

Ministry of Finance Information Destruction Procedures

Contents

Overview	2
Purpose	2
Roles and Responsibilities	3
Destruction Procedure.....	5
Commitment to Review	7
Approval of Information Destruction Authorization Model.....	7
Appendix A: Resources	8
Training	8
Forms.....	8
Tools	8
Additional Information	8

Overview

This document informs and consolidates the Ministry of Finance's defensible information destruction policies and procedures.

Although [Part 2 of the GRS Defensible Information Destruction Guide](#) states there are two types of destructions, Information Destruction Authorizations (IDA) and Redundant Source Information (RSI) Destructions, the Ministry of Finance IDA model considers both types as one simple concept: the destruction of information.

The definition of information, for the purposes of this document, includes:

- Physical records kept on-site (paper, audiovisual, photos, discs etc.), including those managed in EDRMS (p-folders)
- Digital records managed in EDRMS (e-folders), on a LAN, or stored in systems
- Data and metadata stored in systems
- Redundant source information¹

This process does not apply to the following records:

- Records stored off-site (these are handled through a 60-Day Notices process)
- Records with a final disposition of Selective Retention (SR) or Full Retention (FR)
- Records scheduled under the Transitory Information Schedule

If there are questions about the 60-Day Notices process, please contact your Information Management Analyst or the Ministry Coordinator.

Purpose

This document outlines the destruction process for eligible, scheduled ministry information. Information covered under this process becomes eligible once it has reached the Final Disposition stage and has a final disposition of DE (Destroy).

This Finance Information Destruction Application (IDA) Model meets the GRS requirements set by [section 4.1](#) of the Defensible Information Destruction Guide. Requirements are met by the establishment and approval of a defensible process that includes established roles and responsibilities, authorizations, and documentation managed in an appropriate recordkeeping system. The Ministry of Finance uses EDRMS as their appropriate system.

¹ Redundant source information destruction is covered under Step 5 of this process

Roles and Responsibilities

In the Ministry of Finance, all employees have information management responsibilities, including the appropriate destruction of information.² In addition, the overarching responsibility for the governance of information management³ falls to the Deputy Minister and can be delegated. When delegated, it is the responsibility of the delegated positions to ensure the proper organizational structure as well as policies and procedures are put in place and enforced within their divisions and branches.

Destruction must be adequately documented in order to comply with the *Information Management Act*, which includes maintaining a record of destruction approval for the current calendar year plus 30 years.

There are various duties that must be completed which will depend on each branch's internal structure. However, for the most part the destruction process will not change at a branch level.

Location	Roles	Overview
Ministry of Finance	All Employees	All employees have information management responsibilities as indicated in the Appropriate Use Policy: <ul style="list-style-type: none">• Be aware of and fulfill their IM/IT obligations• Employees must only dispose of government information in accordance with an approved information schedule.
Program Area	Preparer	Preparer is the Records Management Contact assigned by the program area <ul style="list-style-type: none">• Possesses sound knowledge of the program's information, recordkeeping systems and relevant classifications.• Prepares adequate documentation pertaining to government information destructions.• Acquires approvals; arranges and carries out destruction actions.

² Appropriate Use Policy 1.4. Employees must only dispose of government information in accordance with an approved information schedule.

³ See the [Core Policy and Procedures Manual Chapter 12: Information Management and Information Technology Management](#) and the [Managing Government Information Policy](#) for responsibilities

Program Area	Approver	<p>Approver is the Executive Director or their delegated authority</p> <ul style="list-style-type: none"> • Confirms that records are not required for operational requirements, related litigation, legal action, requests made under FOIPPA, or investigations that are underway or anticipated.
Corporate Services Division	Ministry Coordinator	<p>Coordinator is the Ministry Information Management Officer</p> <ul style="list-style-type: none"> • Provides governance, oversight, and administration of the Ministry Destruction Authorization Model • Provides the resources, tools, and forms for ministry program areas to adequately document destructions • Issues destruction control numbers and documents approvals and actions • Verifies the accuracy of destruction documentation. • Authorizes destruction request • Maintains the OPR 432-30 file for the mandated retention period • Liaises with IMB for data destruction and destruction within systems
Any Division	Information Mgmt Analyst, or equivalent Information Management professional	Can be contacted for assistance and guidance during the destruction process
Information Management Branch (IMB)	Lead for systems-related information management	Consultation with IMB is required for all system-related destruction, including migrations or system decommissioning.
Government Records Services, CITZ	Government Records Officer (GRO)	<ul style="list-style-type: none"> • Update status of records logged in EDRMS once confirmation of destruction received • Authorize destruction for migrated or digitized information with an approved disposition of SR or FR as required by the Redundant Source Information Schedule process. • Authorize destruction of information with an approved disposition of SR once the information has been assessed by an archivist.

See [Appendix A](#): list of training requirements for the roles listed above

Destruction Procedure

Information Destruction Application (IDA) Steps	Roles
1. Request IDA destruction – initiate process by contacting the Ministry Coordinator	Preparer
2. Assign and log the IDA destruction number (IDA#) 3. Open an OPR ARCS 432-30 file. 4. If not already completed, provide necessary forms and instructions: <ul style="list-style-type: none"> ○ IDA form (ARS518) ○ RSIS digitization form (ARS667) for digitization ○ RSIS migration form (ARS668) for migration (under development) ○ File list template, if necessary or include an EDRMS file list ○ Tobacco Litigation Form D as required 	Ministry Coordinator
5. Complete destruction form(s) and create file list. <ul style="list-style-type: none"> • Program Area retains an OPR file under ARCS 432-35. <p>For Redundant Source Information (RSI)</p> <ul style="list-style-type: none"> • for digitized information (category 4) <ul style="list-style-type: none"> ○ Ministry Coordinator provides form (ARS667) to document the requirements of a digitization project before approving destruction of redundant source records ○ If GRS consultation is required, the Ministry Coordinator will contact Government Records Officer (GRO) and consult with both GRS and the program area. • for migrated & converted information (category 3) <ul style="list-style-type: none"> ○ Collaborate with IMB contact to complete the IDA form (ARS518) ○ Complete an ARS668 Migration RSIS Form (under development) ○ If GRS consultation is required (e.g. final dispositions of SR or FR, or no approved information schedule), the Ministry Coordinator will contact Government Records Officer (GRO) and consult with both GRS and the program area. ○ Ministry migration process to be developed 	Preparer IMB Contact
6. The Preparer will acquire program area approval to confirm the information: <ul style="list-style-type: none"> • is eligible for destruction • is no longer necessary for operational requirements (close triggers/SO are met) 	Preparer Approver

<ul style="list-style-type: none"> is not needed for any litigation, investigations, or FOIPPA requests that are underway or anticipated. 	
7. Submit completed documentation capturing approvals to the Ministry Coordinator via the original email chain and include IDA# in email subject line.	Preparer
8. Review documentation for accuracy and completeness. If necessary, return documentation to Preparer for edits or clarification. Confirm the IDA contains appropriate schedules/classifications, and that IM practices and principles are present. <ul style="list-style-type: none"> See ARCS or appropriate ORCS If accurate and complete, provide the administrative destruction approval. If either of the following applies, send to GRS@gov.bc.ca for final review and approval: <ul style="list-style-type: none"> Seeking destruction authorization for digitized or migrated information with an approved disposition of SR or FR as required by the Redundant Source Information Schedule process. See the Redundant Source Information Schedule for whether an additional form is required. Seeking destruction authorization for information with an approved disposition of SR in order to have it assessed by an archivist. 	Ministry Coordinator
9. Send administrative approval to Preparer, and IMB contact, if relevant. File documentation under ARCS 432-30 and update the destruction log.	Ministry Coordinator
10. Complete destruction. IMB contact assisting with data destruction within systems and migration projects.	Preparer IMB Contact
11. Confirm destruction of records by email to the Ministry Coordinator. Preparer will CC GRS@gov.bc.ca . <ul style="list-style-type: none"> Reply to original email chain and include a description of the method used to destroy the information and the actual date they were destroyed. 	Preparer Ministry Coordinator

<ul style="list-style-type: none"> • See RIMM Section 501A for approved methods of destruction <ul style="list-style-type: none"> ○ Records are considered destroyed when: <ul style="list-style-type: none"> ▪ They are put into a secure Shred-It bin ▪ They are shredded (by the employee or by a contracted company) as per RIMM Section 501A ▪ Otherwise destroyed as per RIMM Section 501A <p>GRO team updates EDRMS status and replies all confirming completion. All parties file confirmation emails.</p>	
12. Update tracking log, include date of destruction confirmation.	Ministry Coordinator

Commitment to Review

The Ministry Information Management Officer commits to completing a fiscal year-end review of the destruction program to evaluate the program's effectiveness and efficiency and to action adjustments to the model where necessary.

Approval of Information Destruction Authorization Model

Name	Title	Date
Jennifer Peters	Ministry Information Management Officer	Nov 1, 2022
Melinda McClung	Senior Data Architect, Lead for Information Management in Systems	Nov 1, 2022
HB Teo	Ministry Chief Information Officer	Nov 8, 2022
Nicole Wright	ADM, Corporate Services Division Information Management Ministry Lead (IMML)	Nov 21, 2022

Appendix A: Resources

Training

[Role-Based Learning](#)

Ministry-specific training may be offered on an ad hoc basis

Forms

[Information Destruction Log ARS](#)

- For the Ministry Destruction Coordinator

[ARS518 – Information Destruction Authorization \(IDA\) Form](#)

- Required for all destruction applications

[ARS661 – File List](#)

- Required if there is no EDRMS-generated file list

[ARS667 – Destruction after Digitization Authorization Form](#)

- Required for the destruction of redundant source information after digitization

[ARS668 – Migration RSIS Form \(under development\)](#)

- Required for the destruction of redundant source information after migration or conversion

[Form D – Tobacco Litigation Form](#)

- Required to check for records that contain information potentially relevant to tobacco litigation.

Tools

[Defensible Destruction Process Checklist](#)

[FIN Information Management Policies and Procedures Manual](#) (to be updated)

Additional Information

[Managing Government Information Policy \(MGIP\)](#)

[Defensible Information Destruction Part 1](#)

- Establishing an Information Destruction Model
- For the Ministry Destruction Coordinator

[Defensible Information Destruction Part 2](#)

- Completing Destruction
- For any employees involved in the destruction process

[Administrative Records Classification System \(ARCS\)](#)

[Operational Records Classification Systems \(ORCS\)](#)

[Special Schedules](#)

- Executive Records
- Transitory Information
- Redundant Source Information

[Digitization Resources](#)

- [Digitizing Government Information Standard](#)
- [Digitizing Government Information Guide](#)
- [How to Use the MFD to Digitize It Right](#)