BOSTON UNIVERSITY

Destruction of Paper Records and Non-Erasable Media (CD-ROMs, DVDs)

This document supplements the requirements of BU Data Protection Guideline 1.2.D - Data Protection Requirements. It provides information related to the proper disposal of sensitive information in such a way as to prevent its continued use.

Overview

There are legal, regulatory, contractual, and policy requirements may extend the duration for which information must be retained beyond its useful life. Before disposing of data please review the University Record Retention Policy (FA-002). DO NOT destroy paper or electronic records that the University Record Retention Policy (FA-002) requires be maintained. In addition, DO NOT destroy records if you have received a "litigation hold" notice from the Office of the General Counsel concerning actual or threatened litigation or if you have reason to believe that documents relate to a dispute that may result in litigation. If you have any questions, please contact BU Information Security or the Office of the General Counsel before you destroy either paper or electronic records.

Paper Records

Paper records are by far the easiest to be dealt with. Paper records containing only Public information should be recycled if possible, or otherwise disposed of appropriately.

Paper records containing Internal, Confidential, or Restricted Use information must be physically destroyed prior to recycling or disposal. While any shredder is sufficient for Internal or Confidential documents, Massachusetts law requires that paper records that contain Restricted Use Information must be burned, pulverized, or shredded so that personal data cannot practicably be read or reconstructed. Boston University recommends that use of a crosscut shredder for these documents. Once shredded, these documents should be recycled if possible, or otherwise disposed of appropriately.

Non-erasable Media (CD-ROMs, DVDs)

Some media is intended for a single use, such as CD-ROMs and DVDs. Once written, the information on these types of media cannot be easily removed. If a piece of media of this type contains Internal, Confidential, or Restricted Use information the media should be physically destroyed when it is no longer needed. Many paper shredders today support physical destruction of this type of media. If your department deals with Internal, Confidential, or Restricted Use information on this type of media, you should ensure that an appropriate mechanism for physically destroying the media exists. In some cases, data destruction services may be contracted to aid in destroying this kind of media.

Data Destruction Services

For offices that need to destroy large quantities of paper documentation, shredding individual documents may present a large burden. These departments should contract with approved data destruction companies that allow documents to be collected in locked bins on site and then are taken off-site for destruction. The preferred vendor at Boston University is Cintas Document Management.

Destruction of Individual Files on Reusable Media

This document supplements the requirements of BU Data Protection Guideline 1.2.D - Data Protection Requirements. It provides information related to the proper disposal of sensitive information in such a way as to prevent its continued use.

Overview

When data is no longer required it must be disposed of in a way that prevents its continued use. Electronic data can be difficult to dispose of effectively. Reusable storage devices are intended to have a long service life and may be erased and rewritten continuously during their life. Hard disk drives, USB storage devices, solid-state memory cards, portable disk drives, floppy diskettes, and data storage tapes are all examples of media intended for reuse.

There are legal, regulatory, contractual, and policy requirements may extend the duration for which information must be retained beyond its useful life. Before disposing of data please review the University Record Retention Policy (FA-002). DO NOT destroy paper or electronic records that the University Record Retention Policy (FA-002) requires be maintained. In addition, DO NOT destroy records if you have received a "litigation hold" notice from the Office of the General Counsel concerning actual or threatened litigation or if you have reason to believe that documents relate to a dispute that may result in litigation. If you have any questions, please contact BU Information Security or the Office of the General Counsel before you destroy either paper or electronic records.

Destroying Individual Files on Reusable Media

Public information may be disposed of using the standard delete function provided by your operating system. However, for most operating systems the delete function merely makes the data unavailable via the standard user interface but does not actually remove it from the storage device. Data deleted in this fashion can be recovered with commonly available tools. For this reason, extra steps must be taken to ensure that Internal, Confidential, or Restricted Use data is properly destroyed.

There are a wide variety of tools to accomplish this, some of which come with the operating system and some require additional installation. We recommend:

- For Windows, use a tool like Eraser:
  http://eraser.heidi.ie/
- For MacOS, use the built in "Secure Empty Trash":
  http://www.macworld.com/article/1166104/how_to_securely_delete_files.html
- For UNIX or Linux use GNU Shred, which is included with BU Linux as "shred" and Solaris as "gshred", use:
  http://www.gnu.org/software/coreutils/manual/html_node/shred-invocation.html

Securely Erasing Entire Reusable Storage Devices

This document supplements the requirements of BU Data Protection Guideline 1.2.D - Data Protection Requirements. It provides information related to the proper disposal of sensitive information in such a way as to prevent its continued use.

Overview

When data is no longer required it must be disposed of in a way that prevents its continued use. Electronic data can be difficult to dispose of effectively. Reusable storage devices are intended to have a long service life and may be erased and rewritten continuously during their life. Hard disk drives, USB storage devices, solid-state memory cards, portable disk drives, floppy diskettes, and data storage tapes are all examples of media intended for reuse.

There are legal, regulatory, contractual, and policy requirements may extend the duration for which information must be retained beyond its useful life. Before disposing of data please review the University Record Retention Policy (FA-002). DO NOT destroy paper or electronic records that the University Record Retention Policy (FA-002) requires be maintained. In addition, DO NOT destroy records if you have received a "litigation hold" notice from the Office of the General Counsel concerning actual or threatened litigation or if you have reason to believe that documents relate to a dispute that may result in litigation. If you have any questions, please contact BU Information Security or the Office of the General Counsel before you destroy either paper or electronic records.

Securely Erasing Entire Reusable Storage Devices (Disk Drives, USB devices, Tapes)

The delete function in most operating systems makes the data unavailable via the standard user interface but does not actually remove it from the storage device. To ensure that the data cannot be recovered, special tools must be used. These tools overwrite the storage device with random data. This form of securely erasing a storage device prior to disposal is a recommended practice for any storage device, even if it contained only Public information.

A reusable storage device *must* be securely erased when it contains *Internal*, *Confidential*, or *Restricted Use* Information and any of the following statements are true:

- It is being permanently taken out of service.
- It is being temporarily taken out of service and will be out of the custody of the Data Custodian or Data Trustee for any length of time.
- The disk will be classified and protected at a lower level than its current classification as defined by the Data Classification Guideline and Data Protection Requirements.
- The disk is being returned to a vendor for replacement under a hardware warranty or contract-support agreement, provided that physical destruction is not required by the following section.

For Intel and AMD hardware platforms we recommend a program called DBAN which will boot on any x86 based hardware and securely erase the disk:

http://www.dban.org/

For Sparc based hardware, we refer you to Sun's documentation for overwriting the entire disk:

http://www.sun.com/software/solaris/trustedsolaris/ts_tech_faq/faqs/purge.xml

BOSTON UNIVERSITY

Physically Destroying Reusable Storage Devices

This document supplements the requirements of BU Data Protection Guideline 1.2.D - Data Protection Requirements. It provides information related to the proper disposal of sensitive information in such a way as to prevent its continued use.

Overview

When data is no longer required it must be disposed of in a way that prevents its continued use. Electronic data can be difficult to dispose of effectively. Reusable storage devices are intended to have a long service life and may be erased and rewritten continuously during their life. Hard disk drives, USB storage devices, solid-state memory cards, portable disk drives, floppy diskettes, and data storage tapes are all examples of media intended for reuse.

There are legal, regulatory, contractual, and policy requirements may extend the duration for which information must be retained beyond its useful life. Before disposing of data please review the University Record Retention Policy (FA-002). DO NOT destroy paper or electronic records that the University Record Retention Policy (FA-002) requires be maintained. In addition, DO NOT destroy records if you have received a "litigation hold" notice from the Office of the General Counsel concerning actual or threatened litigation or if you have reason to believe that documents relate to a dispute that may result in litigation. If you have any questions, please contact BU Information Security or the Office of the General Counsel before you destroy either paper or electronic records.

When Physical Destruction of a Device is Required

In some cases, even securely erasing a disk does not provide adequate protection against unintended disclosure or loss of data. In these cases the device must be physically destroyed.

A reusable device must be physically destroyed when:

- It contains any Confidential or Restricted Use information and it is not possible to delete the data because the device hardware has failed.
- It contains any electronic Protected Health Information (ePHI) as defined in the Device and Media Control Policy (BU-100-003).

This means that for systems storing Confidential or Restricted Use information it is not possible to return the device to the hardware vendor for warranty or contract-based hardware support. This will likely incur an additional hardware cost to the department to support machines containing this information when such events occur.

It is important that these requirements are also made clear to individuals storing Confidential information on personally owned computers and devices. These devices are subject to the same terms, but replacement may be at the owner's expense. Restricted Use information may not be stored on personally owned computers and devices.

Proper physical destruction requires special tools and equipment. Information Services and Technology offers a Media Destruction service. Please see the following URL for more information:

http://www.bu.edu/tech/security/data-protection/media-destruction/