Information Technology Standard for Data Sanitizing
Syracuse University – Information Technology and Services
Information Security Standard – S0104

1.0 Scope
This standard applies to all SU-owned computing equipment being prepared for transfer, disposition or sale. Primary responsibility is held by Information Technology and Services (ITS) support staff or the Distributed Support Person (DSP) of the college or business unit.

2.0 Purpose
Proper disposal of computing devices at Syracuse University is paramount to preserving the confidentiality and integrity of our digital data. We spend substantial time, effort, and resources to protect devices while in use. Similar care should be taken to ensure safe disposal of devices. SU sends many devices to excess property. These devices may contain information that must be kept confidential, such as application data, licensed software, licensing keys, passwords, and business emails. Data removal methods such as manual deletion of files or a full format of the device storage only does not prevent the use of forensic tools for data recovery.

3.0 Standard
All Syracuse University data must be permanently removed from computing and communication equipment prior to transfer, disposition, or sale of said equipment in order to maintain the confidentiality of sensitive information. The method used to fulfil this requirement is dependent on the device and storage type.

3.1 Hard Drives and Removable Media
KillDisk is used for sanitizing data on all hard drives and removable media. It is available for Windows, Linux, DOS, Macintosh (Intel architecture only), USB and most other removable media.

- Contact itsecurity@listserv.syr.edu for a copy of KillDisk.
- Select the Gutmann sanitization method.
- Follow the prompt to erase the disk and render recovery impossible.

3.2 Mobile Devices
For mobile devices, a simple manufacturer reset is not guaranteed to actually sanitize the device's memory completely. Therefore the recommended approach is to "cold reset the device" in which no

additional software is needed. Follow these steps to securely wipe mobile devices containing sensitive data:

1. Before performing factory reset, the device must be fully encrypted* to reduce risk of data recovery.
2. Thereafter mobile devices must have a factory reset* performed, removing all data including the encryption key.

*See phone manufacturer and/or OS information for detailed steps on encryption processes and factory reset.

4.0 Exceptions

For computing devices that will not boot and/or all internal storage is not immediately accessible by sanitizing software, the hard drives shall be rendered permanently inoperative via physical or magnetic destruction. The system unit shall be marked as containing a non-functional hard drive.

5.0 Referred Documents, Web Pages and Contact Information

Item	**Location/Info**
Contact: Information Security Officer	Christopher Croad ccroad@syr.edu

Document Info

Version:	1.0
Effective Date:	June 25th, 2014
Date of Last Review	June 25th, 2014
Date of Next Mandatory Review	June 25th, 2015