



## Sanitization of SULC Data From Information Technology Storage Media Policy Number 8-0010

|                                                                                   |                                         |
|-----------------------------------------------------------------------------------|-----------------------------------------|
| <b>Responsible Unit:</b><br>Information Technology                                | <b>Effective Date:</b><br>5/7/2007      |
| <b>Responsible Official:</b><br>Associate Vice Chancellor, Information Technology | <b>Last Reviewed Date:</b><br>7/15/2019 |
| <b>Policy Classification:</b><br>Information Technology                           | <b>Last Revised:</b><br>7/15/2019       |
|                                                                                   | <b>Origination Date:</b><br>5/20/2007   |

### 1.0 Rationale:

To provide guidance in the removal or wiping of SULC data from Information Technology equipment that is declared as surplus or damaged and considered non-repairable.

### 2.0 Policy Scope:

This policy applies to all SULC information technology equipment that stores SULC data and personal user devices that access SULC information technology resources and may store or have access to SULC data.

### 3.0 Policy Compliance:

Failure to with the policy will result in progressive disciplinary action up to and including termination.

### 4.0 Definitions:

**User** – SULC employees and students, contractors, vendors, and agents working under the auspices of the Law Center.

**Surplus** – Unneeded equipment is considered surplus equipment whether it is still functional or non-functional

### 5.0 Procedure:

#### **Servers Storage Devices - Workstations – Laptops – External Storage Devices**

All obsolete workstations, laptops, and servers will be brought to the SULC Information Technology Department prior to being submitted for disposal as surplus. Hard drives will be wiped utilizing DBAN or Degausser to ensure that sensitive data is completely unrecoverable. DBAN or Degausser utilizes a deletion process in which all spaces on the hard drive are overwritten with random characters. Three passes are made on the hard drive's spaces to ensure that the data is erased.

#### **Tape media**

Retired tape media will be collected by the SULC Information Technology Department and will be destroyed by physically shredding the tape media.

**Optical media**

Optical media, such as floppy disks and CD-ROM disks, will be collected by SULC Information Technology Department for destruction.

**Flash Drives**

Flash drives will be collected by desktop support staff and will be submitted to data sanitization utilizing DBAN or Degausser.

**Smartphones & Tablets**

Devices should be delivered to the SULC Information Technology Department where SULC data will be erased using appropriate software. If the device is owned by a user, the device will be returned after erasure of SULC data is complete.

**Important Note:**

Users should take care to ensure personal data is appropriately stored or backed-up before the SULC IT Department begins data sanitization processes. The SULC IT Department will not backup the user's personal data, nor will the SULC IT Department warrant that the user's personal data will not be erased during the sanitization process.

**6. Policy History and Review**

New policy was created 5/20/2007. Policy revised 7/15/2019. The policy is subject to a five-year policy review cycle and shall be reviewed by the Associate Vice Chancellor for Information Technology and any changes will be submitted to the Chancellor for approval.

**7. Publication of Policy**

This policy is published on the Southern University Law Center website at [www.sulc.edu](http://www.sulc.edu).

**8. Policy Approval**

This policy was approved by the Chancellor on 5/20/2007.

  
John K. Pierre  
Chancellor, Southern University Law Center

  
Date