a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD U8
Destruction of UBC Electronic Information

1. Introduction

1.1 A large proportion of UBC Electronic Information is Medium, High or Very High Risk Information, such as student records, personnel records, financial data, and protected health or research information. If this information is not properly removed when no longer required and before the equipment is disposed of, unauthorized access may occur resulting in harm to an individual and/or the University.

1.2 This document defines standards for Users, including Information Stewards/Owners on the destruction and/or sanitization of UBC Electronic Information (data destruction).

1.3 The Chief Information Officer has issued this standard under the authority of Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems. Questions about this standard may be referred to information.security@ubc.ca.

2. Responsibilities of Users

2.1 Users should only retain information as long as needed or required by policy, legislation or agreement.

2.2 Users are responsible for ensuring that UBC Electronic Information is always removed from a Device before it is transferred to another individual, sold, discarded or taken with the User (with authorization from the Administrative Head of Unit) upon leaving the University. The information needs to be removed even if it does not appear to be Medium, High or Very High Risk. Users should contact University IT Support Staff or the IT Service Centre if they require data destruction assistance.

3. Responsibilities of Service Providers

3.1 Where a third party Service Provider has received copies of UBC Electronic Information for the purpose of UBC work, the Service Provider must destroy all of the information in its possession within seven days of the completion of the project or termination of the agreement, whichever first occurs. Destruction methods must be compliant with this standard and the Administrative Head of Unit must obtain signed confirmation of destruction in a format consistent with the Data Destruction Confirmation procedure.

3.2 Where data destruction is not feasible, Administrative Head of Unit may consult with UBC Cybersecurity to determine appropriate alternate controls.

3.3 This does not apply to collaborations with other research institutions for research purposes where a data retention agreement is in place.

4. Acceptable Data Destruction Methods

4.1 Any of the following are acceptable methods of data destruction:

4.1.1 using a software utility that erases by overwriting or encrypting the data;

4.1.2 magnetically erasing (degaussing) the data;

4.1.3 formatting a Device after encrypting it in compliance with the Encryption Requirements standard; or

4.1.4 using a machine that physically deforms or destroys the Device to prevent the data from being recovered.

4.2 Using the “Empty Recycle Bin/Trash”, “Delete”, “Remove”, and “Format” operating system commands do **not** destroy data and therefore are **not** acceptable methods for preparing media for transfer or disposal.

4.3 Data destruction methods must comply with the minimum standards set out in the IT Media Sanitization (ITSP.40.006) publication issued by the Government of Canada.

5. Special Cases

5.1 To destroy data on flash memory devices (e.g. SD memory cards, USB drives) containing UBC Electronic Information, the User can encrypt the whole device according to the Encryption Requirements standard. After encryption, the User can format the device and reuse it safely.

5.2 Data destruction on smartphones can be accomplished via a factory reset; note that some smartphones have removable memory cards that need to be treated the same as flash memory devices and securely sanitized separate from a phone factory reset. Users can contact their cellular service provider if they are uncertain of how to perform a factory reset.

5.3 Data destruction on IoT Devices can be accomplished via a factory reset; note that some IoT Devices have removable memory cards that need to be treated the same as flash memory devices and securely sanitized separate from a factory reset. Users can contact the device manufacturer if they are uncertain of how to perform a factory reset. Consideration must be given as to whether or not data stored off the device will still be required in the IoT ecosystem, e.g. with service providers. If the data is not required, it must also be destroyed.

5.4 Other imaging devices with a hard drive (e.g. photocopiers, printers, fax machines, etc.) are also subject to the data destruction requirements; additionally, where possible, these devices should have image overwriting enabled. This is a function where scanned or electronic images of a document are immediately overwritten using a data destruction technique. This function is known by various names, e.g. “Immediate Image Overwrite” (Xerox), “Hard Disk Drive Erase Feature” (Canon), “Hard Disk Overwrite Feature” (HP).

6. Related Documents and Resources

Policy SC14, Acceptable Use and Security of UBC Electronic Information and Systems

Data Destruction Confirmation form

Encryption Requirements standard

IT Media Sanitization (ITSP.40.006)