

Clarendon College
Information Technology Services (CLARENDON COLLEGE-IT)
Non-Disclosure Agreement Policy:

PURPOSE:

Non-disclosure agreements are contracts intended to protect information considered to be sensitive or confidential. Information technology resources shall be used only for intended purposes as defined by Clarendon College (Clarendon College) and in compliance with applicable laws.

All individuals are accountable for their actions relating to information technology resources and shall formally acknowledge that they will comply with the Clarendon College security policies and procedures or they shall not be granted access to information technology resources. All employees will complete a non-disclosure agreement for information technology resources on an annual basis.

This document establishes specific requirements for Non-Disclosure Agreements at Clarendon College. (See Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C ([TAC§202](#)) and Texas Administrative Code, Title 1, Part 10, Chapter 203, Subchapter B ([TAC§203](#)))

SCOPE:

The Non-Disclosure Agreement Policy applies to all authorized users who utilize Clarendon College's information technology resources (including, but not limited to, Clarendon College Faculty, staff, student workers, temporary employees, vendors, consultants, employees of independent contractors, and personnel from other schools.)

POLICY STATEMENT:

All users must sign the Clarendon College Non-Disclosure Agreement (NDA) acknowledging they have read and understand Clarendon College requirements regarding computer security policies and procedures. A copy of the Clarendon College Information Users Guide will be sent along with the NDA. This signed non-disclosure agreement becomes permanent record and will be renewed annually.

Electronic signatures are an acceptable means of acknowledgement of Clarendon College's Non-Disclosure Agreement.

DEFINITIONS:

Non-Disclosure Agreement (NDA): 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.

Electronic Signature: The digital equivalent of a handwritten signature offering far more inherent security, which provides the added assurance of evidence of acknowledging informed consent by the signer.

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, version 1.1. This policy was reviewed by Will Thompson, Vice President of IT on July 15, 2023.