Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
IT Physical Access & Environmental Policy:

PURPOSE:

This policy is intended to establish standards for securing Clarendon College-IT data centers, network closets, and protected IT facilities on the Clarendon College campuses. Effective implementation of this policy will minimize unauthorized access to these locations, provide more effective auditing of physical access controls, and ensure environmental threats to Clarendon College-IT data centers are monitored and remediated promptly.

SCOPE:

The IT Physical Access Policy applies to Clarendon College-IT data centers containing enterprise systems and other information processing facilities such as network closets, on-site backup storage locations, and the corresponding network infrastructure and access across campus that serve the Clarendon College user community.

POLICY STATEMENT:

Clarendon College-IT is responsible for the safety and security of data on the Clarendon College network and the equipment used to run the network infrastructure.

1. Environmental conditions in all data centers will be monitored and protected from environmental threats commensurate with the identified risks and their importance to Clarendon College's mission-critical business processes.
2. Physical security systems must comply with all applicable regulations such as, but not limited to, building codes and fire prevention codes.
3. Physical access to all restricted information technology resource facilities must be documented and managed.
4. All information technology resource facilities must be physically protected in proportion to the criticality or importance of their function at Clarendon College.
5. Access to information technology resource facilities must be granted only to Clarendon College support personnel and contractors whose job responsibilities require access.
6. The process of granting card and/or key access to information technology resource facilities must include the approval of the person responsible for the facility.
7. Each individual who is granted access rights to an information technology resource facility must receive emergency procedures training for the facility and must sign the appropriate access and non-disclosure agreements
8. Requests for physical access must come from Clarendon College-IT.
9. Access cards and/or keys must not be shared or loaned to others.

10. Access cards and/or no longer required keys must be returned to the appropriate department. Keys or cards must not be reallocated to another individual, bypassing the return process.

11. The appropriate department must report lost or stolen access cards and/or keys immediately.

12. All information technology resource facilities that allow visitor access will track access with a sign-in/out log.

13. Visitors must be escorted in card access controlled areas of information technology resource facilities.

14. A service charge may be assessed for access cards and/or keys lost, stolen, or not returned.

15. Card access records and visitor logs for information technology resource facilities must be kept for routine review based on the criticality of the protected information resources.

16. The person responsible for the information technology resource facility must promptly remove the card and/or key access rights of individuals who change roles within Clarendon College or are separated from their relationship with Clarendon College.

17. The person responsible for the information technology resource facility must periodically review access records and visitor logs and investigate any unusual access.

18. The person responsible for the information technology resource facility must review card and/or key access rights for the facility periodically and remove access for individuals who no longer require access.

19. Restricted access rooms should be identified with discrete signage.

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 July 15, 2023.

Appendix A: Authorized Personnel List

The following positions are authorized to access Clarendon College Information Technology (IT) data centers.

Location	Position
Main Campus, ALL	Clarendon College President
	Vice President of Academics Affairs
	IT Support Staff
	Vice President of IT
	Director of Maintenance and Ground
	Director of Custodial Services
Pampa Center, Pampa Only	Dean of the Pampa Center
Childress Center, Childress Only	Dean of the Childress Center

NOTE:
Those identified as having access to “All” locations may grant limited access to any IT data center.

Those identified as having access to a specific location may grant limited access to only that location's IT data center.

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 18, 2025.