Server Security Policy

1.0 Purpose

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by Lawrence Technological University. Effective implementation of this policy will minimize unauthorized access to Lawrence Technological University’s proprietary information and technology.

2.0 Scope

This policy applies to server equipment owned and/or operated by the Lawrence Technological University, and to servers registered under any Lawrence Technological University internal network domain. This policy is specifically for equipment on the internal Lawrence Technological University network.

3.0 Policy Statement

All internal servers deployed at Lawrence Technological University must be owned and maintained by a department and/or operational group, which is responsible for all system administration. The EDCC staff of the Information Technology Services department is the responsible for all of the servers located in the EDCC Data Center. Before any department and/or operational group server can be added to the Lawrence Technological University network, it must be approved by the Executive Director of Information Technology Services. To make sure that University servers and their applications are secure from unauthorized access all system administrators must follow the below “Server Security Guidelines”.

3.1 Server Security Guidelines

- **Location**: Servers should be placed in physically secured areas accessible only to authorized personnel. There is no substitute for physical security.
- **Services Supported**: Administrators should run only services on a server that are needed 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.
- **Security Updates**: The latest system patches should be applied regularly.
- **Virus Protection**: It is expected that administrators regularly scan all servers with the most up-to-date anti-virus software that is the corporate standard.
- **Log-on Limits**: Administrators should limit log-on retries.
- **Account Reviews**: Accounts must be periodically reviewed for inactivity, and any dormant accounts disabled.
- **Local Accounts**: Whenever possible, accounts should be located on and authenticated against a Kerberos, NTLM, LDAP or Active Directory based infrastructure. Administrators should only use local accounts when absolutely necessary.
- **Privileged Accounts**: Special care should be taken with privileged accounts (including but not limited to “root” for UNIX and “administrator” for Windows), commensurate with the privileges afforded 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.

- **Password Protection**: All accounts must conform to the Lawrence Technology University Password Policy.

- **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.

- **Sensitive Information**: Lawrence Technology University Information Technology Services must be made aware of any server that contains sensitive data. This includes but is not limited to social security number, credit card numbers, grades and other personal data.

- **Remote Administration**: In order for a vendor or consultant to gain access to a server from off campus, they must be assigned a VPN account. The system administrator is responsible for registering the vendor or consultant before the VPN can be assigned. In addition, that vendor or consultant may be required to sign a non-disclosure agreement before gaining access to a server.

- **Change Control**: All changes to a server Operating System, application, configuration or hardware must go through the Change Control process.

### 3.2 Policy Implementation

Responsibility for implementing this policy rests with the Lawrence Technological University Information Technology Services.