Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Policy Compliance:

PURPOSE

The purpose of this policy is to ensure an information technology infrastructure that promotes the mission of the college. Clarendon College's information services network has been established for the use and benefit of Clarendon College in the conduct of its academic, business, and other operations. This document provides direction and support for the Clarendon College Information Security Program and the Information Technology (Clarendon College-IT) Policies.

This framework of IT security policies collectively represents the basis of the institutional Information Security program and on the aggregate whole meet the objectives as articulated by Texas Administrative Code Chapter 202 (TAC§202), Texas Higher Education Coordinating Board (THECB) and the associated guidelines.

This policy promotes the following goals:

1. To ensure the integrity, reliability, availability, and performance of Clarendon College information technology resources;
2. To ensure that use of Clarendon College information technology resources is consistent with the principles and values that governs Clarendon College as a whole;
3. To ensure that information technology resources are used for their intended purposes; and
4. To ensure all individuals granted access privileges to Clarendon College information technology resources have a clear understanding of what is expected during use and the consequences of violating Clarendon College policies.

SCOPE

This program applies equally to all individuals granted access privileges to any Clarendon College information technology resources.

POLICY STATEMENT

Information technology resources play an integral part in the fulfillment of the primary mission of the college. Users of Clarendon College's information technology resources have a responsibility to protect and respect those resources, and are responsible for knowing the regulations and policies that apply to appropriate use of the college's information technology resources.

Users must understand the expectation that if needed Clarendon College information technology resources may be limited and/or regulated by Clarendon College to fulfill the primary mission of the college. Usage may be constrained as required to assure adequate capacity, optimal performance, and appropriate security of those resources.

Anyone using Clarendon College's information resources expressly consents to monitoring of the network by the college at any time and for any purpose, including but not necessarily limited to, evidence of possible criminal activity, violations of law, contract, copyright or patent infringement, and/or violation of any college policy, rule, or regulation.

Clarendon College's information security policies can be found on the College's website at: http://[LINK TO POLICIES]

The Information Security User Guide which contains a summary of user related policies can be found at: http://[LINK TO SECURITY GUIDE]

The Information Security Program, which contains the framework ensures that the appropriate safeguards are applied to Clarendon College information systems. The program document can be found at: http://[LINK TO INFO SECURITY PROGRAM]

A review of the institution's information security program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and designated by the institution of higher education head or his or her designated representative(s).TAC 202.76(c)

NON-CONSENSUAL ACCESS

Clarendon College cannot absolutely guarantee the privacy or confidentiality of electronic documents. Consequently, persons that use these Clarendon College-owned resources, or any personally owned device that may be connected to a Clarendon College resource, have no right to privacy in their use of these resources and devices. However, Clarendon College will take reasonable precautions to protect the privacy and confidentiality of electronic documents and to assure persons that Clarendon College will not seek access to their electronic messages or documents without their prior consent except where necessary to:

1. Satisfy the requirements of the Texas Public Information Act, or other statutes, laws or regulations;
2. Allow institutional officials to fulfill their responsibilities when acting in their assigned capacity;
3. Protect the integrity of Clarendon College's information technology resources, and the rights and other property of Clarendon College;
4. Allow system administrators to perform routine maintenance and operations, security reviews, and respond to emergency situations; or
5. Protect the rights of individuals working in collaborative situations where information and files are shared.

To appropriately preserve the privacy of electronic documents and allow authorized individuals to perform their assigned duties, specific college staff and law enforcement will sign a Clarendon College Non-Consensual Access to Electronic Information Resources Request Form annually and submit the form to the Vice President of Information Technology. At the beginning of each fiscal year, non-consensual access requests will be resubmitted, reviewed, and approved or denied by the VPIT.

Individuals may request non-consensual access to specific data by initiating the Non-Consensual Access to Electronic Information Resources Request Form, obtaining the approval of their organizational head, and submitting the form to the Vice President of Information Technology (VPIT). If the request appears compliant with college policy, the DIS or designee will coordinate with the Information Security Officer (ISO) as necessary to satisfy the request.

VIOLATIONS

Failure to adhere to the provisions of the information technology security policies may result in:

1. suspension or loss of access to institutional information technology resources
2. appropriate disciplinary action under existing procedures applicable to students, faculty and staff, and
3. civil or criminal prosecution

Potential violations will be investigated in a manner consistent with applicable laws and regulations, and Clarendon College policies, standards, guidelines and practices.

EXCEPTIONS TO POLICY

Exceptions are granted on a case-by-case basis and must be reviewed and approved by the College designated VPIT. The required Policy Exception Form and procedures can be found at http://[LINK TO POLICY EXEMPTION FORM] The IRM will mandate the documentation and additional administrative approvals required for consideration of each policy exception request.

REFERENCE

There are many individual laws, regulations, and policies that establish our information security requirements. The primary applicable references are listed below.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC§202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Government Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

- Texas Department of Information Resources (DIR) Practices for Protecting Information Resources Assets

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.
Reference materials, legal compliance guidelines, and policy enforcement are available in the Policy Compliance Document. The Clarendon College Information Security Program and Clarendon College Information Security User Guide are also available on the Information Technology Services Policies website.

This policy was approved by the Clarendon College Board of Regents on July 17, 2023, version1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.