University of Victoria

GUIDELINES FOR THE SECURE DESTRUCTION AND DELETION OF UNIVERSITY RECORDS AND INFORMATION

Procedural Authority: University Secretary, Vice-President Finance & Operations
Procedural Officers: University Archivist and Chief Information Officer

Effective Date: November, 2014
Supersedes: July 2014
Last Editorial Change:

Parent Policies: Records Management Policy (IM7700)
Information Security Policy (IM7800)

PURPOSE

1.00 The purpose of these guidelines is to protect Records and information in the custody or under the control of the university from unauthorized use or disclosure by informing university employees of:

1.01 How to conduct the physical destruction of paper Records and electronic devices containing information that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction; and

1.02 How to conduct deletion of information in electronic form that is classified as Internal, Confidential or Highly-Confidential under the university Information Security Classification procedures, or designated in the Directory of Records as requiring confidential destruction.

DEFINITIONS

2.00 The definitions contained within the university's Records Management (IM7700) and Information Security (IM7800) policies apply to these procedures.

3.00 **Secure Destruction** means permanent physical destruction of paper records and electronic devices, rendering unreadable or unrecoverable the information they contain.

4.00 **Deletion** means removal of information from electronic devices and storage media.

4.01 **Routine Deletion** means removal or erasure of information from electronic devices and storage media by marking information as deleted. The information still exists, making data recovery possible unless the information is securely deleted or overwritten.

4.02 **Secure Deletion** means the process of deliberately, permanently, and irreversibly removing or erasing information from electronic devices and storage media.

5.00 Sanitization is a process to render access to target data (the data subject to the sanitization technique) on the device or media either effectively inaccessible (but potentially recoverable through data recovery techniques) or effectively irrecoverable. Deletion, erasure (deletion with overwriting), and destruction (physical destruction of the storage media) are actions that can be taken to sanitize media.

SCOPE

6.00 These guidelines apply to the following actions taken after the decision to dispose of Records and information consistent with Directory of Records (DOR) retention rules has been made:

6.01 The physical destruction of information, whether in paper, electronic, audio-visual or other format. This includes computers and other electronic devices and storage media (e.g. mobile phones); see section 16 below for further examples; and

6.02 The deletion of information in electronic form.

GUIDELINES

7.00 The method for Secure Destruction must be appropriate for the medium on which the information is stored.

Security Classification

8.00 Units are expected to refer to the security classification level of the information and Records prior to their destruction to assist in determining an appropriate destruction method. (See http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7800.pdf)

Authorization for Secure Destruction and Secure Deletion

9.00 Unit offices identified as Primary Offices for a particular Record series are responsible for obtaining authorization for Disposition from the University Archives prior to Secure Destruction or Secure Deletion in accordance with the university's Procedures for the Management of University Records (http://www.uvic.ca/universitysecretary/assets/docs/policies/IM7700.pdf and the Directory of Records. See

http://www.uvic.ca/library/locations/archives/records_management/resources.php for authorization forms.

9.01 Unit offices identified as Secondary Offices for a particular Record series may securely destroy or delete Records past their retention period without authorization from the University Archives.

Units are encouraged to consult the University Archives for specific guidance on Records Disposition, including Secure Destruction or Secure Deletion if they are not already familiar with the Disposition process.

Primary Office is an office or offices responsible for keeping the original and/or official versions of Records. Secondary Office is an office or offices which may hold duplicate copies of university Records that are to be maintained for shorter retention periods than original and/or official versions of Records.

Secure Destruction of Paper-Based Information

10.00 Records containing Highly-confidential, Confidential, and Internal information are to be shredded in a secure manner; Records containing public information may be recycled.

10.01 Records containing Highly-confidential information (see Information Security Procedures) should be shredded by a staff member of the Unit that holds the records, or on campus ("onsite") by an external supplier. Records containing Confidential or Internal information may be shredded off campus ("offsite") by an external supplier, or onsite by an external supplier or by a staff member of the Unit that holds the records.

Information Security Level	Highly-Confidential	Confidential	Internal	Public
Destruction, Paper Records	Onsite shredding	Offsite shredding (Onsite optional)	Offsite shredding (Onsite optional)	Recycle

11.00 Units should use the university's preferred external suppliers for shredding services. For supplier names, information on engaging them, and negotiated pricing, see http://www.uvic.ca/purchasing/faculty-staff/preferred-suppliers/index.php (requires NetLink logon).

11.01 If a Unit does not wish to use the preferred external suppliers for shredding services, the following conditions must be met:
- The external supplier must be NAID certified
- The service is selected in accordance with the Purchasing Services Policy (FM5105).

12.00 Units may consider the appropriateness of a Unit staff member supervising shredding by an external supplier, but this is not required.

13.00 Small quantities of paper Records may be shredded by individual Units. Contact Purchasing Services for recommended shredder models if necessary.

- If a Unit uses its own shredders, the Records must be shredded in a secure manner; secure methods include shredding into strips that are a maximum of one centimetre wide, cross-cut shredding, re-shredding or mixing shredded Records to ensure that information cannot be reconstructed.
- For Records with Confidential or Highly-confidential information, cross-cut shredding or re-shredding is recommended.
- If such Records are not cross-cut shredded or re-shredded, the shredded Records should be mixed to ensure information cannot be reconstituted.

If a staff member of a Unit is uncertain about the security classification of the information or Record, the staff member shall use the destruction method for the higher level. Contact the Records Management Archivist with questions.

14.00 Records awaiting Secure Destruction must be kept in a secure manner (i.e. locked cabinet, controlled access area, secure supplier's console, or sealed boxes in a locked room).

Electronic Device or Storage Media Sanitization

15.00 The approach for handling electronic devices and storage media after use is dependent on whether the devices or media are being repurposed for university use or are no longer required for use.

Deletion of Electronic Device or Storage Media Information

16.00 Electronic devices and storage media purchased with university funds or funds administered through the university, and that are repurposed for university use, must have information Sanitized prior to being repurposed.

16.01 Electronic devices and storage media that will be repurposed for university use that contain information classified as Public or Internal may be Sanitized by Routinely Deleting all data on the device in a manner that renders it effectively inaccessible.

16.02 Electronic devices and storage media that will be repurposed for university use that contain information classified as Confidential or Highly-confidential must be Sanitized using a method that erases data by overwriting the data multiple times, prior to being repurposed to another Unit or employee. Erasing overwrites all addressable locations with a character, its complement, then a random character, and verifies. If you require assistance, contact the Computer Help Desk to arrange for erasing of devices and storage media. http://www.uvic.ca/systems/services/contact/index.php

16.03 For best practices on Deletion and erasure, please see the "How To" section on the following University Systems service page: http://www.uvic.ca/systems/services/informationsecurity/diskencryption/index.php

Destruction of Electronic Devices or Storage Media

17.00 Electronic devices and storage media purchased with university funds or funds administered through the university, that are not repurposed for university use, must undergo secure physical destruction when no longer required by a Unit or employee, whether or not they are know to store Internal, Confidential, or Highly-confidential information.

17.01 Units must use the central secure physical destruction program provided by University Systems and Purchasing Services. Contact the Computer Help Desk to arrange for Secure Destruction of electronic devices and storage media. http://www.uvic.ca/systems/services/contact/index.php

17.02 Electronic devices and media requiring secure physical destruction include, but are not limited to: hard drives, flash media, USB keys, thumb drives, CDs, DVDs, floppy disks, computer tapes, audio and video storage devices, PDAs, Smart Phones and cell phones, and hard drives in all printers and copiers.

RELATED POLICIES AND DOCUMENTS

Protection of Privacy Policy (GV0235)
- Procedures for Responding to Privacy Incidents or Privacy Breach

Records Management Policy (IM7700)
- Procedures for Access to and Correction of Information
- Procedures for the Management of University Records

Information Security Policy (IM7800)
- University Information Security Classification Procedures
- Procedures for Responding to an Information Security Breach

RESPONSIBLE OFFICES

Information Security Office
University Archives