**Clarendon College**
**Information Technology Services (CLARENDON COLLEGE-IT)**
**Server Administration Policy:**

**PURPOSE:**
This policy establishes the framework to protect Clarendon College servers against unauthorized access, disclosure, modification, or destruction and to assure information availability, integrity, authenticity, and confidentiality. A server is a computer system dedicated to providing services, as a host, to serve the needs of the users of other computers on the network.

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

**SCOPE:**
The Clarendon College Server Administration policy applies to any servers owned or managed by Clarendon College.

**POLICY STATEMENT:**
All Clarendon College-owned or managed servers will comply with the requirements outlined in this and related Clarendon College policies, TAC§202 (Subchapter C), and other state and federal guidelines and requirements.

1. Server configuration standards and procedures are established and maintained by the Vice President of Information Technology or any company acting on behalf of the Clarendon College IT and approved by the Information Security Officer (ISO).
2. The Information Resources Manager (IRM) is ultimately responsible for managing Clarendon College's information technology resources.
3. All servers must be physically secure and safeguarded in compliance with the IT Physical Access & Environmental Policy. Servers are expressly prohibited from operating from uncontrolled cubicles and office areas.
4. Access control logs will be posted outside all server or network control rooms.
5. All servers that connect to the Clarendon College network must be installed, configured, and managed by the Clarendon College IT.
6. The Clarendon College-IT must:
    a. Install and configure servers according to the Vice President of Information Technology's standard build documents and procedures, to include (but not limited to):
        i. Install an appropriately licensed server operating system and antivirus protection software.
        ii. Make every effort to adhere to the latest applicable security configuration benchmarks published by the Center for Internet Security (CIS).

iii. Disable all default accounts except those required to provide necessary services.
iv. Install the most recent security patches as soon as practical, according to the Change Management Policy.
v. Disable all services and applications not required for the server to meet its mission (e.g., Telnet, FTP, DNS, DHCP, and SMTP on a file server).
vi. Include 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 licensed software required by the Data Owner or Application Administrator.
   i. Disable all application default accounts except those required to provide necessary services.
   ii. Change the application default passwords for all enabled accounts to one consistent with the Clarendon College User Accounts Password Policy.

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

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

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

f. Clarendon College maintains a Clarendon College device registry to facilitate compliance with security policies and procedures and assist in diagnosing, locating, and mitigating security incidents on the College network.
   i. Servers attached to the Clarendon College network must be registered by Clarendon College-IT and approved by the ISO.
   ii. Registration must include contact(s) and location, hardware and operating system/version, primary function(s) of the server, associated applications, and demonstrated compliance with the required Clarendon College policies, TAC§202 (Subchapter C) and other state and federal requirements.
   iii. The ISO will require updating registry information with the annual information security risk assessment process.

7. Application Administrators must:
   g. 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.
   h. Include 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).
8. Backups should be completed regularly based on a risk assessment of the data and services provided and must comply with the Data Backup Policy.
9. Clarendon College-IT will disconnect a server posing an immediate threat to the Clarendon College network to isolate the intrusion or problem and minimize risks.

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

10. Clarendon College cooperates fully with federal, state, and local law enforcement authorities in criminal investigations and will file criminal complaints against users who access or utilize the network to conduct a criminal act.
    k. Under the Clarendon College Technology Incident Management Policy, incident response best practices must be followed to ensure appropriate preservation and treatment of forensic data.
    l. All logs and audit trails about security-related events on critical or sensitive systems will be managed according to the Clarendon College Technology Incident Management Policy.
    m. The ISO will:
        i. Perform periodic reviews to ensure compliance with this policy.
        ii. Notify the Information Resources Manager (IRM) of identified concerns and risks.
11. Exceptions to the Server Administration Policy must be submitted in writing and approved by the ISO. Requests shall be justified, documented, and communicated during the risk assessment.

**DEFINITIONS:**

**Clarendon College IT:** The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

**Related Policies, References and Attachments:**

An index of approved Clarendon College-IT policies can be found on the Clarendon College Information Technology Services Policies website at https://www.clarendoncollege.edu/information-technology. The Policy Compliance Document contains reference materials, legal compliance guidelines, and policy enforcement. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

The Clarendon College Board of Regents approved this policy on March 27, 2025, version 1.2. This policy was reviewed by Will Thompson, Vice President of IT, on February 17, 2025.