SM 1.16	**Date Written: 06/13/08**
Ver. 1.00	Date Approved: 10/05/09
Auth: TM	**Last update: 01/06/2010 10:30 AM**

SM 1.16 Data Disposal Policy

Principle:
Data must be disposed of in accordance with its data classification criticality value.

Objective:
To protect the confidentiality of information and mitigate the threat of unauthorized disclosure, while allowing the reuse of computer storage media or disposing of hardcopy (paper documents).

Policy:
Destruction of sensitive or confidential information captured on paper or computer storage media must only be performed with approved destruction methods including shredders or other industry standard processes.

Commentary:
This policy provides guidance on the approved methods for destroying sensitive information resident on hardcopy or computer storage media. The best destruction method is shredding or some other approach that renders the media unusable. Another technique is a degaussing method that uses electro-magnetic fields to erase data. Degaussing is not relevant to CD-ROMs, magnet-optical cartridges, and other storage media that do not use traditional magnetic recording approaches. Overwriting programs will write repeated sequences of ones and zeros over the information, reducing the chances that it can be recovered. Technical assistance may be needed because overwriting may or may not be acceptable for certain storage media. In system contexts with less pressing security needs, one of the less definitive destruction methods may be acceptable.

Procedure:
Hardcopy disposal:

- Shred using office shredder
- Shred using shredding service

Electronic media disposal (non-reusable)

- Old hard drives and USB keys should be sent to Ivy Tech Information Security Office (ISO) for disposal
    - ISO will erase drive and run multiple re-writes of 1's and 0's to render media unrecoverable
- CD/DVD shredded using CD/DVD shredder
- Back-up tapes should be incinerated

Electronic media disposal (reusable)

- Hard drives that are to be re-used should be re-formatted and overwritten using a software package (ex. Boot-nuke, Norton's SystemWorks, OnTrack's DataEraser, etc.)
    - Three overwrite minimum
- USB drives should be reformatted and wiped using a software package (ex. SecureClean, CCleaner, etc.). USB drives only need to be overwritten once.