RECORDED INFORMATION MANAGEMENT MANUAL

Government Records Service	RIM Number: RIM 501
Province of British Columbia	Approval Date: 2015/03/10

Policy: RECORDS DESTRUCTION

Specifications:
- RIM 501A Specifications for Destroying Records Onsite
- RIM 501B Specifications for Destroying Records in Offsite Records Storage Facilities
- RIM 501C Specifications for Contracted Records Disposal Services

AUTHORITY

From ***Core Policy and Procedures Manual*, 12.3.3 Part III (c):**

1. Government records must be disposed of securely in accordance with approved records retention and disposition schedules and asset management processes.
2. Ministries must establish internal records disposition procedures.
3. Government records scheduled for archival retention must be maintained in a manner that preserves their integrity and authenticity up to and throughout transfer to the government archives.
4. Government records scheduled for destruction must be destroyed in a method appropriate for the recording media and that maintains the security of the information and privacy of individuals.

Security Classification: PUBLIC

1. SCOPE

This policy establishes the responsibilities and requirements for appropriate, secure **destruction** of **government records** in all formats, in accordance with approved **records schedules**, and in a manner that ensures complete obliteration of information.

1.1 Authority

- *Document Disposal Act* (RSBC 1996, c. 99)
- *Core Policy and Procedures Manual (CPPM)*, c.12
- *Procurement Services Act* (RSBC 1996, c. 22)

1.2 Applicability

Ministries, agencies, boards, commissions, and Crown corporations covered by the *Document Disposal Act.*

2. POLICY

Destruction of government records must be managed, authorized and documented appropriately (i.e., in accordance with approved **records schedules**, this policy, and related specifications), and with due regard for existing access, confidentiality, and security provisions that apply to the records.

Government records are eligible for final disposition when their scheduled active and semi-active retention periods have expired, and they have reached the **final disposition** phase of the records **life cycle**. This phase needs to be established in an approved records schedule such as *Administrative Records Classification System* (***ARCS***), program-specific *Operational Records Classification Systems* (***ORCS***), government-wide **Special Schedules**, or another **ongoing** or **one-time records schedule**.

Disposition includes the destruction of records in all formats and media. Destruction actions must be authorized, carried out by authorized persons, and documented appropriately. To ensure this, ministry/agency destruction procedures must comply with policies and specifications established by Government Records Service (GRS). Whatever the format of the records and the methods used, destruction must ensure that information is completely obliterated and cannot be reconstituted.

2.1 Conditions for Records Destruction

Records destruction must only occur under the following conditions:

2.1.1. The records are covered by approved records schedules.

2.1.2. The records have a final disposition of "DE" (destruction) or, if they are scheduled as "SR" (**selective retention**), the records were not selected for archival transfer during the archival selection process (and the archival selection has been completed and an archivist has authorized this in accordance with DRAFT RIM 203A *Specifications for Archival Selection*).[1]

2.1.3. The records are not required for current or upcoming litigation, an access request under the *Freedom of Information and Protection of Privacy Act* (RSBC 1996, c. 165), or other ongoing requirements (i.e., there is no need to place a "hold" on destruction).

2.1.4. Destruction is conducted by an authorized employee or an authorized service provider (see 2.2 below).

2.1.5. Destruction is carried out in a secure, confidential manner that provides the same or stronger access protections required when records were active (e.g., do not use open office recycling bins for confidential or sensitive records).

[1] Records scheduled with any other designations cannot be destroyed. This includes records scheduled for Full Retention (FR) or OT (Outside Transfer, formerly known as OD "other disposition").

2.1.6. Destruction ensures the complete obliteration of the information contained in the records, and ensures the records cannot be subsequently reconstituted.[2]

2.1.7. Destruction documentation is produced and retained as required by government-wide specifications (see RIM 501A, 501B, and 501C) and office-specific procedures.

2.1.8. All destructions must comply with the specifications and related procedures.

2.2 Authorized Destruction Agents

Only persons or agents that have been authorized to carry out destruction may do so. Authorized agents may be employees of the ministry or agency or destruction service providers.

While all government employees are authorized to destroy certain categories of records (e.g., transitory records), under provisions of government-wide policy and ministry/agency procedures, authorization to destroy other categories of records may be limited to designated employees or service providers. Each ministry or agency needs to determine appropriate employee authorizations.

Destruction service providers include government agencies (e.g., the Asset Investment Recovery Branch provides Asset Disposal services) and non-government agencies that have a contract or corporate supply arrangement with government that specifies records destruction services (e.g., an approved records storage facility or an approved records disposal agency).

Destruction agents must follow the standards established in:

- RIM 501A *Specifications for Destroying Records Onsite*,
- RIM 501B *Specifications for Destroying Records in Offsite Storage Facilities*,
- RIM 501C *Specifications for Contracted Records Disposal Services*, and
- Office of the Chief Information Officer (OCIO) policy *Disposal of Information Storage Assets* (OCIO Information Security Branch Policy Summary No. 2, CIO-SPS-2010-000-V3).

[2] Ensuring that records cannot be reconstituted will vary according to the records format, the method of destruction, and other factors. For example, records shredded in high volume at a destruction facility have a lower risk of being reconstituted than records shredded in a home or office shredder. For this reason, RIM 501A *Specifications for Destroying Records Onsite* recommends smaller shred sizes for these.

2.3 Destroying Onsite Records

Only records eligible for destruction (DE) under approved schedules can be disposed of onsite.

The following records must **not** be disposed of onsite:

- Records that are scheduled for full or selective retention (FR or SR),
- Records that have not yet reached final disposition (still active or semi-active),
- Records required for current or upcoming litigation, requests under *FOIPPA*, or for other ongoing purposes, and
- Unscheduled records (i.e., there is no approved records schedule for the records).

Onsite destruction must be appropriately authorized. The authorization process requires **Records Officer** signoff using the appropriate form provided on the Records Management website.

Onsite destruction must comply in all respects with this policy (RIM 501) and with related specifications (RIM 501A *Specifications for Destroying Records Onsite*). The following options exist:

a) Destruction of onsite records may be carried out by office staff, by a contracted records disposal service (for paper records only), or by an authorized government agency (for records on digital storage devices or film).[3]

b) Contracted disposal service may take place in an authorized, secure vehicle at the office site (defined by Procurement Services as "onsite shredding") or a secure destruction facility (defined by Procurement Services as "offsite shredding"). Certain records may be designated as "onsite shredding only" due to security concerns.

Onsite **physical** records are maintained in a government office, rather than in offsite storage. When these records are eligible for destruction, the office is responsible for administering this process.

Onsite **digital records** are stored in a variety of environments and applications. When these records are eligible for destruction, it may be carried out within the office according to internal procedures (e.g., for records on a LAN/shared drive or a SharePoint site that the office manages) or it may need to be carried out with assistance from the service provider using application-specific procedures (e.g., for records managed in business application databases such as **EDRMS** TRIM or the Corporate Accounting System [CAS]).

[3] Destruction service for devices that store digital data (hard drives, cell phones, BlackBerrys, etc.) as well as for microfilm and other recordings on film is available from the Asset Investment Recovery Branch (see Secure Electronic Media Destruction).

2.4 Destroying Records in Offsite Storage

Inactive records in offsite storage must be disposed of and documented by the contracted facility staff under the following conditions:

- In accordance with authorization and specifications provided by GRS, as described in the RIM 501B *Specifications for Disposing of Records in Offsite Records Storage Facilities,*
- After GRS has notified relevant offices that records are eligible for disposition ("60 day notifications"), and
- After the ministry or agency has authorized removal of any "holds" that it has placed on records disposition (due to litigation or other requirements).

2.5 Contracting Records Destruction Services

Contracts for records destruction are executed in accordance with the *Procurement Services Act* and associated regulations and policies.

Contractors must be insured, and must provide and manage facilities and services that comply with RIM 501C *Specifications for Contracted Records Disposal Services* and/or RIM 423B *Specifications for Approved Offsite Records Storage Facilities*.

2.6 Disposing of Records on Digital Storage Devices

All digital media, microfilm, hard drives, and devices containing digital data (e.g., mobile devices such as smart phones and laptop computers, and removable storage devices such as memory sticks) must be destroyed in a manner that ensures the data cannot be reconstructed, when they reach the end of their useful life.

Follow government policy and use appropriate government services to ensure digital storage devices are properly destroyed (see section 2.2 above).

3. ROLES AND RESPONSIBILITIES

3.1. Government Records Service (GRS)

GRS is responsible for:

- Establishing destruction policy,
- Establishing government-wide standards and specifications for the physical destruction of government records,

- Establishing government-wide corporate supply arrangements, in collaboration with with Procurement Services (the government branch responsible for CSAs), in order to provide cost-effective records destruction services to ministries and agencies,
- Managing and authorizing the disposition process for inactive records in approved offsite records storage facilities, including notifications and administration of any disposition "holds" requested by ministries and agencies, and
- Assuming the costs of destroying eligible records stored in government-contracted storage facilities.

3.2. Ministries and Agencies

Ministries and agencies are responsible for ensuring that disposition of their records complies with government records schedules and this policy. This includes:

- Establishing internal records disposition procedures in compliance with policies, procedures and standards established by GRS,
- Ensuring that only records eligible for destruction under approved records schedules are identified as candidates for destruction,
- Ensuring that employees conducting or authorizing destruction are authorized to do so,
- Ensuring that records required for current or upcoming litigation, requests under *FOIPPA*, or other ongoing purposes are not destroyed,
- Arranging for the destruction of eligible records that are onsite (whether physical or digital) in a secure, confidential manner, and
- Using staff resources or GRS-approved contracted records destruction services.

Ministries and agencies are responsible for the costs of destroying onsite records.

3.3. Contracted Destruction Services

Contracted offsite records storage facilities and contracted records destruction services are responsible for destroying government records only when specifically authorized to do so, and for complying with the specifications associated with this policy.

RELATED POLICIES AND SPECIFICATIONS

The following specifications are founded upon this policy:

RIM 501A *Specifications for Destroying Records Onsite*
RIM 501B *Specifications for Destroying Records in Offsite Storage Facilities*
RIM 501C *Specifications for Contracted Records Disposal Services*

Also closely related to this policy are:

RIM 423 *Provision of Offsite Records Storage Services*

Draft RIM 203 *Archival Appraisal of Government Records*
Draft RIM 203A *Specifications for Archival Selection*

Relevant Office of the Chief Information Officer (OCIO) policy includes:

OCIO *Disposal Handbook: A Guide to Tangible and Intangible Asset Disposals in the Government of British Columbia* (see especially section 6.A *Recommended IT Asset Disposal Management Process*).

RELATED GUIDES – see RM Guides and Online Training Modules

Closing and Boxing Files Module 5 of Records Management Basics (*online training module*)

Revision History: First approved: 2015/03/10 Revised: n/a

This supersedes the following policies:

- 2-02 *Destruction of Government Records*
- 2-03 *Authority to Apply Records Schedules* (partially)
- 2-04 *Disposition of Government Records* (partially)
- IM/IT Supplement 2007 *(policy supplement to CPPM formerly posted by IM/IT Governance Branch of the Office of the Government CIO)*:
  12.3.3 III (a) ii. Final Disposition of Government Records

Index and Glossary Terms – see ***RIM Glossary*** for definitions of *terms that appear in bold blue text (for the first usage of each term in the policy, as well as below)*

ARCS	Holds on disposition	Records on digital storage devices
Contracts	**Inactive records**	**Records schedule**
Destruction of records	**Life cycle**	Records storage facility
Digital records	**One-time records schedule**	**Selective retention**
Final disposition	**Ongoing records schedule**	**Special schedule**
FOIPPA	***ORCS***	Unscheduled records
Government records	Records Officer	