RIM 501A SPECIFICATIONS FOR DESTROYING RECORDS ONSITE

Type of Records	Destruction Agent	Location	Specifications
1. All	Can include: • Employees (as authorized by records schedules and office procedures) • Authorized service provider	All (see RIM 501 *Records Destruction*, section 2.3)	The destruction process must: • Be applied only to records eligible under RIM 501 Section 2.1, • Be fully secure throughout (i.e., only accessible to authorized staff), • Ensure that the information contained in the records is completely obliterated and cannot be reconstituted, and • Be cost-effective and environmentally friendly.
2. Sensitive/ confidential records	May require special authorization under office or government-wide procedures.	May be restricted to destruction at office site rather than at the destruction facility	These include records identified as sensitive by either the ministry/agency or by government as a whole, for a variety of reasons (e.g., cabinet confidential records, personal information). The records may have "high" or "medium" security classification using the Information Security Classification Framework (see OCIO guidelines). For paper records that are sensitive, **do not use open office recycling bins**.
3. Digital records	Employee or authorized service provider (i.e., agency that manages the system where the records reside)	Server managed by office or service provider	**Delete digital records** stored online (e.g., in an email application, in a shared drive/LAN, on a SharePoint site or website, or in a digital system). Also delete any **extra copies** that may exist, except for copies filed elsewhere in the office recordkeeping system and routine computer backup files.
4. Storage devices for digital records	Best practice is to use the Secure Electronic Media Destruction service provided by the Asset Investment Recovery (AIR) branch.	AIR facility, Victoria	Use an industrial hard drive shredder[1] to destroy hard drives and other digital records storage devices (e.g., mobile devices such as smart phones and laptop computers, and portable storage devices such as memory sticks) when they reach the end of their useful life for the ministry or agency.

(*continued next page*)

[1] The only such shredder currently available in Western Canada is AIR's EDDIE (Evil Destroyer of Delicate Internal Electronics).

RIM 501A	SPECIFICATIONS FOR DESTROYING RECORDS ONSITE		
Type of Records	**Destruction Agent**	**Location**	**Specifications**

(*continued from previous page*)

5. Paper	Contracted records disposal service (as authorized under a supply arrangement)[2] *or* Employee	Authorized destruction facility *or* Office site	**Shred paper records** using a cross-cut shredder with one cut shredded to a width of 1 cm (3/8") or less and any length, and the other cut at 15 mm (5/8") or less, to ensure that the information they contain is obliterated. Using a **home or office shredder** increases the risk of records being reconstituted because the volume of shredded material is low. Therefore smaller shred sizes are recommended and **larger shred sizes are unacceptable**. After shredding, the resulting material may be **recycled or pulped**.
6. Film, microfilm, etc.	Best practice is to use the Secure Electronic Media Destruction service provided by the Asset Investment Recovery (AIR) branch.	AIR facility, Victoria	Shred anything stored on magnetic media or film, whether digital, analogue, audio, or audiovisual (e.g., microfilm, microfiche, VHS tape).
7. Records created and received by mobile workers	Employee (if authorized) or authorized service provider	As authorized by office	Best practice is for mobile workers to bring any paper records into the office for destruction, and to ensure all digital records are managed online using government servers and devices. Ministries and agencies may develop specific procedures that accord with relevant government-wide policy; for guidance see OCIO's Working Outside the Workplace Policy and GRS's RM Guide: Teleworking – Working Outside the Workplace.
8. Other			For records in any special media not covered above, seek advice from Government Records Service (GRS).

[2] Ministries are required to use the appropriate Corporate Supply Arrangement (CSA) for asset disposal. Broader public sector agencies are strongly recommended to use the CSA but not required to do so.