ADMINISTRATIVE PROCEDURE

ITP-TBD (previous ITP-42)

STANDARD FOR BASELINE SECURITY OF SERVERS

Number: ITP-TBD	Name: STANDARD FOR BASELINE SECURITY OF SERVERS
Purpose: Marshall University server administrators must take reasonable security measures to secure their hosts as outlined by this baseline standard. Ensuring proper computer security is a continual process. It is the frame of mind that there are real threats and part of a server administrator's job includes keeping users, data, and transactions safe from these threats.	
Responsible Unit: Information Technology	
Approved by:	Approval Date:

1. General Information

1.1. Scope: This standard applies to all computer system administrators managing a computer server providing any type of service to other users and connected to the Marshall University Network (MUNet). The following standards define common sense security practices expected of all computer server administrators.

1.2. Authority: Marshall University Chief Information Officer, as defined by ADMIN-20 Approval of Board of Governors Rules, University Policies and Administrative Procedures

1.3. Passage Date: April 18, 2014.

1.4. Effective Date: April 18, 2014.

1.5. Date Revised: August 19, 2019, and June 22, 2025.

2. Server Administration Ownership and Responsibilities

A server administrator, upon connecting their server to the Marshall University Network (MUNet), is responsible for the security of that device in accordance with the University Policy for General Administration Information Security Policy (UPGA-10) and applicable Information Technology Council (ITC) standard, procedures, and guidelines. A server administrator and their Department, Division or College will be held accountable when a data breach and/or system compromise occurs. It is also expected that the administrator will demonstrate reasonable precautions to ensure the security of their hosts. MUIT is available to consult with server administrators to ensure that the appropriate precautions and standards are in place.

3. Server Registration

All servers will be registered with the Marshall University Information Technology (MUIT). Campus Colleges, Departments and Business Units must use the ITP-42F Server Security Standard Registration Form to report any servers operating in their department. This registration form will collect important data elements about the general use, data stored, security and administrative contacts such as names and phone numbers of people to call in emergency situations including contact information during semester breaks.

Note: When security-related issues arise and this information is not available or inaccurate, there may be no choice other than to disconnect a server without notice. MUIT must be notified upon discovery of any system breach or suspected system breach. MUIT reserves the right to disconnect any server which poses a threat to the campus network. Any server not following the above procedures will be considered unsafe, and as such poses a threat to the campus network and other systems.

4. Baseline Security for Servers

4.1. Location

For servers located on campus, they should only be in physically secure areas and accessible by authorized personnel. For cloud servers, there should be logical controls that restrict public and administrative access to servers, such as VPN requirements, logical network segmentation, and multi-factor authentication for access.

4.2. Services Supported

Administrators should only run essential services on a server that are necessary for it to complete its designed task. Every service running should be regarded as a mode of entry. The number of entry points should be limited to only those needed. Note: The chance that a computer will be compromised is increased with the number of services being run. Therefore, it is expected that every administrator knows exactly which services they are running and why they are necessary. Administrators should nost host or process any restricted or confidential information on a server that also processes or hosts public information.

4.3. Security Updates

It is the sole responsibility of the Server Administrator to maintain the latest Operating System patches and security updates as they are released. At least a monthly cadence of updates and patches is recommended. It is also required that Administrators routinely review and update security system rules to ensure maximum protection of our network and of the data being stored.

4.4. Virus Protection

Server administrators are expected to install supported anti-virus software (where available) and regularly scan their servers to ensure system health.

4.5. Log-on Limits: Administrators should limit log-on retries

Password guessing applications have a greater probability of cracking a password if given a chance. For most situations, MUIT recommends account lockout after five failed log-on attempts.

4.6. Account Reviews

Accounts must be regularly reviewed for inactivity, and any dormant accounts disabled. Note: Old accounts should be terminated regularly. When people leave the University, administrators should have a clear deadline for account termination. Dormant accounts make attractive targets to intruders since no one will notice the activity.

4.7. Local Accounts

Whenever possible, accounts should be located on and authenticated against the MUNet ID system (Active Directory-based infrastructure) or Microsoft Entra (Cloud Based AD). Administrators should only use local accounts when necessary. Linux accounts that are not connected to Active Directory authentication should use a stronger form of authentication than just a password, such as SSH keys.

4.8. Privileged Accounts

Care should be taken with privileged accounts (including but not limited to "root" for Linux and "administrator" for Windows), commensurate with the privileges afforded by the account. Passwords for privileged accounts should be given only to people with a need for privileged access. For Windows Servers, the "administrator" account should be renamed. High-level privilege for servers (root on Linux or Administrator level access on Windows) should not be granted to standard user accounts but restricted to distinct administrative accounts or an account governed by a privileged identity management system. Non-Systems users that need elevated privileges should be granted the Power User role in Windows and only elevated to a full administrator when technically necessary.

4.9. Password Protection

All accounts must conform to the Marshall University Information Security Policy and applicable password standards.

4.10. Service Banners

Wherever feasible, a log-on banner, stating that the system is for authorized use only, should be displayed for anyone attempting to connect to the system. Note: If possible, log-on restrictions (by time of day, by system address, etc.) should be implemented. All operating system, version/release numbers, and vendor information provided in log-on/sign-on banners should be limited or disabled. Providing this information makes attacks easier by allowing intruders to pinpoint hosts with known security vulnerabilities.

4.11. Backups

It is the sole responsibility of server administrators to conduct regular backups to protect important data. Backup retention should be consistent with applicable data retention policies.

4.12. Server Logs

Logs of user activity must be retained for a period of six months to provide documentation of access. MUIT recommends that server logs be kept for six months where possible. Logs should include (where feasible) the time and date of activities, the user ID, commands (and command arguments) executed, ID of either the local terminal or remote computer initiating the connection, associated system job or process number, and error conditions (failed/rejected attempts, failures in consistency checks, etc.). Logs should be checked for signs of malicious activity on a regular basis. Knowledge that logs are kept acts as a deterrent to abuse. Logs are also essential in investigating incidents after the fact.

4.13. Restricted or Confidential Information

Servers containing restricted or confidential data are to be registered with MUIT and must be reviewed annually according to the guidelines established in ITP-1 and UPGA-10. Examples of restricted and private data can be found in UPGA-10. To maintain the security of restricted or confidential data stored on Marshall infrastructure, the University leverages Purview Data Loss Prevention (DLP) to identify and label restricted or confidential data. DLP will also enable the encryption of data at rest and data in transit. This would apply to several data types, such as, but not exclusive to HIPAA and FERPA data.

4.14. Remote Administration

Vendors or consultants who wish to gain access to a server from off campus should be assigned a MUNet ID and provided with VPN access. The system administrator is responsible for requesting the account and VPN access for the vendor or consultant. In addition, that vendor or consultant may be required to sign a non-disclosure agreement before gaining access to a server. Many servers require administration by outside vendors or consultants. In these cases, it is preferred that this outside access be obtained by using either a VPN connection or through a Remote Desktop Gateway access server. The account allows for secure remote access to the server. In the case of Windows servers, Remote Desktop Services should be used through the secure VPN connection to administer the server. UNIX, Linux, or Mac servers should use secure shell (SSH).

5. Incident Response

5.1. Response Procedure

A server administrator must read and understand the Marshall University Information Security Incident Response Procedure listed in UPGA-10 Information Security Policy.

5.2. Incident Confidentiality

Information regarding security incidents will be kept confidential by all parties involved. Only authorized personnel may disclose such information.

5.3. Compliance

MUIT the right to scan systems for known vulnerabilities. When vulnerabilities are discovered, they will be reported to the designated system administrator who will be expected to quickly act to close all known security vulnerabilities for which there are reasonable methods to close such vulnerabilities. If the administrator is unable to do this in a timely fashion, MUIT is authorized to disconnect any networked device which may negatively impact management, reliability, or integrity of the campus network.