Information Asset Management Policy

1. **Overview**
    - **a.** The purpose for this policy is to establish a culture of security and trust for all faculty, staff, and students. An information asset management policy will benefit the University by ensuring compliance with FERPA regulations and protecting other information assets. All employees should familiarize themselves with the guidelines of this policy.
2. **Purpose**
    - **a.** The main reasons for an information asset management policy are:
        - i. To ensure information assets that should be protected are handled in an appropriate manner.
        - ii. It reduces the threat of a security incident as protected information will be locked away when unattended.
        - iii. Improperly handled assets can result in FERPA violations or compromise research conducted by instructors.
3. **Responsibility**
    - **a.** All faculty, staff, and entities working on behalf of Southern Illinois University Carbondale are subject to usage of this policy. Students are also encouraged to develop similar strategies.
4. **Scope**
    - **a.** To encourage familiarity and adherence to the Clean Desk Policy.
    - **b.** Both electronic and hard copy information assets that contain protected information or be of a sensitive nature that require controlled handling by authorized personnel.
5. **Action**
    - **a.** Keep assets (e.g. unfinished research, student papers, etc.) of similar nature grouped together in a secure location.
    - **b.** Comply with the Clean Desk Policy in order to ensure that assets of a protected nature or that falls under the purview of FERPA regulations are not accessible to unauthorized individuals.
    - **c.** Hard-copy information assets that are no longer necessary should be disposed of in a paper shredder, not thrown in a trash bin or recycle bin.
    - **d.** Electronic information assets that are no longer required should be securely deleted using a utility such as *Sdelete* for Windows or *shred* for Linux.
    - **e.** Storage medium that contains protected information assets should be stored in a secured location.
    - **f.** Storage medium used for backups that have reached their expiration date should be securely erased before put back into rotation for another backup cycle.
    - **g.** Storage medium not used for backup that will contain information assets of a protected nature should be registered and kept with either a particular piece of equipment or to a specific user/group.
    - **h.** When a storage medium is not longer usable or transferred to new ownership, it should be securely erased.

   i. When a storage medium is disposed of, it should be securely destroyed.
   j. Information Assets should be backed up to a separate location (e.g. a thumb drive, backup tape, etc.) and not to another location on the same device (e.g. a different folder on the same PC).

6. **Enforcement**
   a. Any employee found to have violated this policy may be subject to disciplinary action, in accordance with University policies and procedures.
7. **Definitions**
   a. FERPA – (Family Educational Rights and Privacy Act) Federal law that was established to protect student records, but is only applicable to school that receive Federal funding from the U.S. Department of Education. It essentially is a set of guidelines on what sort of information about students can be shared and with whom.
   b. Protected – Personal, confidential, or otherwise sensitive information in electronic format or hard copy that is exclusively for the use of the owner and authorized entities.
   c. Sdelete – A Windows based program that securely deletes a file by randomly writing 1's and 0's to a particular area on a storage medium in order to completely destroy all traces of a named file or folder. (http://technet.microsoft.com/en-us/sysinternals/bb897443.aspx)
   d. Shred – A Linux program that comes installed on most distributions that first overwrites a file with random data before deleting it.
8. **Revision History**
   a. Policy is in effect on 01/01/2011
   b. Document revised on 11/19/2010
      i. Revised by Brett Ussher