Establishing an Information Destruction Model

This guide sets out recommendations and considerations for establishing an information destruction model which supports accountability, access, privacy, and security requirements.

1.0   Information Destruction Model Best Practices

Ministries should determine the model which best meets the needs of their organization. Information Destruction Model best practices include:

- Clearly defined ministry responsibilities.
- Availability of learning materials to support staff training.
- Demonstrating a consistent, repeatable, appropriate, and documented standard to destroy government information, including necessary resources, tools, and forms.
- Formal approval of the information destruction model.
- Regularly reviewing the model to ensure adequacy and effectiveness over time.

2.0   Ministry Responsibilities

Responsibilities within a ministry may be combined, divided, and refined as necessary so long as all responsibilities are addressed.

Destruction Coordinator

- Provides oversight and administration of the model.
- Acts as a liaison with ministry IM employees to ensure consistency and collaboration across Information Management (IM) initiatives.
- Ensures necessary resources, tools, and forms are available.
- Defines, documents, and communicates ministry-specific training requirements.
- Ensures destruction control numbers are issued and documentation of approvals is maintained.
- Leads reviews on the model's effectiveness.

Approver

- Responsible for verifying the destruction is appropriate based on program area knowledge.
- Confirms records are not needed to meet operational or administrative requirements, related litigation, requests made under FOIPPA, or investigations that are underway or anticipated.
- Ensures records are only destroyed in accordance with approved information schedules.

Preparer

- Responsible for preparing adequate documentation pertaining to government information destruction based on knowledge of records management principles and practices.
- Liaises with Information Management Branch (IMB) or equivalent to coordinate destruction of ministry data.
- Ensures records are only destroyed in accordance with approved information schedules.

Systems/Applications

Product Owner

- Provides advice to application development project teams on database application design, packaging, delivery, and migration.
- Actions the destruction of the data and any related metadata, as appropriate
- Provides confirmation of destruction to the destruction coordinator and preparer.
- Product owners may be applications /systems roles within an Information Management Branch (or equivalent)

Data Custodian (Systems/Applications)

- Oversees the management of data in their program area throughout its lifecycle.
- Meets the requirements of the Data Management Policy and ensures information schedule retentions are applied.

3.0 Learning Materials - Information Destruction

Ministries should provide learning opportunities for staff to support their responsibilities.

The [Information Destruction Learning document (PDF)](#) identifies suggested training resources.

4.0 Information Destruction Documentation Standards

Ministries should define the documentation required for information destruction. These should include:

A) Information Destruction Logs
Ministries should create and manage a log for issuing and tracking destructions.

B) Information Destruction Number Naming Convention Standard
To ensure compatibility with existing data in the Enterprise Document and Records Management System (EDRMS) the recommended information destruction number naming convention standard is: DE-24-123-0001-CITZ

DEYY-	Two-digit fiscal year e.g. DE24-
###-	Three digit information destruction number e.g. 123-
BOX #-	Four digit numerical box code e.g. 0001-
MIN	Alphabetical divisional code e.g. CITZ

The overall length of the Information Destruction Number (IDA) should not exceed 15 characters. Note, if using EDRMS the ministry code is auto populated and cannot be updated. For ease of retrieval it is recommended IDA numbers are issued in a consistent format over time.

C) Information Destruction Request Classification
Information destruction authorizations should be maintained under the ARCS classification 432-30 Destruction Case Files – Authorized Internally. The file will provide evidence of defensible destruction and long-term reference for future accountability.

5.0   Document and Communicate the Model

It is recommended the ministry information destruction model be documented and made available to staff.

6.0   Regularly Review Model Effectiveness

To ensure relevancy, effectiveness, and efficiency over time, it is recommended ministries regularly review (e.g., annually) the model. Ministries may contact their Government Records Officer to request assistance with their information destruction model.