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

PURPOSE:
Understanding the importance of computer security and individual responsibilities and accountability for computer security are paramount to achieving organization security goals. This will be accomplished with a combination of general computer security awareness training and targeted product-specific training. The philosophy of protection and specific security instructions needs to be taught to and re-enforced with technology users. The security awareness and training information needs to be continuously upgraded and reinforced.

The purpose of the Technology Security Training Policy is to describe the requirements that ensure each user of Clarendon College information technology resources receives adequate training on technology security issues. Additionally, state law requires that institutions of higher education provide an ongoing information security awareness education program for all users of state-owned information resources (Texas Administrative Code (TAC) §202).

SCOPE:
The Clarendon College Technology Security Training policy applies equally to all employees.

POLICY STATEMENT:

1. All employees must attend the Clarendon College Security Awareness Training within 30 days of initially being granted access to Clarendon College information technology resources, or per request of the data owner or supervisor.

2. Annually, all employees must complete the Clarendon College Security Awareness training and pass the associated examination.

3. Annually, all employees must sign a non-disclosure agreement per Non- Disclosure Agreement Policy stating they have read and understand Clarendon College requirements regarding Clarendon College-IT policies and procedures.

4. Clarendon College-IT must prepare, maintain, and distribute an Information Security User Guide that concisely describes Clarendon College information security policies and procedures.

5. Clarendon College-IT must develop and maintain a communication plan that will communicate security awareness to the Clarendon College user community.

DEFINITIONS:
Information Security User Guide: Describes the requirements that ensure each person has the knowledge to protect Clarendon College information technology resources, protect themselves and comply with applicable laws.

Non-Disclosure Agreement: Formal acknowledgement that all employees must sign acknowledging they have read and understand Clarendon College requirements regarding computer security policies and procedures. This agreement becomes permanent record and will be renewed annually.

Security Awareness Training: Annual training required by Texas Administrative Code §202 to re-familiarize users with the Clarendon College policies, their responsibility to protect Clarendon College resources and to behave in a responsible, ethical and legal manner.

Texas Administrative Code (TAC) §202): State law that outlines mandatory user security practices, specifically security awareness training and non-disclosure agreements.

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.