(A) Policy statement

All servers, systems and devices installed on the server network or in the datacenters must follow the approval and provisioning process which is facilitated through Network Services. Any system that does not follow this process will not be permitted to remain on the network. Additionally this policy outlines requirements for all servers located anywhere on the university network including those not housed in information technology’s data centers.

(B) Purpose

This policy establishes procedures for the installation of servers, systems, and devices on the server network and to ensure that all servers located anywhere on the university network are appropriately maintained and secured. The goal is to promote a supportable and sustainable environment and to prevent the addition of unauthorized systems which may interfere with any server or network.

(C) Scope

The scope of this policy includes all servers, systems, and devices installed on the server network or in the data centers, servers housed anywhere on the university network, and includes devices installed anywhere on the university's network(s) if they are found to interfere with network operations.

(D) Procedures for servers maintained by information technology.

(1) Server requests
   (a) All new requests will need to be submitted to information technology for approval.
   (b) Information technology will determine the appropriate hardware design, resource requirements, disaster recovery, and high availability requirements, feasibility, and estimated costs.
   (c) Requestor will decide whether to proceed with the installation.

(2) Server Implementation
(a) Server team will install the hardware and operating systems according to the server provisioning procedure.
(b) Hardware and OS will adhere to the minimum hardware and software specifications per information technology standards.
(c) Access to the server will be granted according to the Access Control Policy (3364-65-02)
(d) Server will be made available for use.

(E) Server Requirements

All servers that are on the internal university network, whether housed on the server network, in the data centers, or elsewhere on the network must follow the requirements listed below to the maximum extent possible within the constraints of the servers’ operating system.

(1) Domain authentication. The UTAD domain is an integral part of the security and management of the university network. All servers 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.

(2) Passwords. All system or root credentials and any associated application authentication credentials must comply with the university’s password security policy, 3364-65-07, and any default passwords must be changed from default settings.

(3) Antivirus. Antivirus software is a fundamental component of network and workstation security. All windows servers must have installed and updated antivirus software. Antivirus software is provided by information technology for university owned servers.

(4) Patching. All operating systems and associated applications will be patched and maintained in accordance with industry best practices.

(5) Local admin access. Information technology must have the ability to gain local administrator access to all university owned servers regardless of operating system.

(6) Registered MAC address. All servers on the health science campus must have the MAC address registered with information technology to gain access to the university network. Any server without a registered MAC address may be removed from the network without notice.

(7) Physical security. All servers must be secured against theft and inappropriate access.

(8) Encryption. All servers that are not housed and secured in information technology managed computer rooms that have locally-stored sensitive data (PHI, SSNs, etc.) must use encryption technology to secure data content. Encryption software is provided by information technology.

(9) Data Backup. Data backup for servers not housed in information technology computer rooms is the responsibility of the server owner. Information technology strongly encourages that a copy of such data be stored on server-based storage that information technology backs up. Back-up copies of any sensitive data (PHI,
SSNs, etc.) that is not protected within information technology computer rooms must be maintained in an encrypted format.

(F) Violations

If a server is found to be on the server network that did not go through the identified process or otherwise not in compliance with the requirements of this policy, the server will be disconnected from the network, reviewed, and appropriate actions will be taken. Please reference policy 3364-65-03 section B, periodic scans will be performed to ensure this policy is adhered to. Waiver authority for this policy is delegated to the Information Security Officer or designee.