

# Data Disposal and Reuse Policy

Current Version	Compliance Date	Approved Date
2.1	12/31/2018	11/13/2018

## 1. Purpose

---

To prevent disclosure of confidential information as a result of improper disposal or reuse of computer hardware and electronic media.

To prevent illegal distribution of licensed software as a result of improper disposal or reuse of computer hardware and electronic media.

## 2. Policy

---

### A. Removal of Data

When a University-owned or University-leased\* Information System (IS) or electronic medium has failed, is no longer needed, or will be used for a different purpose, the department that owns or leases the equipment must take steps to ensure that all University data is completely removed using a method that meets NIST SP800-88 Rev1 Standards for data destruction.

### B. Retirement or Decommission of Media

GreenSafe is a designated no cost procedure for OKC-based organizations of the OU Health Sciences Center to comply with NIST SP800-88 Rev1 Standards for data destruction. The department manager may also request approval from IT Security for data removal to be completed by the IS Administrator or an outside vendor and will require a Certificate of Destruction as evidence.

IT Security has identified device types that require a factory reset prior to destruction. The IS Owner and/or IS Administrator is responsible for ensuring devices are factor reset prior to destruction, in accordance with documented OUHSC Information Security Standards. IT Security will make the IS Owner and/or IS Administrator aware of this requirement during the Information Security Risk Assessment process.

\*For leased systems or media, contact IT Sales or the Purchasing Department to determine what actions are permitted by the University and what actions are required of the vendor to destroy stored University data before the systems or media are returned to the vendor.

### C. Repurpose or Reuse of Media

Electronic media may be repurposed or reused once the data has been completely removed using an authorized deletion method. An authorized deletion method produces a Certificate of Destruction that confirms secure deletion of data using a 7-pass wipe of data, in accordance with NIST SP800-88 Rev1 Standards.

### D. Logging Disposal or Destruction

Electronic media is considered to be ready for disposal or destruction if the device will not be reused or repurposed. Disposal of all University-owned or leased electronic media and information systems must be tracked and logged by the department manager or Tier 1/IT Representative. At a minimum, such tracking and logging must provide the following information:

- Date and time of disposal or destruction
- Who requested and who performed the disposal or destruction
- Brief description of media or information systems that was disposed of or destroyed, including model number, serial number, or inventory number if available

- Reason for disposal or destruction
- Approving manager's signature (IS Owner)
- Current Data Classification
- Completed Chain of Custody Form, as provided by IT Security
- Verification of data removal or destruction prior to disposal or destruction (see Record of Destruction form for details)

The OUHSC Service Desk must retain the Greensafe Certification of Destruction form, in accordance with the *OUHSC Records Retention Policy*.

A *Record of Destruction* form is available from the OUHSC Records Management and Storage Office for destruction of University data that does not include payment card data. Please contact 405-271-2311 to obtain a copy of the University data *Record of Destruction* form. Please contact 405-271-2433 for instructions on destroying payment card data.

#### E. Outside Vendors

If a department manager wishes to use an outside vendor to perform disposal or destruction services, the department manager must submit an Information Security Risk Assessment for the use of outside vendor services. Information Security, during the Information Security Risk Assessment, must confirm that the vendor is required by contract to comply with the requirements above, including to provide an OUHSC record of destruction for each piece of equipment, and that the vendor is contracted with the University through the Purchasing Department.

#### F. IS or Electronic Media Containing Protected Health Information (PHI)

If the IS or media contains Protected Health Information, the department manager must also comply with the requirements of the HIPAA, Device and Media Controls policy, in the destruction or disposal process of the IS or media.

#### G. Exceptions

Requests for exceptions to this policy must be submitted in writing to IT Security. IT Security will evaluate such requests and make a determination based on the risk to the IS or electronic media, to the data, and to the University.

#### H. Inventory Reconciliation

IS Owners or IS Administrators must update the device/equipment inventory form at a minimum, quarterly, to remove any devices that have been destroyed or disposed of.

### **3. Training**

---

IS Owners and/or IS Admins must undergo training at least annually, and more often as necessary.

### **4. Enforcement**

---

This policy is authorized and approved by the OUHSC Dean's Council and the Senior Vice President and Provost and enforced by the IT Chief Information Officer. Internal Audit may periodically assess Business Unit compliance with this policy and may report violations to the Board of Regents.

### **5. Scope**

---

This policy is applicable to all OUHSC Business Units that operate IS or electronic media.

### **6. Regulatory References**

---

- HIPAA 45 CFR 164.308(a)(1)(ii)(B) and 164.312(c)

- Section 501(b) of the Gramm-Leach-Bliley Act (“GLB Act”)
- FERPA: 34 CFR Part 99 [Family Educational Rights and Privacy Act]
- Payment Card Industry (PCI) Data Security Standard
- HITRUST 09.q Information Handling Procedures
- HITRUST 06.c Protection of Organizational Records

## 7. Review Frequency

---

This policy is scheduled to be reviewed, updated and modified annually and sooner, if necessary.

## 8. Revision, Approval, and Review

---

### 8.1 Revision History

Version	Date	Updates Made By	Updates Made
11/16/2005	1.0	OUHSC IT	Baseline Version
10/12/2015	1.1	OUHSC IT	Updated policy statements.
10/31/2016	2.0	OUHSC IT	Applied new template. Added roles and responsibilities.
03/26/2018	2.1	ISRB	Minor revisions.

### 8.2 Approval History

Version	Date	Approved By
1.0	11/16/2005	OUHSC Dean's Council
2.1	11/13/2018	Information Security Review Board

### 8.3 Review History

Date	Reviewed By
11/14/2014	OUHSC IT
10/31/2016	OUHSC IT
11/14/2016	Legal Counsel
02/22/2018	Randy Moore, Jill Raines, Chad Miller
03/05/2018	Subject Matter Experts