

## Completing an Information Destruction Request





It is important that ministries demonstrate that information existed but was legally destroyed through a documented process. Information to be destroyed must be covered by an approved information schedule.

### 1.0 Physical / digital information stored in a recordkeeping system

Destruction applications can cover government information in any format. This includes physical records such as paper files, audio visual records and photographs. Increasingly, records are held in digital formats such as data in line of business applications, e-records stored in EDRMS Content Manager and electronic records stored on network drives.

### 2.0 Destroying information under the Redundant Source Information Schedule (RSIS)

There are 4 categories of information covered by the RSIS, however only 2 categories require a destruction application to be completed:

RSIS Category	Description	Requires application for destruction?
1. Digital communications	This category includes messages moved from the location where they were created or received to an appropriate system. e.g. Outlook messages	
2. Encrypted records that have been decrypted	This category includes encrypted source records after they have been replaced by decrypted copies.	
3. Original source copies of migrated or converted system data	This category includes data and other information copied or moved from one hardware or software configuration to another, or from one file format to another	
4. Digitized physical information	Digitization is the process of copying physical records into digital form. (e.g., paper, magnetic media and microfilm)	

### 3.0 Destroying System Data

Ministries may destroy system data when it is eligible for destruction according to the relevant information schedule (see the System Overview section at the end of the relevant ORCS).

# Appropriate Information Destruction – Part 2

Examples of data destructions:

**Legacy system data - System decommissioning or upgrade:** Prepare an application for destruction each time a system is decommissioned or upgraded containing legacy data is decommissioned or upgraded.

**Routine data purges:** Simplify these requests for destruction by preparing a single destruction application to enable destruction on an ongoing basis.

## 4.0 Documenting and Tracking Destructions

The following table provides a list of the forms, documents, and tracking needs for each type of destruction application covered in this guide. Forms and a sample information destruction log can be found in the resources area of the [appropriate information destruction webpage](#).

Document/Process Listing	Physical / Digital Information stored in a recordkeeping system	Original source copies of migrated or converted system data	Digitized Physical Information	Legacy System Data / Routine Data Purges
Information Destruction Authorization (IDA) (ARS518)	✓	✓	✓	✓
Digitization Process Worksheet (ARS667)	✗	✗	✓	✗
Tobacco Litigation Form D Ministry of Health and Ministry of Finance Tobacco Tax Selection ONLY	✓	✓	✓	✓
File List	✓	✓	✓	✓
File completed destruction application packages in ARCS-432-20	✓	✓	✓	✓
Track applications in an information destruction log	✓	✓	✓	✓

## 5.0 EDRMS Content Manager – Systems Updates

Once your destruction application is complete and if it contains information being managed within the EDRMS system, please submit a request to [EDRMS.Help@gov.bc.ca](mailto:EDRMS.Help@gov.bc.ca) to update the system and delete and authorized government information.