Server Management Policy

1. POLICY STATEMENT

01.01 This policy statement promotes the appropriate management of institutional servers to achieve consistency, increase availability and security, facilitate disaster recovery, coordinate technical operations and apply sound Information Technology management practices consistently throughout the institution.

2. RELATED DOCUMENTS

a. Appropriate Use Policy
b. Server Management Policy
c. Information Security Policy
d. Server Management Standards and Procedures

3. DEFINITIONS

3.01 **Device Registry** – A database of LIT network devices maintained by Technology Services to assist with incident response and alerts. This registry includes information about the device such as device name, function, operating system, and primary and secondary contact information.

3.02 **Penetration Test** - A penetration test evaluates the security of a computer system or network by simulating an attack from a malicious source. The process involves an active analysis of the system for vulnerabilities that may result from poor or improper system configuration, known or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures. This analysis is carried out from the position of a potential attacker, and can involve active exploitation of security vulnerabilities. The intent of a penetration test is to determine the feasibility of an attack and the potential impact of a successful exploit, if discovered.

3.04 **Server** – a physical or virtual device that provides a specific type of service on behalf of another computer or computer user (i.e., a client). Examples include a file server that stores and manages access to files, a Web server that facilitates access to Web sites and pages, and a name server that maps user and computer names to machine and network addresses.

3.05 **Server Administrator** – an individual designated by the server owner as principally responsible for performing server management functions, including the installation, configuration, security, ongoing maintenance, and registration of the server.
3.06 Server Management – Functions associated with the oversight of server operations. These include controlling user access, establishing and maintaining security measures, monitoring server configuration and performance, and risk assessment and mitigation.

3.07 Server Owner – The department or unit supervisor charged with overall responsibility for the server asset in LIT’s inventory records.

3.08 Vulnerability Patch – An update provided by a vendor to correct a flaw or weakness in a component's design, implementation, or operation and management that could be exploited to violate the component's security or integrity. All software and hardware are subject to vulnerability and firmware patches.

3.09 Vulnerability Scan – A procedure that proactively identifies the vulnerabilities of a networked computing system to determine if and where that system is vulnerable to exploitation or threat. Vulnerability scanning employs software that seeks out security flaws based on a database of known flaws, tests the system for these flaws, and reports the findings to improve the security of the system and the network to which the system is connected.

4. GENERAL REQUIREMENTS

4.01 Before connecting to the LIT network, servers must comply with the General Requirements outlined in this policy, as well as all of the following:
   - Network Management Policy (specifically section 04 describing the requirements for devices connecting to the LIT network),
   - LIT’s Server Management Standards and Procedures,

   Contact the Technology Services Help Desk with questions about the guidance provided in these documents.

4.02 Technology Services maintains a device registry to facilitate compliance with security policies and procedures and assist in diagnosing, locating and mitigating security incidents on the LIT network. Server owners must register their servers in this registry and maintain the accuracy of their servers’ registry information. Technology Services will require the update of registry information in conjunction with the annual information security risk assessment process.

4.03 The server owner is responsible for the management, operation, and security of the server. At a minimum, the owner must assure the following:
   - the server is registered in the device registry described above,
   - physical and network access to the server is properly controlled, and
• the server’s operational configuration is maintained within the security and operational parameters described in this policy.

The owner may delegate specific server management responsibilities to a server administrator to achieve these objectives, but the server owner retains ultimate responsibility.

4.04 Before purchasing any equipment for use as a server, departments should contact Technology Services to explore alternatives for centrally hosting the desired services. If adequate resources do not already exist, Technology Services will assist the department in configuring a server adequate to address the requirements.

4.05 System owners and administrators shall adhere to the provisions of Section 04.10, Information Security Policy, when transferring, repurposing, destroying, or otherwise disposing of their server.

4.06 System administrators must subscribe to vendor notification and automated update services appropriate to the software hosted on their servers. System administrators may be required to subscribe to notification and update services (or equivalent) as those services become available.

4.07 It is not possible for this policy to address every specific issue that might arise regarding server management at LIT. Server owners and administrators are expected and encouraged to seek guidance from Technology Services as necessary to meet these responsibilities.

4.08 Exceptions to this policy require collaboration with Technology Services and express permission from the Director of Computer Services or a designee.

5. PROCEDURES FOR RESPONSE TO THREATS AND POLICY VIOLATIONS

5.01 Technology Services employs a variety of techniques and technologies, including regular network vulnerability scans and penetration tests, to identify potential risks to campus information resources and to monitor compliance with this policy. Technology Services will notify the registered server administrator of any protection deficiencies discovered in the course of these activities and recommend options for eliminating the deficiencies. If the deficiencies are not corrected or the server remains out of compliance for three or more calendar days following notification, Technology Services may disable the server’s connection to the LIT network until the deficiency is remedied.

5.02 Emergency circumstances: Technology Services will attempt to notify the server owner or administrator whenever it determines that a server has become an imminent threat to institutional information resources, such as when a server’s
integrity is compromised, when it places other network users at risk, or when its
defenses against compromise are seriously inadequate for the purpose it serves.
If Technology Services cannot contact the server administrator or the
administrator does not respond in a timely manner, Technology Services may
isolate the offending server from the network until the risk is mitigated. If the
threat results in the inappropriate disclosure of sensitive or confidential
information, Technology Services will initiate the incident management
procedures in Section 10 of the Information Security Policy.