and ISO 32000-02:2017.

**PDF/A** (Portable Document Format/Archival) refers to a long-term preservation formation for electronic records. Everything needed to render or print a PDF/A file must be contained within the file. This includes all visible content like text, raster images, vector graphics, fonts, colour information, etc. PDF/A is an ISO standard, ISO 19005-1:2005, ISO 19005-2:2011 and ISO 19005-3:2012.

**Permanent return** means a file or box has been retrieved from a GNWT records centre and will not be returned to the records centre, usually because the contents of the file or box are being changed.

**Personal information** refers to any information that can be used in isolation or in combination with other sources to uniquely identify, contact, or locate a specific individual. Also referred to as personally identifiable information or PII.

**Physical item** refers to a paper file folder, records centre box, document, or other item that takes a physical, usually paper, format.

**PNG** (Portable Network Graphics): A raster graphics file that supports lossless data compression.

**Policy** refers to a formal direction that imposes specific responsibilities on departments. Policies explain what deputy heads and their officials are expected to achieve.

**Preservation** refers to the process and operation involved in ensuring the technical and intellectual survival of authentic records over time.

**Procedure** refers to the manner and steps in which some action is taken which may be written or unwritten.

**Protection** refers to a Generally Accepted Recordkeeping Principle: an information governance program shall be constructed so the information assets generated by or managed for the organization have a reasonable and suitable guarantee of authenticity and reliability.

**Public record** means a record that is created by or for or is received by a government body in carrying out its activities, but does not include

- (a) a record of the Legislative Assembly, the office of the Speaker of the Legislative Assembly or the office of the Clerk of the Legislative Assembly,
- (b) a record of a committee of the Legislative Assembly,
- (c) a record of a member of the Legislative Assembly, other than a member of the Executive Council,
- (d) a record of a member of the Executive Council that relates to his or her activities as a member of the Legislative Assembly,
- (e) correspondence sent or received by a member of the Legislative Assembly, unless the correspondence relates to his or her responsibilities as a member of the Executive Council,
- (f) a record of a member of the Legislative Assembly, including a member of the Executive Council, that relates to his or her constituency office or to his or her representation of constituents, or
- (g) a surplus copy of a record or a copy of a record that is created only for convenience of reference.

**Quality assurance** refers to procedures for monitoring and accessing the records system, aiming to maintain a desired level of quality.

**Quality control** refers to a system of maintaining predetermined standards in a digitized record by testing/reviewing a sample of the output against the specifications within the standard.

**Reactivation** *see Permanent return*

**Recordkeeping** refers to the systematic creation, use, maintenance, and disposition of records to meet administrative, programmatic, legal, and financial needs and responsibilities.

**Recordkeeping system** refers (1) to coordinated policies and procedures that enable records to be collected, organized, and categorized to facilitate their management, including preservation, retrieval, use, and disposition; or (2) to an information system which captures, manages, and provides access to records over time.

**Record** is a record of information, regardless of its form and characteristics, the means by which it was created and the media on which it may be stored and, without limited the generality of the foregoing, include

- (a) a document, book, ledger, photograph, image, audio-visual recording, x-ray, map and drawing, and
- (b) a record created or stored in digital or other intangible form by electronic means,

but does not include software or a mechanism that produces records.

**Records and information management (RIM)** refers to the field of management responsible for establishing and implementing policies, systems, and procedures to capture, create, access, distribute, use, store, secure, retrieve, and ensure disposition of an organization's records and information.

**Records centre or records center** refers to a storage facility operated by the Department of Infrastructure which is responsible for the transfer, processing, storage, and retrieval of inactive records owned by government bodies.

**Records coordinator** refers to a member of the Department Records Management Team who is charged with coordinating some or all of the elements of the government body's records and information management program. Records coordinator also refers to a role assigned to some individuals within DIIMS.

**Records Disposition Authority (RDA)** a plan respecting the preservation and destruction of public records as described in the *Archives Regulations*, which must (a) include a comprehensive description of each class of public records; (b) specify the criteria for determining whether a class of public records should be preserved or destroyed; and (c) specify the minimum periods during which the government body must retain each class of records that it intends to destroy.

**Records inventory** *see Inventory*

**Records life cycle** *see Life cycle*

**Records management** *see Records and information management*

**Records scheduling** refers to the process of planning the life cycle of a record, including the establishment of retention periods for their active, semi-active, and inactive phases, selection of departmental or records centre storage for semi-active and inactive records, and determination of whether records will be destroyed or transferred to NWT Archives when they are no longer needed by the government body.

**Records Transfer Slip** refers to a form used to identify a set of records centre boxes (a transfer) which is ready to be shipped to a GNWT records centre.

**Register** (noun) *see File list.*

**Reliable record** is a record whose contents can be trusted as being the full and accurate representation of a transaction.

**Repository** refers to a physical or digital storage area where documents and records are kept.

**Retention** refers to the continued use, existence, or possession of something or someone.

**Retention and disposition schedule** *see Records Disposition Authority.*

**Retention period** refers to the length of time a record must be retained in order to satisfy administrative, fiscal, legal and research requirements of a government body. Retention periods are usually specified in number of years or by reference to the termination of a project or event.

**Retention schedule** *see Records Disposition Authority. Also referred to as a Records Retention Schedule, a Retention and Disposition Schedule, or a Records Schedule.*

**Retrieval** refers to (1) the process of locating and withdrawing a physical record from a filing system or a records centre; or (2) the action of searching and accessing electronic records from stored data on a computer system.

**RIM** *see Records and information management*

**S/O** *see Superseded/Obsolete*

**Semi-active** refers to the intermediary stage in the records life cycle where records are still needed but are not in daily use.

**Semi-active record** means a record that is no longer required for constant referral in the course of daily business, but which is still of some use to the government body. The record may be required for occasional consultation and may be retained because of administrative or legal requirements.

**Standard** refers to a set of operational or technical measures, procedures, or practices for government-wide use. Standards provide more detail on how managers and functional specialists are expected to conduct certain aspects of their duties.

**Storage** means the act of putting and keeping of things in a special place for use in the future, or the place where you put things.

**Substantive record** means written evidence that an action did or did not happen, transactional records, decisions, and policies.

**Superseded/Obsolete (S/O)** is used in retention schedules to identify records which must be kept as an open file until the occurrence of an event. When the event occurs the S/O is triggered and the file is closed. Examples of events include expiration of a contract, end of a project, cancellation of a program, disposal of an asset, or the resolution of a claim.

**Technology Service Centre (TSC)** refers to a division in the Department of Infrastructure which is responsible for providing and managing information technology services (IT) for the GNWT, such as e-mail, IP phone system, application and website hosting, network and internet, mobile devices, purchasing of computers and software, and computer evergreening.

**TIFF** (Tagged Image File) is an open standard image format for storing raster graphic images. TIFF files are lossless, meaning they are in an uncompressed format. TIFF is an ISO standard, ISO 12639:2004.

**Transfer** (noun) refers to a group or set of records centre boxes and the records contained within.

**Transfer** (verb) refers to (1) the movement of records from one storage location to another; or (2) the change of custody, ownership, and/or responsibility for records.

**Transitory** means (1) lasting for only a short time; or (2) not permanent or temporary. (Cambridge Dictionary)

**Transitory records** are records that are needed only for a limited time for the completion of a routine action or to prepare a subsequent record. Transitory records do not include records required by government organizations to control, support, or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of the government.

**Transparency** refers to a Generally Accepted Recordkeeping Principle: an organization's business processes and activities, including its information governance program, shall be documented in an open and verifiable manner, and that documentation shall be available to all personnel and appropriate interested parties.

**Trigger** refers to an occurrence, either calendar-or event-based that begins a retention period (ARMA International)

**TSC** *see Technology Service Centre*

**Unscheduled records** mean records which have not been classified and scheduled in accordance with an approved records disposition authority.

**Vital record** refers to a record that is fundamental to the functioning of an organization and necessary to the continuance of operations. Also referred to as an essential record.

**Vital statistics record** refers to a record of the civil registration of a birth, marriage, divorce, change of name, change of sex designation, or death.

**Volume** refers to (1) one of a set of file folders which together form a single file or relate to a single person, place, thing, case, or subject matter; or (2) in DIIMS, a physical file folder.

**WAV** (Waveform Audio File) is an audio file format standard used for storing an audio bitstream. It is usually uncompressed.

## Sources

*Archives Act*, R.S.N.W.T. 1988, c.A-6

ARMA International, *Glossary of Records Management and Information Governance Terms*, 5<sup>th</sup> edition, ARMA International TR 22-2016, Overland Park, KS: ARMA International, 2016.

Cambridge University Press, *Cambridge Dictionary*, <https://dictionary.cambridge.org/>, accessed May 2020.

Canada, Treasury Board, *Foundation Framework for Treasury Board Policies*, <https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=13616>, accessed May 2020.

*Merriam-Webster Dictionary*, <https://www.merriam-webster.com/>, accessed May 2020.

New South Wales, State Archives and Records, *Glossary of Recordkeeping Terms*, <https://www.records.nsw.gov.au/recordkeeping/resources/glossary>, accessed May 2020.

Northwest Territories, Department of Health and Social Services, *Health Information Act Guide: A Practical Guide to the Northwest Territories' Health Privacy Legislation*, Yellowknife, NT, 2015.

Northwest Territories, Department of Justice, *Access and Privacy Directory 2019*, Yellowknife, NT, 2019.

Northwest Territories, Department of Public Works and Services and Northwest Territories Archives, *Records Management Glossary*, Yellowknife, NT, 2002.

Society of American Archivists, *Dictionary of Archives Terminology*, <https://dictionary.archivists.org/index.html>, accessed May 2020.

*The Free Dictionary by Farlex*, <https://www.thefreedictionary.com/>, accessed May 2020.

University of British Columbia, *Electronic Records Management Guidelines*.