3364-65-05 **Technology asset management policy.**

(A) Policy statement

The procurement, deployment, and disposal of technology must be conducted in a manner that serves the university's mission and its requirements for quality, cost reduction, durability, serviceability, safety, environmental protection, and security. Technology assets procured outside university approved channels may not be supported by information technology and may not be granted access to university resources.

(B) Purpose

This policy identifies requirements for the acquisition, handling, and disposal of all technology assets in a manner authorized by the vice president, chief information officer/chief technology officer "CIO/CTO" or designee. The intended result of this policy is to maintain consistently high standards of quality, durability, serviceability, and security of technology assets, efficient and effective of university operations, security and privacy of information, proper licensing and use of software and intellectual property, efficient and effective use of consumables and supplies, and the safe handling of hazardous materials in the acquisition, operation, disposal, servicing or transfer of university technology assets.

(C) Scope

This policy applies to the procurement and acquisition, operation, disposal, servicing, transfer, and disposal of all university technology assets by university agents and affiliates, including all university acquired, owned, or issued electronic hardware and software assets, such as desktop, laptop, and tablet computers and any computing systems purchased to be used as a server or network device, whether purchased by the university, procured through a grant, donated to the university.

(D) Definitions

(1) Technology asset. Technology assets are the hardware and software acquired by, owned by, controlled by, or in the custody of the university.

(2) Information technology asset. Information technology assets "IT assets" are the subset of technology assets that consist of computer

workstations and other general computing assets and their peripherals, university mobile computing devices, and network and storage infrastructure equipment used to carry out university business or to access, store, or transmit, or receive university data.

(3) Device. Device means any electronic computing technology asset with associated equipment, peripherals or storage media, regardless of ownership or control, such as a personal microsoft windows or apple mac os-based desktop, laptop, or tablet computer (personal computer) "pc", a personal mobile device such as a tablet, e-reader, or smartphone, or any other such equipment used for university business or to access, store, or transmit, or receive university data. Devices may be owned by the university, by an individual, or by a third party (such as home pc's and personally owned tablets or smartphones). In addition to the requirements established by this policy, devices are technology assets subject to the additional conditions specified in the "device and workstation policy".

(4) Sanitization. Sanitization refers to the process by which information is rendered reasonably unrecoverable or removed from a technology asset, such as by overwriting information with meaningless data.

(5) Sensitive data. Sensitive data is data for which the university has an obligation to maintain confidentiality, integrity, or availability.

> Appropriate use of data is to be used on the role you are serving the institution. User rights to this data should be role based when system functionality is applicable.

(6) Workstation. Workstations are the subset of devices acquired by, owned by, controlled by, or in the custody of the university, whether leased or purchased directly by the university, procured or issued through a grant, donated to the university, or provided to the university by private funding. In addition to the requirements established by this policy, workstations are technology assets subject to the additional conditions specified in the device and workstation policy.

Appropriate use of resources; use only those computing resources in manner that they were authorized or intended for.

(E) Policy

The information technology department coordinates the procurement of information technology assets through the university purchasing department. Other university organizations must obtain information technology approval for all information technology asset purchases. Purchases may be made from the pre-approved sources identified on information technology's computer equipment purchase website: (http://www.utoledo.edu/it/ns/computer_purchases.html.)

University organizational units must comply with the following general requirements in the acquisition, handling, and disposal of technology assets:

(1) Procurement management. The following requirements must be met for all acquisitions of technology assets:

(a) Information technology assets. Except as otherwise directed by the vice president, CIO/CTO or delegate, the selection, approval, procurement, coordination, and disposal of information technology assets for all university offices, departments, and colleges is the responsibility of university's information technology office.

(b) Other technology assets. The procurement of all other technology assets must follow all applicable academic, research, administration, and clinical policies and procedures.

(2) Maintenance contracts. All hardware and software purchases will include an appropriate maintenance or warranty agreement to cover the expected useful life of the asset. Additionally, computer systems may be taken out of service or replaced prematurely to prevent the continued maintenance of equipment that has been determined to be beyond its useful lifespan or unserviceable.

(3) Licensing. Where available, accompanying licensing for software, firmware, or other intellectual property components of a technology asset must be secured for as long as the asset is in use by the university. Except as agreed by the vice president, CIO/CTO and otherwise allowed by law, software licensed to the university may not be transferred to an outside entity.

(4) Disposition, custody and control of technology assets.

(a) The disposition, custody and control of university technology assets must be reasonably known until disposed of or permanently transferred outside the university.

The university information technology department maintains inventory data for information technology assets ensures that each procured asset is assigned to a university organizational unit. The disposition, custody, and control of technology assets procured by other university organizational units must be reasonably maintained by the procuring organizational unit.

(b) Risk assessment. Prior to relinquishing ownership, custody, or control of technology assets, university organizations must conduct an assessment of the information stored on such equipment to determine the relative risk of unwanted disclosure of sensitive data from improper disposal. If a reasonable risk of unwanted disclosure exists, the technology asset must be sanitized of the sensitive data prior to relinquishing custody of the asset.

(5) Servicing. Prior to servicing technology assets in situations where the asset leaves the custody of the university, university organizations shall secure information in a manner consistent with the nature of the data stored on the device to prevent the unauthorized disclosure or use of the data, up to and including temporary removal or permanent sanitization of the device or associated storage media.

Technology assets which access, store, process, transmit, or receive sensitive data may only be sent to maintenance and repair service providers who have agreed in writing to:

(a) Maintain the confidentiality of university information;

(b) Access information only if it is necessary for maintenance or servicing purposes; and

(c) Destroy, sanitize or return any equipment or components that are still capable of storing information, in accordance with university policy.

(6) Disposal and transfer of technology assets.

Except as directed by the vice president, CIO/CTO, university organizations must ensure that technology assets are sanitized of all sensitive data prior to a temporary or permanent transfer of ownership, custody, or control, such as by loan, sale, donation, transfer to another organization, transferring equipment to the university surplus program, or disposing of the asset.

(a) Short-term loans and transfers.

(i) To other university organizational units. Prior to lending technology assets among organizational units within the university, university organizations must secure the asset in a manner consistent with the nature of the information stored on the asset. If the asset contains sensitive information, the organization must either sanitize the asset or encrypt the information before transferring the asset.

(ii) To organizations external to the university. Prior to lending technology assets to organizations external to the university, university organizations must sanitize any sensitive data stored on the asset to prevent the unauthorized disclosure of information. Any software that by the terms of its license is limited to use by the university must be removed prior to transfer. Technology assets on short term loan to external organizations are university property and the custody and control of the asset

must be reasonably known until returned to the university.

(b) Long-term loans and transfers.

(i) To other university organizational units. Prior to long-term loan or reassignment of computing equipment among organizational units within the university, the asset must be wiped and restored to a default configuration by operating system reinstallation, restore procedure, or similar mechanism.

(ii) To organizations external to the university. Prior to the long-term loan, reassignment, or donation of computing equipment to organizations outside the university, the asset must be sanitized and must not contain any software licensed to the university.

(c) Disposal.

(i) University of Toledo "UT" disposal. If disposed of by the university, technology assets must be sanitized prior to disposal. The disposal of technology assets containing hazardous materials or other electronic waste must be conducted in accordance with all federal, state, and locals concerning the disposal of such waste.

(ii) Vendor disposal. Technology assets which access, store, process, transmit, or receive sensitive data may only be sent to sanitization, disposal or destruction service providers who have agreed in writing to:

(a) Maintain the confidentiality of university information;

(b) Destroy, sanitize or return any equipment or components that are still capable of storing information, in accordance with university

policy;

(c) Account for each asset to the point of sanitization or destruction and disposal; and

(d) Certify that it has disposed of the asset in accordance with the requirements of this policy.

(7) Sanitization. Sanitization of technology assets must be conducted in a manner that assures that sensitive information stored on the asset cannot be recovered, such as by physical destruction, shredding, or overwriting of stored data. For the purposes of this policy, destruction or deletion of an encryption key by university personnel such that data on an asset is rendered unrecoverable is sufficient to comply with the sanitization requirement.

(8) Violations. Violations of this policy will be subject to the university's disciplinary process and may result in disciplinary action up to and including termination. Criminal activity subject to applicable state and federal criminal penalties may be referred to law enforcement as appropriate.

Effective: 12/14/2020

CERTIFIED ELECTRONICALLY

Certification

12/02/2020

Date

Promulgated Under:	111.15
Statutory Authority:	3364
Rule Amplifies:	3364
Prior Effective Dates:	05/21/2018