

Disposal of Digital Files and Media



The purpose of this policy is to establish the standards for the proper and secure disposal of media containing digital data. Disposal methods will be different depending upon the type of media and the intended disposition of the media.

Audience

Members of the University of Missouri – St. Louis.

Policy Statement

It is the policy of the University of Missouri – St. Louis Department Information Technology Services to securely wipe any digital media that will be redeployed or surplused so that it cannot be recovered by conventional methods. Digital media that will be disposed of must be securely wiped and/or destroyed so that it cannot be recovered by any means.

It is the responsibility of the data owner to protect digital University records per [BPM-911 Electronic Records Administration](#) before the media is presented for destruction, removal or redeployment.

Processes

Desktop/Laptop Computer Hard Drives Intended for Redistribution or Surplus

Redistribution

Hard drives NOT containing data covered by compliance such as PCI, GLBA or HIPAA must be reformatted and reimaged before being transferred from one employee to another employee. This may be done via imaging software such as Ghost.

Hard drives containing data covered by compliance areas must be wiped and then reimaged before being transferred from one employee to another employee. This may be accomplished by utilizing disk wiping software such as GDisk or DBAN that comply with the current US Department of Defense (DOD) standards for data sanitation and imaging software such as Ghost.

Surplus

All hard drives sent to University surplus must be wiped. This may be accomplished by utilizing disk wiping software such as GDisk or DBAN that comply with the current US Department of Defense (DOD) standards for data sanitation. There are procedures in place at Surplus to make sure that this happens.

Disposal

Hard drives that are going to be disposed of must be degaussed, physically destroyed or wiped to DOD standards.. Drives that contained data covered by compliance must be physically destroyed.

Server Hard Drives and Backup tapes

Server Hard Drives

Server hard drives must be securely wiped to DOD Standards or degaussed before they are surplus. Server hard drives containing data covered by compliance such as PCI, or HIPAA must be degaussed and physically destroyed. Exceptions can be made with written approval of the Information Security Officer.

Backup Tapes

Backup tapes cannot be surplus and must be disposed of in a secure manner. These tapes must be degaussed and/or physically destroyed.

Printers, Fax Machines, Copiers

Many of these devices contain hard drives or other types of media in them. They often store past data that has been copied or printed and pose a data security risk. It is the responsibility of the department to make sure that these devices do not have data on them when they are surplus. Please contact ITS if you need assistance.

Other Digital Media

All other digital media should be destroyed when it is no longer useful to the University. Just being erased is not good enough; it must be destroyed so that it is not recoverable by any means. If you do not want to destroy them yourself, you can send them to Information Technology Services to have them destroyed. ITS has a means to securely destroy all types of digital media.

Cell Phones, PDAs, and Digital Cameras – Securely erase internal memory (if possible) or by shredding.

Floppy Diskette – Physically destroy by breaking the case and cutting the disk inside or by shredding the disk.

Caseless Optical (CD/DVD) – Physically destroy by cutting into pieces or by shredding.

ZIP/Cartridge Media -- Physically destroy by breaking with hammers, drilling or shredding.

Solid State USB/Flash Drives, SD memory – Physically destroy by breaking with hammers, drilling or shredding.

Original Issue Date

January 2010

Revision Date