Server Management Technical and Security Standards and Procedures

No server may be connected to the LIT Network unless and until it complies with the following minimum technical and security standards.

1. All servers that deliver services across the LIT network must be registered with Technology Services. Upon registration, Technology Services will facilitate an information resources risk assessment to ensure compliance with state and institutional standards and best practices. For registration and assessment details, contact the Technology Services Help Desk (TSHD) at (409) 839-2074 or helpdesk@lit.edu.

   The server owner/administrator shall repeat the risk assessment annually. The server owner/administrator must document a risk mitigation plan to address the risks identified by the risk assessment. If the risk assessment reveals the absence of any standard controls, the plan must document the risk management decision that justifies the absence of those controls and, if applicable, the compensating controls employed to provide the same or better protection.

2. Services that are not required for the server to meet its mission must be disabled whenever the server is connected to the LIT network.

3. The following services are prohibited and must be disabled whenever the server is connected to the university network:
   - Telnet
   - Anonymous File Transfer Protocol (FTP)
   - Domain Name Services (DNS). DNS is allowed only on Technology Services centrally administered DNS servers
   - Dynamic Host Configuration Protocol (DHCP). DHCP is allowed only on the Technology Services’ centrally administered DHCP servers
   - Simple Mail Transport Protocol (SMTP).

4. Prior to connecting the server to the LIT network the system administrator shall:
   - disable all default accounts except those required to provide necessary services
   - change the default passwords for all enabled accounts, consistent with LIT password standards (see section 08.06 of Information Security Policy)
   - terminate or disable all unnecessary user and support accounts
   - establish a minimal number of user accounts with administration privileges
   - apportion user accounts and/or groups to achieve proper separation of duties and to avoid the granting of excess privileges to any individual user or group
   - use the local administrator account only to perform server management functions
• register the server with Technology Services and establish server protections through the LIT’s network edge protection mechanisms (e.g., perimeter firewall, etc.).

5. The server must run an approved and appropriately licensed server operating system supported by Technology Services. Generally speaking, an approved server operating system is any version for which maintenance support and periodic updates are available from the vendor and/or another reputable third party.

6. The server must employ intrusion protection measures appropriate to its operating system, such as virus protection software, an independent intrusion protection appliance, Linux IP tables, and/or a host-based firewall. Anti-virus software is provided by the TSHD.

7. Vulnerability patches and updates must be applied regularly, normally within 72 hours of becoming available and vendor certified. If compliance with this standard will conflict with operation or support of any application(s) hosted on the server, the server administrator must contact Technology Services to identify alternative protective measures.

8. System administrators must subscribe to notification and/or automated update services appropriate to the server hardware and software. System administrators must subscribe to notification/update services (or equivalent) as those services become available.

9. Backups should be completed regularly based on a risk assessment of the data and services provided. Restoration of software and data from backups should be tested on a regular basis to assure viability in the event of a service disruption. If backup media contains sensitive or confidential data, the data on the backup media or the media itself must be encrypted. Depending on the level of risk, Technology Services may designate specific backup procedures.

10. The server must authenticate all users other than local administrators, using a centrally administered login service and identity management credentials (i.e., ID and password) if the operating system or application permits. All communication of authentication credentials between the authenticating client and server must be encrypted. Authentication credentials must always be encrypted while in transit from a client or when at rest on the server. The server must enforce institutional password standards (located in section 08.06 of Information Security Policy).

11. The server must capture and archive critical user, network, system, and security event logs to enable review of system data for forensic and recovery purposes. The system administrator must review these logs for signs of malicious activity on a regular basis. Such logs should be retained for a period sufficient to address business requirements, document changes to access permissions, and provide an adequate history of
transactions to satisfy audit requirements. Maintaining external copies of these logs is also recommended.

Based upon risk assessment, server logs should:
- provide the means for authorized personnel to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or result in the release of confidential information;
- maintain audit trails to establish accountability for updates to mission critical information, hardware and software, and automated security or access rules; and
- maintain a sufficiently complete history of transactions to permit an audit of the server by logging and tracing the activities of individuals through the system.

12. To the extent possible, the system administrator must configure the server operating system and/or resident applications to display a log-on banner to anyone requesting a connection to the server or application. The logon banner must meet the specification described in section 08.03 of Information Security Policy.

13. The server must not be used for multiple purposes that would put its security or performance at risk. For example a server must not be used as a personal workstation or to host multiple applications, such as a Web server and a database accessible from that Web server. Questions about incompatible uses should be addressed to the TSHD at (409) 839-2074 or helpdesk@lit.edu.

14. Physical access to the server and backup media must be restricted to persons with a legitimate need for such access.

15. The server must never be connected to any network other than the LIT Network.

16. Access to the server from outside of the LIT Network should not be provisioned unless absolutely necessary. If remote access is necessary, the following restrictions apply:
- Remote access sessions must be encrypted using SSH, VPN, or similar technologies
- Remote access should be provisioned to the fewest number of IP addresses possible (preferably only one)
- Host-based intrusion detection should be installed
- System and application logging should be enhanced

17. The server must not be administered remotely unless the remote access methodology has been specifically approved by Technology Services. At a minimum, information transmitted during remote administration sessions must be encrypted. The server should accept remote administration commands from the fewest number of predefined hosts. Vendor accounts used for this purpose must be inactive at all times except when the vendor is actively engaged in providing support services.