


Name of Policy: Workstation policy. Policy Number: 3364-65-12 Approving Officer: President Responsible Agent: Vice President of Information Technology Scope: all University of Toledo campuses		 Original effective date: January 29, 2009	
<input type="checkbox"/>	New policy proposal	<input type="checkbox"/>	Minor/technical revision of existing policy
X	Major revision of existing policy	<input type="checkbox"/>	Reaffirmation of existing policy

(A) Policy statement

All university owned workstations on the university's network must conform to standardized requirements to assure effective security, performance and support for the network.

(B) Purpose

To define workstations and list the associated requirements and procedures in order for those workstations to be permitted on the internal university network.

(C) Scope

Compliance with this policy is mandatory for all university owned information technology equipment permitted on the internal university network.

Information technology procurement activities will incorporate this policy and associated standards as system requirements in the procurement process.

(D) Definition

Workstations are user-based computing devices with an operating system capable of interacting with other systems on the university network. These include desktop computers (PC's), laptops, handhelds and any other network devices that a user can use to interact with other systems.

(E) Requirements

University information technology systems that are on the internal university network must follow the requirements listed below.

- (1) Workstation image. Information technology supplied workstation images will be used during initial configuration of all university owned workstations to enhance support and security of the university's computing infrastructure.

- (2) Domain authentication. The UTAD domain is an integral part of the security and management of the university network. All workstations that have the technical capability to authenticate to the UTAD domain must do so when on the network. UTAD domain authentication provides additional management tools needed to secure and protect the network.
 - (3) Antivirus. Antivirus software is a fundamental component of network and workstation security. All windows workstations must have installed and updated antivirus software. Antivirus software is provided by information technology for university owned workstations.
 - (4) Local admin access. Information technology must have the ability to gain local administrator access to all university owned workstations regardless of operating system.
 - (5) Registered MAC address. All workstations on the health science campus must have the MAC address registered with information technology to gain access to the university network. Any workstation without a registered MAC address may be removed from the network without notice.
 - (6) Physical security. All workstations must be secured against theft and inappropriate access. Systems which access PHI or other sensitive information must be located in a way that prevents viewing by individuals who should not have access to that information. Portable devices should be secured at all times and extra care must be taken to prevent loss or theft of the device.
 - (7) Encryption. All portable devices and workstations that have locally-stored sensitive data (PHI, SSNs, etc) must use encryption technology to secure data content. Encryption software is provided by information technology.
 - (8) Data Backup. Computer users and department management are responsible for maintaining accurate backups of any critical university data stored locally on workstations. Information technology strongly encourages that a copy of such data be stored on server-based storage that information technology backs up.
- (F) Supported hardware and software
- (1) 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. A list of vendors that are currently supported by information technology is available by visiting the information technology website or by calling the help desk at x2400.
 - (a) If a department chooses to purchase hardware from a vendor other than those supported, the chair/director will be required to sign an unsupported product affidavit before a purchase order will be issued.

- (2) Supported software. Information technology has identified a list of supported software for university owned workstations.
- (a) Operating systems. The current supported operating systems are Windows and Mac OS.
 - (b) Enterprise applications. Enterprise applications are those that impact many departments or functional areas.
 - (c) Licensed software. Information technology maintains institutional licensing for a broad range of clinical, business, academic and research related software. Software with limited licensing may be restricted to functional areas, departments or individuals and licensing purchased within departments.
- (G) Prohibited. The following actions are prohibited:
- (1) Disabling anti-virus or other security software implemented by IT
 - (2) Manually assigning IP addresses without prior consent and assignment by IT
 - (3) Spoofing MAC and/or IP addresses
 - (4) Making hardware changes to IT supported hardware
 - (5) Network monitoring
 - (6) Attacks to systems or network devices
 - (7) Storing unsecured sensitive data (i.e. PHI, SSN, etc.)
 - (8) Hosting network services (i.e. DHCP, wireless access points, routing, etc.)
- (H) Violations. Violations of this policy will be subject to the university's disciplinary process and will result in disciplinary action up to and including termination. Minor violations will result in removal of the network device from the network at the discretion of information technology. Criminal or legally non-compliant activity will be subject to applicable state and federal criminal code with appropriate law enforcement authorities notified as appropriate.
- (I) Exceptions. Exceptions are granted in extreme cases without alternatives and only when a significant clinical, academic/research or business need exists. These exceptions must be approved by information technology.

<p>Approved by:</p> <p><u>/s/ laj</u> Lloyd A. Jacobs, M.D. President</p> <p><u>January 29, 2009</u> Date</p> <p>Review/Revision Completed by: Vice President of Information Technology</p>	<p>Policies Superseded by This Policy:</p> <ul style="list-style-type: none">• <i>022 – Workstation Policy (former Health Science Campus Policy, effective 01/2005)</i>• <i>3360-70-05 – Supported Hardware and Software Policy (former Main Campus Policy, effective 09/2002)</i> <p>Initial effective date: January 29, 2009 Review/Revision Date: Next review date: January 29, 2012</p>
---	---