


| | | | |
|--|-----------------------------------|---|---|
| Name of Policy: <u>Disposal, servicing and transfer of IT equipment policy.</u> | |  Original Effective date: November 18, 2008 | |
| Policy Number: 3364-65-06 | | | |
| Approving Officer: President | | | |
| Responsible Agent: Vice President of Information Technology | | | |
| Scope: all University campuses | | | |
| <input checked="" type="checkbox"/> | New policy proposal | <input type="checkbox"/> | Minor/technical revision of existing policy |
| <input type="checkbox"/> | Major revision of existing policy | <input type="checkbox"/> | Reaffirmation of existing policy |

(A) Policy statement

Whenever a university organization relinquishes custody of information technology (IT) equipment or its components, whether to lend, donate, service or dispose of the equipment, the agency shall take reasonable measures as outlined in this policy to prevent the unauthorized release of information, unauthorized use of licensed software and intellectual property, and improper disposal of rechargeable batteries and other hazardous materials.

(B) Purpose

This policy is intended to mitigate risk with regard to university data, licensed software and intellectual property, and rechargeable batteries and other hazardous materials in the disposal, servicing or transfer of university information technology (IT) equipment.

(C) Scope

Compliance with this policy is mandatory for all university computing systems and end users.

The scope of this information technology policy includes university computer and telecommunications systems and the employees, contractors, temporary personnel and other agents of the university who use and administer such systems.

(D) Procedure

University organizations shall implement associated procedures in compliance with this university policy and shall ensure that employees, contractors, temporary personnel and other agents of the university adhere to those procedures.

Nothing in this policy prohibits the authorized transfer of information, licensed software and intellectual property stored on transferred IT equipment.

- (1) Risk Assessment: Prior to relinquishing custody of IT equipment, organizations shall conduct a risk assessment of the information stored on such equipment, in accordance with The University of Toledo “Information Security Framework.”
- (2) Short-Term Loan.
 - (a) To other university organizations. Prior to lending IT equipment within the university, university organizations shall secure information in a manner consistent with the findings of their risk assessment to prevent the unauthorized disclosure or use of contained information. If the equipment contains sensitive information, the organization shall either sanitize the equipment or encrypt the information commensurate with the risk-assessment findings.
 - (b) To organizations external to the university. Prior to lending IT equipment to organizations external to the university, university organizations shall sanitize equipment to prevent the unauthorized disclosure or use of contained information.
- (3) Servicing. Prior to servicing IT equipment where the device leaves the custody of the university, university organizations shall secure information in a manner consistent with the findings of their risk assessment to prevent the unauthorized disclosure or use of the information. If the equipment contains sensitive information, the organization shall either sanitize the equipment or encrypt the information commensurate with the risk-assessment. Securing, sanitizing, or encrypting is not required prior to servicing if the equipment is no longer capable of being secured, sanitized or encrypted. In such cases, removal of storage media such as hard disks that contained sensitive data may be appropriate, or it may be possible to sanitize the storage media in another similar and fully functional piece of IT equipment prior to releasing custody of the equipment to be serviced.
 - (a) University organizations may send IT equipment only to maintenance and repair service providers who have agreed in writing to:
 - (i) maintain the confidentiality of university information;
 - (ii) access information only if it is necessary for maintenance or servicing purposes; and
 - (iii) destroy, sanitize or return any equipment or components that are still capable of storing information, in accordance with university policy.
- (4) Disposal, long-term loan, university surplus or other permanent transfer. University organizations shall ensure that IT equipment is sanitized prior to either lending such equipment long-term or permanently transferring ownership, such as when donating equipment, transferring equipment to another organization, transferring equipment to the university surplus program, or disposing of such equipment.
 - (a) University organizations must at a minimum sanitize IT equipment and computer media that is to be permanently transferred by overwriting

information with meaningless data in such a way that information cannot be reasonably recovered.

- (b) For sensitive information, the sanitation procedures that university organizations use must provide additional assurance that information cannot be recovered. More rigorous methods, such as increasing the number of overwrites, degaussing, or physical destruction must be used as the levels of confidentiality and risk merit.
 - (c) Organizations may only send IT equipment to IT sanitation service providers who have agreed in writing to:
 - (i) maintain the confidentiality of university information;
 - (ii) access information only if it is necessary for sanitation purposes; and
 - (iii) sanitize any equipment or components capable of storing information in accordance with agency policy.
 - (d) The sanitation measures taken under this section shall be appropriate to reasonably prevent the violation of software license agreements prior to transferring IT equipment.
 - (e) University organizations shall dispose of IT property that contains hazardous materials in accordance with appropriate federal and state law.
 - (f) In the event that equipment capable of persistent data storage is transferred and sanitation methods such as data overwriting or degaussing are not technically feasible, organizations shall implement alternatives appropriate for the equipment to prevent the unauthorized disclosure of sensitive information or shall remove and destroy the storage media.
- (5) Sanitization methods. Sanitization of university IT equipment and storage media will be accomplished through the following methods.
- (a) Magnetic rigid disk (hard drives)
 - (i) Overwriting. Minimum requirement is a three-pass overwrite with all addressable locations overwritten with a character, then its complement, then all locations overwritten with random characters.
 - (ii) Degaussing using Type I, II, or III degausser.
 - (iii) Destruction.
 - (b) Magnetic tape
 - (i) Degaussing using Type I, II, or III degausser.
 - (ii) Destruction.
 - (c) Persistent memory devices

- (e.g. flash drives, USB memory, memory cards and solid-state hard drives)
- (i) Overwriting. Minimum requirement is a three-pass overwrite with all addressable locations overwritten with a character, then its complement, then all locations overwritten with random characters.
 - (ii) Destruction.
- (d) Optical (CD/DVD) and magnetic floppy disks should be destroyed to ensure information is unrecoverable.
- (6) Documentation. If performed by external vendors, the destruction, disposal, clearing and/or sanitization of university IT equipment will be documented to include:
- (i) Date of destruction/disposal/sanitization.
 - (ii) Method of destruction/disposal/sanitization.
 - (iii) Description of the destroyed/disposed/sanitized record series or medium.
 - (iv) A statement that the equipment was destroyed/disposed/sanitized.
 - (v) The signatures of the individuals supervising and witnessing the destruction, disposal, clearing and/or sanitization.

Documentation shall be retained by the organization with custodial responsibility of the device for a period of 1 year.

(E) Definitions:

- (1) Custody. In the context of this policy, the responsibility of control of a device through ownership, acceptance on loan, or a service agreement.
- (2) Data. Coded representation of quantities, objects and actions. The word, "data," is often used interchangeably with the word, "information," in common usage and in this policy.
- (3) Degaussing (i.e., demagnetizing). A procedure that reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. Properly applied, degaussing renders any previously stored data on magnetic media unreadable and may be used as a method of sanitization.
- (4) Destruction. Rendering IT-related property unusable and its data unrecoverable through shredding, incineration or other equivalent procedure.
- (5) Disposal. The final transfer of ownership or custody of an information technology device.
- (6) Donation. Transferring ownership and custody of IT-related property to another entity through a gift program, grant program, or their equivalent.

- (7) License. A contract that authorizes access to software and information and outlines rights regarding the use, distribution, performance, modification, or reproduction of software and information.
- (8) Licensed Software. Software in any form, whether commercial, proprietary, or gratuitous, that is provided by the intellectual property holder under terms of a contract that governs use, copying, modification and distribution.
- (9) Overwriting. Process of writing patterns of data on top of the data stored on a magnetic medium.
- (10) Ownership. The responsibilities of owning a device, which includes, but is not limited to, the data risks associated with devices capable of persistent data storage.
- (11) Persistent Data Storage. The ability of a device to store data that is recoverable beyond a complete power cycle.
- (12) Risk Assessment. A process for analyzing threats to and the vulnerabilities of information systems as well as determining the potential impact that the loss of information or system capabilities would have on the organization. Risk assessments provide a foundation for risk management planning and the attainment of optimal levels of security. See University of Toledo, "Information Security Framework," for assessment guidelines.
- (13) Sanitize. To expunge data from IT equipment so that data recovery is reasonably prohibitive. Sanitizing includes such measures as overwriting, degaussing and destruction.
- (14) Sensitive information. Include protected information including personal health information (PHI), personally identifiable information (PII) and student information protected under the Family Educational Rights and Privacy Act (FERPA) as well as nonpublic customer information, information about a pending criminal case, or infrastructure specifications. Information systems that must contain sensitive information will likely deploy techniques such as passwords, and could possibly include encryption.
- (15) Surplus. In the context of this policy, excess information technology property that university organizations send to surplus sale programs.
- (16) Trade-in. Transferring ownership and custody of an electronic device to a vendor through a procurement incentive program.

| | |
|--|--|
| <p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>November 18, 2008</u> Date</p> <p>Review/Revision Completed by: Vice President of Information Technology</p> | <p>Policies Superseded by This Policy:</p> <p>None</p> <p>Initial effective date: November 18, 2008</p> <p>Review/Revision Date: Next review date: November 18, 2011</p> |
|--|--|