INFORMATION TECHNOLOGY PROCEDURE

DISPOSAL OF CONFIDENTIAL INFORMATION

BALL STATE UNIVERSITY INFORMATION SECURITY SERVICES

1. INTRODUCTION

Transferring or disposing of computers, storage media and paper documents improperly can result in inadvertent disclosure of confidential information, resulting in significant penalties to the responsible parties (Indiana law IC 24-4-14). In order to ensure compliance with these requirements the *Office of Information Security Services* (OISS), in consultation with the Director of Auditing and the Director Finance Legal Affairs, has established the following standards and procedures.

2. CONFIDENTIAL INFORMATION

With regard to this standard, Confidential Information includes all personal and financial information requiring protection from threats to its confidentiality and integrity as stated in the Gramm Leach Bliley Act (GLBA), the Family Educational Rights and Privacy Act (FERPA), other state and federal regulations, and other University policies.

3. APPLICABILITY OF THESE STANDARDS

These standards apply to all members of the university community when internally transferring computer hardware previously used to access confidential information; disposing of confidential information stored on computer or peripheral hard drives and media (i.e., CDs, DVDs, magnetic tapes, flash drives, and disks); or releasing computer equipment to third-parties such as recyclers or resellers. Security procedures prevent the unauthorized disclosure of confidential information and apply to these conditions:

a. Reassigning computers between employees or departments.
b. Disposing of inoperable computer hard drives.
c. Disposing of CDs, DVDs, magnetic tapes, flash drives, and disks used to store confidential information.
d. Transferring out-of-date computers for sale or release to third-party resellers.

4. REMOVING INFORMATION FROM COMPUTERS AND ERASABLE MEDIA

Useable computer hard drives and other read/write media (i.e., CD/RW, flash drives, floppy disks, and memory sticks) may be erased using approved methods which render the recovery of confidential information commercially infeasible. Standard file management utilities used to “reformat” or delete files from media are not sufficient methods to safeguard information from theft. Contact OISS for a current list of approved software tools to perform complete erasure or selectively erase files from hard drives, flash drives, and other related read/write media types. Selection of methods from the approved list and appropriate use of these tools remains the responsibility of the employee.

5. DISPOSING OF NON-FUNCTIONAL COMPUTERS AND HARD DRIVES

Departments must contact the Office of Inventory Control and Moving, which will accept custody of the equipment for proper disposal using the B-450 Move/Release form. Inventory Control and Moving will dispose of non-functional equipment in accordance with at least one of the following methods:

a. *Physical Destruction*: Physical force sufficient to crush, mangle, and destroy the internal drive platters is acceptable. Destroying the drive platters is necessary, since destroying only the drive electronics (the circuit board or connectors) leaves the confidential data exposed to unauthorized disclosure.

b. *Destruction by Certified Vendors:* During the warranty period, computer hard drive manufacturers frequently offer secure drive erasure services and many third-party vendors offer fee-based hard drive destruction services. A non-disclosure and indemnification agreement must exist between the vendor and Ball State University before transfer.

c. *Destruction by Magnetic Degaussing:* Degaussing machines erase magnetic storage devices (including hard drives) using a strong magnetic field, rendering all data unrecoverable.

6. Disposal of Non-Functional Removable Media

Prior to its disposal of non-functional CD/DVD, flash drives, magnetic tapes and other removable media out-of-date media or non-functional devices containing confidential information must be physically destroyed or made permanently unreadable:

a. *CD and DVD Media*: Destruction may be by using a device designed for CD/DVD destruction, or a paper shredder capable of handling this material. Other methods such as breaking apart by hand or cutting with office scissors should be avoided due to the danger of injury. Recycling the acrylic and plastics from shredded CDs and floppy disks is permissible provided the disks are first destroyed according to these procedures before transferred them to an outside party for recycling.

b. *Flash Drives, Magnetic Tapes, and Other Media*: If the device has a Ball State University inventory control tag, contact the Office of Inventory Control and Moving and follow the same procedures as for non-functional computer hard drives. For all other devices, contact OISS for disposal assistance. Do not discard in trash or attempt manual destruction.

7. Paper Document Destruction

Paper documents containing confidential information must be destroyed using shredders approved for high-security document destruction. Do not use "strip-cut" shredders which produce long and narrow ribbons of paper, as these can be reassembled with minimal effort. Instead, use only "cross-cut" or "particle-cut" shredders designed for the destruction of high-security documents. Contact OISS for equipment recommendations.

Departments routinely handling confidential information should consider instituting an office policy requiring all paper documents be shred before they are discarded. Although a single high-capacity shredder can serve an entire office, OISS recommends purchasing multiple "personal" shredders and placing them in close proximity to employee workstations.

Departments may also contract with an outside service for on-site shredding. Contact the Purchasing Office (285-1532) for more information about approved services.