Name of Policy: **Device and workstation policy** **Policy Number**: 3364-65-06 **Approving Officer**: President **Responsible Agent**: Vice President, CIO/CTO **Scope**: All University organizational units	**Effective Date:** January 12, 2017

☒	New policy proposal	☐	Minor/technical revision of existing policy
☐	Major revision of existing policy	☐	Reaffirmation of existing policy

(A) Policy Statement

All computing devices used on university's behalf must conform to standardized requirements to ensure the security, reliability, and stability of university resources.

(B) Purpose

To define devices and workstations, and to list their respective requirements and procedures in order for those workstations and devices to be granted access to university resources.

(C) Scope

Compliance with this policy is mandatory for all university agents, employees, students, and affiliates using any device or workstation on the university's behalf.

(D) Definitions

(1) 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 ("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).

(2) 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.

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

(E) Policy

(1) Device requirements.

All devices must meet the following requirements:

(a) Software and hardware updates.

Devices used to access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality must use operating system and application software that is eligible and configured to receive ongoing security updates from its vendor. Devices with unsupported or End-of-Life ("EOL") software may be denied access to the university network. Users with devices not owned or issued by the university may seek assistance from Information Technology for configuration if the intended use of the device is for university business.

(b) Device registration.

The university may require a device to be registered with the university's management tools prior to it being granted the ability to access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality. Access, storage, transmission or receipt of data for which the university has an obligation to maintain confidentiality confers consent to the university to manage the registered device, including enforcement of security

settings such as inactivity timeouts, personal identification number ("PIN") or password strength requirements, remote device tracking features, remote lock and device wipe features, and other security features available on the device.

Except for designated guest networks, all devices on the health science campus network must have the device's media access control ("MAC") address registered with the information technology department in order to access the university network. Any device without a registered "MAC" address may be removed from the health science campus network without notice.

(c) Anti-virus / Anti-malware protection.

To limit risk to university data from malicious software, all devices based on the Microsoft Windows operating system platform used to access, store, or transmit, or receive data for which the university has an obligation to maintain confidentiality must have an installed and operating anti-virus software with definitions not more than seven days old. Anti-virus protection is recommended but not required on other operating system platforms, such as Apple MacOS, Linux, or tablet/smartphone mobile device operating systems. Information technology provides guidance and limited support on anti-malware software for non-UT issued devices if the intended use of the device is for university business.

(d) Encryption of data at rest.

Strong encryption is required to render unusable, unreadable, or indecipherable the following categories of data while stored on devices or nonvolatile media:

(i) Medical and health information, including electronic protected health information ("ePHI"), as defined by the Health Insurance Portability and Accountability Act of 1996 and related regulations, "HIPAA").

(ii) Cardholder data (As defined by the Payment Card Industry Security Council's Data Security Standards, "PCI-DSS").

(iii) Certain personally identifiable information ("PII") when combined with an individual's name or date of birth, including:

(a) Government identification numbers such as Social Security Numbers ("SSNs"), passport numbers, state identity document numbers, or driver's license numbers;

(b) Banking or financial account numbers and related account data.

(iv) Any other data for which the university has an obligation or incentive to encrypt.

Encryption is highly recommended but not required for devices not purchased, owned, or issued by the university so long as the device does not store the above categories of data. The information technology department provides guidance and limited support on encryption software for non-UT issued devices if the intended use of the device is for university business. Exceptions for devices where no feasible encryption technology exists may be made on a case by case basis and may be subject to compensating controls established by the university CIO/CTO, information security officer ("ISO"), or designee.

(e) Physical security.

All devices must be reasonably secured against loss, theft, and inappropriate access. Devices which access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality must be physically situated in a manner that prevents viewing of confidential data by individuals who are not authorized to view the data. Unlocked devices may not be left unattended while authenticated to the university network.

(f) Operating system inactivity lockouts.

Devices used to access, store, or transmit, or receive data for which the university has an obligation to maintain confidentiality must have a reasonable and appropriate operating system inactivity lockout feature enabled.

(g) Network security.

All devices which access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality must be configured with a basic host firewall or reasonable substitute.

(h) Logging; consent to audit.

All devices which access, store, transmit, or receive ePHI or cardholder data must have available vendor default application and security logging enabled, and such devices must be made available to university administration for investigation, inspection, and audit upon request.

(i) Disposal.

When disposing of a device, the owner must make a reasonable effort to erase or remove all university of Toledo information from the device.

(j) Loss, theft, damage.

The University of Toledo is not responsible for damage, loss, or theft of devices not owned by the university. Lost or stolen devices with access to university information systems or containing data for which the university has an obligation to maintain confidentiality must be reported to University of Toledo information technology help desk as soon as practicable, by telephone at (419) 530-2400 or (419) 383-2400, or by e-mail at ithelpdesk@utoledo.edu.

(2) Workstation requirements.

In addition to the requirements for general devices set forth above, university workstations must also meet the following requirements:

(a) Workstation baseline image. To enhance the security and supportability of the university's computing infrastructure, standard device operating system and software images supplied by information technology are mandatory for initial deployments of all university-issued workstations. Workstations requiring a custom or nonstandard image are subject to review and approval by information technology, and are supported on a best-effort basis.

(b) Domain authentication. The university's active directory ("UTAD") domain is the foundation of the university's network security and network management capabilities. Except as directed by the vice president, CIO/CTO or designee, all university issued workstations that have the technical capability to authenticate to the UTAD domain must do so when present on the University's network.

(c) Anti-virus / anti-malware protection. Antivirus software is a fundamental component of network and workstation security. All university issued workstations must have an installed and operating antivirus software with definitions not more than three days old. Antivirus software is provided by Information Technology department for all university issued workstations in the standard workstation image.

(d) Encryption. All university workstations must use encryption technology to secure data at rest except as otherwise directed by the university's information security officer ("ISO").

(i) The workstation encryption mechanism standards are determined by the ISO based on a risk analysis;

(ii) Encryption algorithm and key length standards are determined by the ISO based on a risk analysis;

(iii) The ISO shall publish and update the workstation encryption standards as appropriate from time to time.

(e) Physical security. All university workstations must be reasonably secured against loss, theft, and inappropriate access. Devices which access, store, transmit, or receive any data for which the university has an obligation to maintain confidentiality must be physically situated in a manner that prevents viewing of confidential data by individuals who are not authorized to view the data. Portable workstations must be reasonably secured at all times and extra care must be taken to prevent loss or theft of the device. Lost, stolen, or damaged workstations must be reported to the information technology department as soon as possible.

(f) Workstation user authentication. Workstations used to access, store, or transmit, or receive data for which the University has an obligation to maintain confidentiality must have reasonable and appropriate workstation user authentication features enabled. The following controls may be enabled at the direction of the information security office:

(i) University workstations are configured to use the UTAD active directory login to authenticate a user to the workstation and to the university network.

(ii) University workstations in clinical environments and other appropriate areas are additionally configured with a single sign on technology determined by the ISO, based on a risk analysis.

(iii) Configuration and use of workstation automatic logon and logoff features are determined by the ISO based on a risk analysis, in consultation with the affected department.

(iv) Workstation screen saver activations and session idle timeouts are determined by the ISO, in

consultation with the affected college or department, and are based on a risk analysis.

(a) The default operating system idle timeout for all clinical workstations is five (5) minutes.

(b) The default operating system idle timeout for all other workstations used to access, store, transmit, or receive ePHI is fifteen (15) minutes, but may be extended upon college or department request and completion of a risk analysis by the information security office.

(c) The maximum operating system idle timeout for workstations used to process or transact in cardholder data is fifteen (15) minutes. Idle timeouts for workstations with access to cardholder data may not be extended beyond 15 minutes.

(d) The default operating system idle timeout for all other workstations used to access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality is twenty minutes unless otherwise arranged with the affected college or department.

(e) The default operating system idle timeout for all other workstations is one hour, but may be extended upon user request.

(f) Workstations that are not used to access, store, transmit, or receive data for which the university has an obligation to maintain confidentiality and workstations provided for public use may be configured with nonstandard idle timeouts, as appropriate. In some situations, compensating controls

may be required by the University Information Security Office to limit the risk of malicious activity.

(v) Configuration and use of workstation locking mechanisms is determined by the ISO, in consultation with the affected department, and is based on a risk analysis. By default, all clinical workstations require user authentication prior to deactivating an operating system screen saver.

(vi) The information security officer shall publish and update the workstation user authentication standards as appropriate from time to time.

(g) Local administrator access. University information technology must have the ability to gain local administrator access to all workstations regardless of operating system, and regardless of the ownership of the workstation. By default, users are not granted administrator access to workstations except as necessary. Users with a business need for elevated access to a specific workstation may submit an IT help desk request to be granted the appropriate level of access.

(h) Data backup. Users are responsible for maintaining accurate and secure backups of any data stored locally on workstations. The university does not back up individual workstations and is not responsible for the incidental loss of data stored on workstations. The university strongly recommends that a copy of such data be kept on server storage provided by Information Technology so that secure backups may be made without user action.

(i) Disposal. Disposal of university workstations must comply with all university workstation disposal and decommissioning policies and standards, including the university's technology asset management policy.

(3) Supported hardware and software.

(a) Supported hardware. Hardware vendors are evaluated and recommended by appropriate means for financial stability, research and development activities, strong quality assurance, advanced testing programs, and strong support from third-party suppliers, among other factors. For a list of vendors that are currently supported by the information technology department, contact the IT help desk. If a department chooses to purchase hardware from a vendor other than those supported by IT, the equipment may not be provided access to the university network.

(b) Supported software. Information technology has identified a list of supported software for workstations:

(i) Operating systems. Supported operating systems include current vendor-supported versions of Microsoft Windows, Apple Mac OS, Apple IOS, Android, and enterprise Linux distributions. Except in cases where paid vendor support is available, other operating systems are supported on a best effort basis, and access to university resources from assets using an unsupported operating system is not guaranteed.

(ii) Enterprise applications. Requests for new enterprise or clinical applications are reviewed via the procurement process. A list of currently supported enterprise applications is maintained by information technology.

(iii) Licensed software. Information technology maintains institutional licensing for a broad range of academic, business, clinical, and research related software. Software with limited licensing quantities or licensing purchased within departments may be restricted to functional areas, departments or individuals.

(4) Prohibited activities.

The following activities are prohibited:

(a) Destruction, alteration, damage, or unauthorized modification of workstation hardware without prior approval by information technology.

(b) Hosting of network services on devices attached to the university network (e.g., DHCP, wireless access points, routers, switches, etc.) without the prior review and approval by information technology.

(c) Circumvention of workstation security controls, including:

(i) Disabling anti-virus or other security software;

(ii) Disabling or circumventing workstation encryption software;

(iii) Disabling or modifying workstation idle timeouts and lockouts.

(d) Circumvention of network security controls, including:

(i) Internet protocol (“IP”) or MAC address manual assignment without prior review and approval by information technology;

(ii) Circumventing network firewalls, proxy servers, and intrusion detection and prevention devices; and

(iii) Unauthorized monitoring of the university network.

(e) Use of a workstation for illegal activity, including unauthorized “hacking”, “cracking” or intrusion of University or third party devices, systems, or networks.

(f) Storage, processing, transmission, receipt, or access to information for which the university has an obligation to maintain confidentiality on a device or workstation in violation of the requirements of this policy.

(5) Compliance and audit.

In the event of a security incident or alleged breach, the university has the authority to investigate and identify any data involved involving workstations, and to the extent possible, fulfill the university's obligations to mitigate the effects of the incident. Use of the university network constitutes consent to provide access to a device in this regard, including making the equipment available to audit and investigation by university personnel.

(6) 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. Minor violations will result in removal of the offending device from the university network at the discretion of information technology or administration. Criminal activity subject to applicable state and federal criminal penalties may be referred to law enforcement as appropriate.

Approved by: /s/ Dr. Sharon Gaber, PhD President January 12, 2017 Date Review/Revision Completed by: Senior Leadership Team Vice President, CIO/CTO	**Policies Superseded by This Policy:** • *3364-65-12 Workstation policy, effective date July 18, 2014* • *3364-65-15 Malicious Code security policy, effective date August 1, 2012* • **Initial effective date:** January 12, 2017 • **Review/Revision Date:** • **Next review date:** January 12, 2020