Collin College Technology Services (CC-TS)
Server Administration – Information Security Procedure (ISP):

PURPOSE:

The purpose of this ISP is to establish a framework to protect Collin College (CC) servers against unauthorized access, disclosure, modification or destruction and to assure the availability, integrity, authenticity, and confidentiality of information. A server is defined as a computer system dedicated to providing services, as a host, to serve the needs of the users of other computers on the network.

This ISP establishes standards for the base configuration of server equipment (physical or virtual devices), licensing, unnecessary services, default passwords, and disconnection/isolation of threatening servers that are owned and/or operated by CC.

SCOPE:

The CC Server Administration ISP applies to any servers that are owned or managed by CC.

STATEMENT:

All CC-owned or managed servers will comply with the requirements outlined in this and related CC Board policies, TAC§202 (Subchapter C) and other applicable state and federal guidelines and requirements.

1. Server configuration standards and procedures are established and maintained by the Manager Network Security and Support Services and approved by the Chief Information Security Officer (CISO).

2. All servers must be in physically secure locations and must be safeguarded in compliance with the IT Physical Access & Environmental ISP. Lab staff or designated employees are responsible for physically securing local lab servers if any. Servers are specifically prohibited from operating from uncontrolled cubicle and office areas.

3. Most servers that connect to the CC network must be installed, configured, and managed by the CC-TS Server Team. Some lab servers are supported and built by CC Campus Technology staff specifically for campus computer management but will still have oversight by CC-TS Server Team.

4. The CC-TS Teams must:

    a. Install and configure servers according to the Manager Network Security and Support Services' standard build documents and procedures, to include (but not limited to):

- Install an appropriately licensed server operating system and antivirus protection software.
- Disable all default accounts except those required to provide necessary services.
- Install the most recent operating system security patches as soon as practical according to Change Management ISP.
- Disable all services and applications that are not required for the server to meet its mission (e.g., Telnet, FTP, DNS, DHCP and SMTP on a file server).
- Include the use of standard security principles of least-required access to perform a function (e.g., do not use root access when a non- privileged account will do).

b. Install appropriately approved licensed software required by the Data Owner. The CC-TS Application Administrator normally handles software installations.

    - Disable all application default accounts except those required to provide necessary services.
    - Change the application default passwords for all enabled accounts to one consistent with CC User Accounts Password ISP.

c. If a methodology for secure channel connection is necessary ore required by law, privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).

d. Servers must have the necessary vulnerability scans performed before providing service to the campus or internet. Any serious vulnerability must be corrected before being placed into production.

e. Those servers that house confidential College data, or that provide access to it, may be required to meet additional requirements as defined by the appropriate Data Owner.

f. An CC device registry is maintained by CC-TS to facilitate compliance with security policies, ISP's and procedures and assist in diagnosing, locating and mitigating security incidents on the College network.

    - Servers that attach to the CC network must be registered by CC-TS and approved by the CISO.
    - Registration must include contact(s) and location, hardware and operating system/version, main function(s) of the server, associated applications, and demonstrated compliance with the required CC ISP's, TAC§202 (Subchapter C) and other state and federal requirements.

- The CISO will require the update of registry information in conjunction with the annual information security risk assessment process.

5. Application Administrators must:

    a. Enforce the application's usage policies, implement the application-specified access controls, and configure and maintain the server's application according to the required standards.
    b. Include the use of standard security principles of least-required access to perform a function (e.g., do not grant an administrative account access to the application when a non-privileged account will do).

6. Backups should be completed regularly based on a risk assessment of the data and services provided and must comply with the Backup Recovery ISP.

7. CC-TS Security or Server Management Team will disconnect a server or remove files posing an immediate threat to the CC network in order to isolate the intrusion or problem and minimize risks.

    a. This can be done without contacting the owner or application administrator if circumstances warrant.
    b. The server will remain disconnected until it is brought back into compliance or is no longer a threat to the CC network.

8. CC cooperates fully with federal, state, and local law enforcement authorities in the conduct of criminal investigations and will file criminal complaints against users who access or utilize the CC network to conduct a criminal act.

    a. In accordance with the CC Security Incident Response Plan, incident response best practices must be followed to assure appropriate preservation and treatment of forensic data.
    b. All logs and audit trails pertaining to security-related events on critical or sensitive systems will be managed according to the CC Incident Response Plan.
    c. The CISO will:

        - Perform periodic reviews to ensure compliance with this ISP.
        - Notify the Vulnerability and Risk Management Committee of identified concerns and risks.

9. Exceptions to the Server Administration ISP must be submitted in writing and approved by the CISO. Requests shall be justified, documented, and communicated as part of the risk assessment process.

Related Policies, References and Attachments:
An index of approved CC-TS ISP's can be found on the CC Information Technology Services ISP website at https://www.collin.edu/security/.