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

PURPOSE:

Data Classification provides a framework for managing data assets based on value and associated risks and for applying the appropriate levels of protection as required by state and federal law as well as proprietary, ethical, operational, and privacy considerations. All Clarendon College data, whether electronic or printed, must be classified as Confidential, Protected, or Public. Consistent use of data classification reinforces with users the expected level of protection of Clarendon College data assets in accordance with Clarendon College policies.

The purpose of the Data Classification Policy is to provide a foundation for the development and implementation of necessary security controls to protect information according to its value and/or risk. Security standards, which define these security controls and requirements, may include document marking/labeling, release procedures, privacy, transmission requirements, printing protection, computer display protections, storage requirements, destruction methods, physical security requirements, access controls, backup requirements, transport procedures, encryption requirements, and incident reporting procedures.

SCOPE:

The Clarendon College Data Classification policy applies equally to all Data Owners and Data Custodians.

POLICY STATEMENT:

Data Owners and/or Data Custodians must classify data as follows:

1. Confidential: Sensitive data that must be protected from unauthorized disclosure or public release based on state or federal law, (e.g. the Texas Public Information Act, FERPA, HIPPA) and other constitutional, statutory, judicial, and legal agreements. Examples of Confidential data may include, but are not limited to:
    a. Personally identifiable information such as a name in combination with Social Security Number (SSN) and/or financial account numbers
    b. Student education records such as posting student identifiers and grades
    c. Intellectual property such as copyrights, patents and trade secrets
2. Medical records.
3. Protected: Sensitive data that may be subject to disclosure or release under the Texas Public Information Act but requires additional levels of protection. Examples of Protected data may include but are not limited to:
    a. Operational information

   b. Personnel records
   c. Information security procedures
   d. College-related research
   e. internal communications
4. Public: Information intended or required for public release as described in the Texas Public Information Act.

Data Custodians will review annually the following for all data under their responsibility:

1. Data Classification, check to ensure that data has been properly classified.
2. Data owner access and relevance.

DEFINITIONS:

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 their category of Confidential, Protected or Public.

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 a level of 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.
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 3/21/2024, version1._. This policy was reviewed by Will Thompson, Vice President of IT on 3/25/2024.

Appendix A

The following is a listing of the various data categories and the respective data owners. Data includes all collected data and communications.

Data Category	Title of Data Owner
Admissions	Director 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 Instruction
Contracts	Assistant to the President
Library Resources	Librarian
Work Force Education	Dean of CTE
Housing/Student Life	Dean of Students
Athletics	Athletic Director
Facility Maintenance	Maintenance Supervisor
IT Services and Systems	Vice President of IT