a place of mind
THE UNIVERSITY OF BRITISH COLUMBIA

INFORMATION SECURITY STANDARD #08
Destruction of UBC Electronic Information

Introduction

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.
2. This document defines standards for Users on the destruction and/or sanitization of UBC Electronic Information (data destruction).
3. The Chief Information Officer has issued this document 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.

Responsibilities of Users

4. Users should only retain information as long as required.
5. Users are responsible for ensuring that UBC Electronic Information is always removed from a Device before it is transferred to another individual, sold, or discarded. 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.

Responsibilities of Service Providers

6. 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, using destruction methods compliant with this standard and give the Administrative Head of Unit a signed confirmation of destruction in a format consistent with the Data Destruction Confirmation procedure.
7. Where data destruction is not feasible, Administrative Head of Unit may consult with UBC Information Security to determine appropriate alternate controls.

Acceptable Data Destruction Methods

8. Any of the following are acceptable methods of data destruction:
   a. using a software utility, such as "Secure Erase", that erases, overwrites or encrypts the data;
   b. magnetically erasing (degaussing) the data;
   c. formatting a Device after encrypting it; or
   d. using a machine that physically deforms or destroys the Device to prevent the data from being recovered.
9. 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.
10. Data destruction methods must comply with the minimum standards set out in the IT Media Sanitization (ITSP.40.006 v2) publication issued by the Government of Canada.
11. Wherever encryption is used before formatting a device, it must be AES-128/256 bit encryption with strong passwords or passphrases; it is recommended that this be supplemented with other data destruction methods whenever possible.

Special Cases

12. To reuse 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.
13. Smartphones must have all data removed (factory reset) prior to being transferred to another person or being turned in for recycling; 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.
14. 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).

Related Documents

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

Encryption Requirements standard

Data Destruction Confirmation form