

Little Cypress-Mauriceville CISD Server Management Plan

The Technology Department provides coordination, planning and support to aid in the effective use of District technology resources and information security technology for LCMCISD teachers, students, and staff. Our goal is to provide quality technology services that are efficient, reliable, and responsive to the needs of Little Cypress-Mauriceville CISD.

Technical and security standards for servers are developed by the Technology Department. Servers must comply with the general requirements before connecting to the LCMCISD network. Servers must be registered with the Technology Department to assure protection of District information resources.

Technology server administrators are responsible for the management, operation, and security of District servers. The Technology Department maintains an inventory to assure compliance with District security efforts and assists in diagnosing, locating, and mitigating security incidents on the District network. All server administrators must supply information such as: location, contact information, services required, need for firewall rules, etc. related to the server for inclusion in the registry.

The Technology department routinely scans the network to monitor compliance with policy. The technology department will notify Department Directors of deficiencies, including lack of inclusion in the inventory.

The server must run an approved and appropriately licensed server version of an operating system supported by LCMCISD Technology. Services which are deemed unnecessary or potentially disruptive must be disabled before connecting the server to the District network. Any services not utilized should also be disabled.

Prior to connecting the server to the network the system administrator must:

- Disable all default accounts except those required to provide necessary services
- Change the default passwords for all accounts which are enabled
- Terminate or disable all unnecessary user accounts including those for users no longer affiliated with the server
- Establish a limited number of user accounts with administration privileges. Limit files access categories for user accounts to prevent excess user privileges.

All servers must have virus protection software installed be configured to automatically apply updates as they become available. Anti-virus software can be requested by calling the Technology Help Desk at extension 2000. Vulnerability patches and updates must be applied regularly. Backups should be completed on a regular basis. If backup media contains sensitive or confidential data, encryption should be used. The server must capture and archive critical user, network, security, and system event logs for regular review by the Technology department. Physical access to the server and backup media should be restricted. If administered remotely, access should be limited from the fewest number of predefined hosts.