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

INTRODUCTION:
Clarendon College complies with state and federal statutes that protect confidential information.

Information technology resources that contain or transmit confidential information must be protected with the specified minimum requirements for encryption key standards and management.

SCOPE:
The Clarendon College Digital Encryption Policy applies equally to all individuals entrusted with any Clarendon College information technology resources.

POLICY STATEMENT:
Minimum encryption requirements to protect confidential information from unauthorized disclosure shall be limited to the following State of Texas encryption requirements:

1. Public information, described in the Texas Public Information Act or other enabling laws, rules, and regulations, has no minimum encryption requirements.
2. Confidential information must be protected from unauthorized disclosure or public release based on state or federal law, and personal identifying or sensitive personal information, as defined in the Texas Business and Commerce Code, must be encrypted with a minimum of 128-bit key length. The preferred key length is AES 256-bit length.
3. Federally protected data, federal tax information, protected health information, and law enforcement information must comply with NIST certification to FIPS 140-3 (Security Requirements for Cryptographic Modules) standards or the current standard.

Confidential information transmitted through or stored in an externally accessible location shall be encrypted from when it leaves a secure location until it is received in a safe location.

Confidential information should not be copied to or stored on removable media or a non-agency-owned computing device that is not encrypted.

Clarendon College may also implement these protections for data classifications other than Confidential.

Information resources assigned from one state agency to another or from a state agency to a contractor or other third-party representative shall be protected by the conditions imposed by the providing state agency.

DEFINITION:
Data Encryption: Data encryption translates data into another form or code so that only people with access to a secret key (formally called a decryption key) or password can read it. Encrypted data is called ciphertext, while unencrypted data is called plaintext.

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 18, 2025.