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

PURPOSE:
This policy establishes a framework for classifying and protecting Clarendon College data based on its value, sensitivity, and associated risks. Classification ensures compliance with state and federal requirements, including the Texas Administrative Code (TAC) 202, the DIR Data Classification Guide and Template, and federal standards such as NIST SP 800-59 and FIPS 199/200.

SCOPE:
This policy applies to all data owned, created, received, maintained, or transmitted by Clarendon College, in any form (electronic, printed, or verbal), and to all individuals with access to that data, including employees, contractors, vendors, and third-party service providers.

POLICY STATEMENT:
Clarendon College classifies data into three levels in alignment with DIR and TAC 202:

Confidential Data (High Impact)
Definition: Information exempt from disclosure under the Texas Public Information Act or other state/federal law. Unauthorized disclosure could result in legal liability, identity theft, financial loss, or significant reputational damage.

Examples:
- Personally Identifiable Information (PII) such as SSN, driver's license, or financial account numbers
- Student records protected by FERPA
- Protected Health Information (PHI) under HIPAA
- Payment Card Information (PCI DSS)
- IRS Federal Tax Information (FTI)
- Attorney–client privileged documents

Sensitive Data (Moderate Impact)
Definition: Information not classified as Confidential but that could cause harm to individuals, operations, or third parties if improperly disclosed.

Examples:
- Internal memos and draft reports
- Gross salary information
- Employment records are not protected by law
- Departmental strategy documents

Public Data (Low Impact)

Definition: Information explicitly approved or required for public release with minimal risk if disclosed.

Examples:

- College website content
- Press releases
- Course catalogs
- Public research findings

PII (Personally Identifiable Information)

Refers to any data that can be used to identify, contact, or locate an individual on its own or when combined with other information.

Examples of PII:

- Direct Identifiers (can identify a person alone)
    - Full name
    - Social Security Number (SSN)
    - Driver's license number
    - Passport number
    - Email address
    - Phone number
- Indirect Identifiers (can identify a person when combined with other data)
    - Date of birth
    - IP address
    - Employment records
    - Physical address
    - Biometric data (fingerprints, retina scans)
- Sensitive vs. Non-Sensitive PII
    - Sensitive PII: Requires extra protection (e.g., SSN, financial info, medical records).
    - Non-Sensitive PII: Publicly available but can still be linked to a person (e.g., zip code, workplace).

Data Owner and Custodian Responsibilities

- **Data Owners must:**
    - Classify data according to this policy.
    - Approve and periodically review access rights.
    - Ensure that custodians implement appropriate safeguards.

- Document and retain annual reviews for audit purposes.

- **Data Custodians must:**
  - Implement technical, physical, and administrative controls.
  - Enforce encryption, authentication, backup, and logging requirements.
  - Report incidents involving data loss, exposure, or unauthorized access.
  - Maintain systems in compliance with TAC 202 and DIR standards.

Safeguards by Classification Level

Classification	Storage	Transmission	Access Control	Disposal
Confidential	Encrypted at rest (AES-256 or equivalent); stored only on approved systems.	Encrypted in transit (TLS 1.2+, VPN)	Role-based access; MFA required	Secure shredding or DoD/NIST wipe
Sensitive	Limited access; departmental drives with access logs	TLS recommended	Departmental approval; least privilege	Deleted per retention schedule
Public	No restrictions	Open transmission	Public access allowed	Standard disposal

Review and Compliance

- Annual Reviews: Data Owners must review data classifications annually and document findings.
- Audits: Reviews will be retained for compliance with TAC 202.72 and are subject to internal/external audit.
- Incident Response: Any Confidential or Sensitive data breach must be reported immediately under the Clarendon College Information Security Program.

DEFINITIONS:

Personally Identifiable Information (PII): Refers to any data that can be used to identify, contact, or locate an individual, either on its own or when combined with other information.

Confidential Data: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g., the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreement requirements).

Data Classification: Classifying data according to its Confidential, Protected, or Public category.

Data Custodian: The person responsible for overseeing and implementing physical, technical, and procedural safeguards specified by the data owner.

Data Owner: Departmental position responsible for classifying business data, approving access to data, and protecting data by ensuring controls are in place. See Appendix A for a listing of data owners.

Protected Data: Sensitive data that requires protection but may be subject to disclosure or release – Public Information Act.

Public Data: Information intended or required for public release.

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.

Other related state and federal policies:

- DIR Data Classification Guide
- Data Classification Template
- TAC 202.24(b)(1)
- TAC 202 1(5)
- NIST 800-59

The Clarendon College Board of Regents approved this policy on September 18, 2025, version 1.3. This policy was reviewed by Will Thompson, Vice President of IT, on September 11, 2025.

Appendix A

The following lists the various data categories and the respective data owners. Data includes all collected data and communications.

Data Category	Title of Data Owner
Admissions	Associate Dean of Admissions
Financial Aid	Director of Financial Aid
Accounting	Comptroller
Purchase Management	Accounts Payable Clerk
Human Resources	Benefits and Payroll Coordinator
Transcript/Grade Management	Registrar
Curriculum	Vice President of Academic Affairs
Contracts	Assistant to the President
Library Resources	Librarian
Work Force Education	Dean of CTE
Housing/Student Life	Vice President of Student Affairs
Athletics	Athletic Director
Facility Maintenance	Maintenance Supervisor
IT Services and Systems	Vice President of IT

The Clarendon College Board of Regents approved this policy on September 18, 2025, version 1.3. This policy was reviewed by Will Thompson, Vice President of IT, on September 11, 2025.