UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Hardware Repurposing and Decommissioning	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	POL-UMIT-A150-009-01
APPROVER:	David Ertel	VERSION:	2
	Interim Senior Vice President	EFFECTIVE:	March 1, 2017
	Business and Finance		

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the following framework has been identified to promote the best balance possible between information security and academic freedom.

I. PURPOSE:

To ensure adequate protection of protected data stored on University of Miami owned, leased, or personally owned hardware, this policy establishes requirements for the transfer, removal and disposal of all hardware housing such information.

II. SCOPE:

This policy applies to all hardware housing Protected Data (University owned, leased or personally owned). This policy also applies to employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties who have access to University resources.

III. POLICY:

All personnel must adhere to the minimum requirements outlined below to properly destroy data on any hardware that is transferred or loaned long term (outside the Unit the device is assigned), removed, repurposed, or decommissioned. Department management or appropriate staff members should contact assigned IT Support staff for guidance regarding handling of electronic devices. The requirements are as follows:

- When hardware is transferred, removed or repurposed, all configuration settings must be reset to factory default and all data must be properly sanitized adhering to government standards (DOD 5220.22-M).
- If hardware is decommissioned, all storage media must be made permanently unusable adhering to government standards (DOD 5220.22-M) by campus Information Technology department/division or designee as follows:

  - Hard drives and other electronic media (CDs, DVDs, Tapes, optical drives, solid state disks, etc.) must be degaussed and labeled or physically destroyed via shredding.
  - Other hardware such as routers, printers, handhelds, etc. must be reset to factory default.
  - Disposal of any electronic device and electronic media containing protected data shall be tracked and logged by the responsible system admin and/or custodians.
    - Tracking shall provide the following minimal information:
    - Date and time of disposal
    - Who performed the disposal
    - Description of media or information system that was disposed (i.e., Backup DLT tape, CDs, etc.)
    - If applicable:
      - UM Decal Number
      - Device model and serial numbers
- When a vendor services a device, any hardware requiring replacement must be reset to factory default and all data must be sanitized adhering to government standards (DOD 5220.22-M). The University should maintain possession of any hard drives for degaussing or physical destruction whenever possible.
- When personally owned hardware that has contained Protected Data is going to be sold, given away or abandoned, the user should adhere as closely to these policies as would be the case for University owned equipment. University IT personnel will be available to assist in those tasks.

IV. DEFINITIONS:

Hardware: Any electronic device (i.e. servers, workstations, electronic media, Blackberry ® devices and other cell phones with PDA capabilities, thumb drives, routers, firewalls, printers, copy machines, etc.) housing any Protected Data.

Hardware loan/transfer: Includes any instance where hardware is moved from one location to another and will service a different department or client. For example, if a workstation is moved from the IT department to the Treasury department or if a server previously used by IT is repurposed to service the Human Resources department.

Hardware Removal/Repurposing: Any time hardware is disconnected from the University of Miami data network and is left idle, waiting to be reused once again as a backup system, or spare parts, or is put back into production immediately to perform a different function/role.

Hardware Decommissioning: Any time hardware is disconnected from the University of Miami data network with the intention to surplus, sell, donate or discard.

Securely Erase/Sanitize Media (DOD 5220.22-M): The United States Department of Defense has identified standards for properly erasing media. The standard recommends the approach of overwriting all addressable media locations a minimum of three times, with a character, its complement, then a random character, and verifying the process.

Degaussing: The process of demagnetizing a storage media disk so that all data stored on the deProtected Data: Any data governed under Federal or State regulatory or compliance requirements such as HIPAA, FERPA, GLBA, PCI/DSS, Red Flag, and FISMA as well as data deemed critical to business and academic processes which, if compromised, may cause substantial harm and/or financial loss.

Protected Data: Any data governed under Federal or State regulatory or compliance requirements such as HIPAA, FERPA, GLBA, PCI/DSS, Red Flag, and FISMA as well as data deemed critical to business and academic processes which, if compromised, may cause substantial harm and/or financial loss.

- **HIPAA:** The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient's medical records.
- **FERPA:** The Family Educational Right and Privacy act of 1974 with the purpose of protecting the privacy of student education records.
- **FISMA:** The Federal Information Security Management act of 2002 recognizes the importance of information security to the economic and national security interests of the United States and as a result sets forth information security requirements that federal agencies and any other parties collaborating with such agencies must follow in an effort to effectively safeguard IT systems and the data they contain.
- **GLBA:** The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer's financial information.
- **PCI/DSS:** Payment and Credit Card Industry Data Security Standards is guidance developed by the major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments.
- **Red Flag:** A mandate developed by the Federal Trade Commission (FTC) requiring institutions to develop identity theft prevention programs.

System Administrator: An individual who performs network/system administration duties and/or technical support of network/systems that are accessed by other people, systems, or services. Only full-time and permanent part-time employees of the University and/or third party vendors approved by IT may function as system administrators.

Data Custodian: The person responsible for, or the person with administrative control over, granting access to an organization's documents or electronic files while protecting the data as defined by the organization's security policy or its standard IT practices. vice is permanently destroyed. Degaussing will render some media permanently unusable.

V. PROCEDURE:

System Administrators:

- Responsible for ensuring hardware under their auspices is maintained secured until data is properly destroyed adhering to government standards and this policy.

Campus IT Department/Division or designee:

- Responsible for the proper handling of hardware, depending on the scenario (loan, transfer, repurpose, removal, decommission) to ensure data is destroyed adhering to government standards and this policy.

Chief Information Security Office:

- Responsible for regular review of the Hardware Repurposing and Decommissioning policy. The review will occur annually or when significant changes occur.

Responsible Vice President or CIO:

- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

Sanctions:

- Knowing violations of the policy will be addressed by disciplinary policies and procedures applicable to the individual.
- All known and/or suspected violations must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable department.. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.
- Penalties may include:
    - Suspension or termination of access to computer and/or network resources;
    - Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
    - Suspension or termination of contract computer and/or network services; or
    - Criminal and/or civil prosecution.

Other Applicable Policies:

- Information Security Policy
- B043: Permanent Change of Equipment Location Within the University
- B044: Change in Use/Disposition of Equipment Purchased with Federal Funds
- B046: Redistribution of Excess Equipment to Other UM Departments
- B047: Sale, Disposition of Equipment
- B048: Equipment Donations & Transfers to Other Institutions
- B049: Equipment Deletion from University Assets
- HSP 13.1 – Policies and Procedures Disposal

Enforcement:

System Administrators:

- Responsible for ensuring hardware under their auspices is maintained secured until data is properly destroyed adhering to government standards and this policy.

Campus IT Department/Division or designee:

- Responsible for the proper handling of hardware, depending on the scenario (loan, transfer, repurpose, removal, decommission) to ensure data is destroyed adhering to government standards and this policy.

Chief Information Security Office:

- Responsible for regular review of the Hardware Repurposing and Decommissioning policy. The review will occur annually or when significant changes occur.