Policy No: 808
Area: Information Technology Services
Adopted: 8/6/2012

Information Security Operational Procedures
Information Storage and Disposal Policy

PURPOSE

The purpose of this policy is to provide guidance that outlines the safe storage and disposal of information that, if compromised may be damaging to individuals or the University.

POLICY

HARDCOPY INFORMATION

STORAGE

Hardcopy information that is deemed confidential shall be stored in an area secured by lock and out of plain view. Access to that information shall be logged and limited to parties deemed appropriate by the Administrative Office "owning" the information (as described in the Electronic Communications Policy). Storage of confidential information shall be in a facility that is:

- Not readily accessible by window
- Has limited door access
- Is protected from environmental extremes

DISPOSAL

Hardcopy information that is deemed confidential may be destroyed in accordance with applicable state and federal document retention laws. Confidential documents must be shredded prior to disposal. Third parties may be contracted to dispose of documents, but an agent of CSU must witness the destruction of all documents.

DIGITAL INFORMATION

STORAGE

Digital information deemed confidential and "owned" by the University may not be stored on client machines, media, drives, or disks. Digital information noted above may be stored on approved University resources and secured using a controlled authentication mechanism. Each user provided access to those resources shall be given a unique account and all access attempts shall be logged. The University resource storing confidential information shall be regularly scanned for vulnerabilities, patched, and backed-up. Information stores will be segregated based on need.

DISPOSAL

Digital information may only be destroyed by the Division of Information Technology (IT) using a secure wipe program or hardware device. Applications that remove data to a degree meeting or surpassing DoD standards are required if a hardware DoD wipe device is not used. All surplus computers shall be cleaned using an approved mechanism. CD's, DVD, tapes, disk, etc. shall be destroyed prior to disposal. CD's and DVD's containing confidential information shall be shredded or broken in multiple pieces. USB keys and memory sticks shall be crushed prior to disposal.

CREDIT CARDS

Credit card numbers shall not be stored digitally or in hard copy on University resources. Any need to accept credit card transaction shall be approved by the CIO prior to accepting the card information. Credit card transactions using contracted resources shall be approved by the CIO to ensure that due care has been use in securing those transactions.

LOSS OF INFORMATION RESOURCES

The loss of control or custody of University information shall reported to the CIO immediately upon realization of the loss. The CIO shall be provided with detailed information including:

- Suspected time of loss
- Itemization of information lost
- Location of loss
- Details regarding loss