Overview

This Addendum governs the management of computing devices within the UTHSC network that function as servers or as hosts.

Purpose

The purpose of this Addendum is to establish standards for the base configuration of internal host/server equipment. Effective implementation of this policy will minimize unauthorized access to University proprietary information and technology.

Scope

This Addendum applies to server equipment owned and/or operated by University personnel on any University owned internal network domain. The policy also applies to host device(s) and administration staff provided by and/or supported by third-party providers.

Definitions

Term	Definition
Open Zone or DMZ:	A network segment with a less restricted set of internet access rules than the corporate production network (also called DMZ).
Host:	A computer capable of accepting electronic dialogs with one or more users or other computers.
Server:	For purposes of this policy, a Server is defined as a computer providing services to multiple persons or other computers, internal to or external from the UTHSC backbone network. For the purpose of this policy it is assumed that servers are not used for day to day routine tasks of individuals, rather they are devices dedicated to providing a few services primarily to other computers.
Outbound Server:	A UTHSC server that will accept a connection request from a computer residing outside the University network.
Internet-Facing Server	An Outbound Server

Policy

Ownership and Responsibilities

1. All servers deployed at the University shall be maintained by an operational group that is responsible for system administration. Approved server configuration guides must be established and maintained by each operational group, based on business needs and approved by UTHSC SECURITY TEAM. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. Each operational group shall establish a process for changing the configuration guides, which includes review and approval by UTHSC SECURITY TEAM.

2. Servers shall be registered with Computing and Telecommunications. At a minimum, the following information is required to identify the point(s) of contact positively:
   - Server location
   - Server contact(s) and backup contact(s).
   - Hardware configuration, operating system, version, and patch level
   - Main functions and applications

3. Registration information shall be kept up-to-date.
4. Configuration changes for production servers must follow defined change management procedures.
5. Access to the equipment and to its system logs shall be granted to UTHSC SECURITY TEAM staff upon request. (**Risk/Vulnerability Assessment Addendum**)

Configuration Requirements and Guidelines

6. Operating System (OS) configuration shall be in accordance with approved UTHSC SECURITY TEAM guidelines.
7. OS services and applications that are not required for the server mission should be disabled.
8. Access to services should be logged and/or protected, if possible, through access-control methods such as SSH.
9. The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements. Operational groups shall have procedures in place for remaining current on all appropriate upgrades, patches, and hot fixes.
10. Since trust relationships between systems are a security risk, their use shall be avoided unless no other method of communication will suffice. If trust relationships are required, they must be documented and approved by UTHSC SECURITY TEAM.
11. Always use standard security principles of least required access to perform a function.
12. Do not use root when a non-privileged account will do.
13. If a methodology for secure channel connection is available (i.e., technically feasible and practical), privileged access must be (and other access preferably should be) performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
14. Host content updates shall take place over secure channel connections.
15. Servers shall be physically located in an access-controlled environment. Servers are specifically prohibited from operating in uncontrolled cubicle areas
16. For areas supporting mission critical information and/or applications, physical access shall be restricted to authorized personnel. Authorized visitors shall be supervised and their entry and exit shall be logged.

Monitoring

17. All security-related events on computing devices that store, process,access,or distributes (make available) mission critical or confidential information must be logged and have audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.

- Daily incremental tape backups of logs will be retained for at least 1 month.
- Weekly full tape backups of logs will be retained for at least 1 month.
- Monthly full backups of logs will be retained for a minimum of 2 years. [Reference **Mission Critical Information Addendum]**

18. Security-related events shall be reported to UTHSC SECURITY TEAM, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

<u>Compliance</u>

19. Assessments and audits will be performed on a regular basis by authorized organizations within the University.
20. Audits will be managed by the internal audit group or UTHSC SECURITY TEAM. The UTHSC SECURITY TEAM will filter findings not related to a specific operational group and then present the findings to the appropriate support staff for remediation and/or justification.
21. Every effort will be made to prevent audits from causing operational failures or disruptions.

Enforcement

Reference **Enforcement** in Acceptable Use document.

Additional Information

Any inquiries relating to this Host/Server Security Policy should be directed to the Security Director.