**Clarendon College**
**Information Technology Services (Clarendon College-IT)**
**Data Access Review Policy:**

**PURPOSE:**
The Clarendon College Guidelines for Data Standards, Data Integrity and Security document designates authority and responsibility for the ownership of College enterprise operational data. Commensurate with these designated roles, the specified Data Owners and Data Custodians are designated the responsibility of ensuring the security of information is maintained by establishing controls to confirm compliance with official procedures and policies.

**SCOPE:**
The Clarendon College Data Access Review policy applies equally to all Data Owners and Data Custodians.

**POLICY STATEMENT:**
The following distinctions among owner, custodian, and user responsibilities guide determination of the roles:

**Data Owner**
The owner or his or her designated representative(s) are responsible for:

1. classifying information under their authority, with the concurrence of the Clarendon College President or his or her designated representative(s), in accordance with Clarendon College's established information classification categories;
2. approving access to information resources and periodically review access lists based on documented risk management decisions;
3. formally assigning custody of information or an information resource;
4. coordinating data security control requirements with the ISO;
5. conveying data security control requirements to custodians;
6. providing authority to custodians to implement security controls and procedures;
7. justifying, documenting, and being accountable for exceptions to security controls. The information owner shall coordinate and obtain approval for exceptions to security controls with the Clarendon College information security officer; and
8. participating in risk assessments as provided under §202.75 of the Texas Administrative Code.

**Data Custodian**
Custodians of information resources, including third party entities providing outsourced information resources services to Clarendon College shall:

1. implement controls required to protect information and information resources required by this program based on the classification and risks specified by the information owner(s) or as specified by the policies, procedures, and standards defined by the Clarendon College Information Security Program;
2. provide owners with information to evaluate the cost-effectiveness of controls and monitoring;
3. adhere to monitoring techniques and procedures, approved by the ISO, for detecting, reporting, and investigating incidents;

4. provide information necessary to provide appropriate information security training to employees; and
5. ensure information is recoverable in accordance with risk management decisions.

**Users**

1. The user of an information resource has the responsibility to:
2. use the resource only for the purpose specified by Clarendon College or information-owner;
3. comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
4. formally acknowledge that they will comply with the security policies and procedures in a method determined by the Clarendon College President or his/her designated representative.

**Data Owners and Data Custodians must:**

1. No less than annually, document a complete review of parties having access to data under their area of responsibility.
2. Ensure data access reviews are performed more periodically, as deemed necessary by the Data Owner, relative to the risk of the data accessed.
3. Ensure any staffing changes are reflected as necessary to access authorizations, in a timely manner.
4. Ensure data access requests are reviewed, and granted or denied as appropriate based on essential College documented need, in a timely manner.
5. Ensure any changes to data access for any users comply with the Change Management Policy.
6. Ensure controls are established as required, or deemed necessary by the Data Owner, to ensure information security is maintained.
7. Maintain documentation of compliance with this policy.

**Information Security Officer (ISO)**

Clarendon College shall have a designated Information Security Officer (ISO), and shall provide that its Information Security Officer reports to executive level management, has the authority for information security for the entire college and possesses training and experience required to administer the functions described below.

The ISO is responsible for:

1. developing and maintaining a college-wide information security plan as required by §2054.133, Texas Government Code;
2. developing and maintaining information security policies and procedures that address the requirements of this program and the institution's information security risks;
3. working with the business and technical resources to ensure that controls are utilized to address all applicable requirements of this program and the institution's information security risks;
4. providing for training and direction of personnel with significant responsibilities for information security with respect to such responsibilities;
5. providing guidance and assistance to Clarendon College senior officials, information owners, information custodians, and end users concerning their responsibilities under this program;
6. ensuring that annual information security risk assessments are performed and documented by information-owners;

7. reviewing the Clarendon College inventory of information systems and related ownership and responsibilities;
8. developing and recommending policies and establishing procedures and practices, in cooperation with the Clarendon College Information Resources Manager, information-owners and custodians, necessary to ensure the security of information and information resources against unauthorized or accidental modification, destruction, or disclosure;
9. coordinating the review of the data security requirements, specifications, and, if applicable, third-party risk assessment of any new computer applications or services that receive, maintain, and/or share confidential data;
10. verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated prior to the purchase of information technology hardware, software, and systems development services for any new high impact computer applications or computer applications that receive, maintain, and/or share confidential data;
11. reporting, at least annually, to the Clarendon College President the status and effectiveness of security controls; and
12. informing the parties in the event of noncompliance with this chapter and/or with Clarendon College's information security policies.

The Information Security Officer, with the approval of the Clarendon College President, may issue exceptions to information security requirements or controls in this Program. Any such exceptions shall be justified, documented and communicated as part of the risk assessment process.

**Information Resources Manager (IRM) (TAC 211)**

The Clarendon College Information Resources Manager (IRM) is responsible to the State of Texas for management of the college's information resources. The designation of the colleges Information Resources Manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of Clarendon College's information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of Texas to implement Security Policies, Procedures, Practice Standards, and Guidelines to protect the Clarendon College Information Resources. TAC§211
if the IRM position falls vacant, the role defaults to the college President, who is then responsible for executing the duties and requirements of an IRM, including continuing education. The college's Vice President of Information Technology will serve as the IRM unless otherwise designated.

**The IRM will be assigned and designated these authorities:**

1. a senior official within the organization,
2. reports directly to a person with a title functionally equivalent to executive director or deputy executive director, and
3. has been vested with the authority necessary to fulfill his/her duties as the Information Resources Manager.

**Statutory IRM Responsibilities**

Per the Information Resources Management Act, the IRM will:

1. oversee the Biennial Operation Plan (BOP) preparation, subject to instructions from the Legislative Budget Board (LBB);

2. provide input into the Agency Strategic Plan;
3. comply with IRM continuing education requirements provided by DIR;
4. oversee the implementation of the organization's project management practices; and
5. demonstrate in the organization's strategic plan the extent to which the organization uses its project management practices.

**Other IRM Responsibilities**

***Other IRM responsibilities for this organization include***

1. overseeing the acquisition and management of the organization's information resources;
2. reporting on the information resource (IR) investment and benefits to executive management, DIR, the Legislature, and the Legislative Budget Board;
3. adopting and executing IR standards, policies, practices, and procedures; and
4. complying with legislative mandates.

The IRM must have an educational background, experience and qualifications provided by the Texas state Department of information (DIR) resources. §211.21 (1)

The IRM shall complete continuing education programs, including educational materials and seminars as provided by the Texas State DIR and approved by the board of the DIR. The President of Clarendon College is responsible for ensuring their appointed IRM remains qualified to serve as IRM. §211.21 (2)

The Clarendon College Information Security Officer (ISO) is designated the authority for oversight of this policy.

**The ISO will:**

1. Perform periodic reviews to assure compliance with this policy.
2. Notify the Information Resources Manager (IRM) of identified concerns and risks.

**DEFINITIONS:**

**Data Access Review**: The review and documentation of parties having access to data under the Data Owner's area of responsibility.

**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.

**Information Resources Manager (IRM):** Officer responsible to the State of Texas to manage Clarendon College information technology resources.

**Information Security Officer (ISO)**: Officer designated to administer the College Information Security Program.

**Director of Information Technology (DIT):** Officer has responsibilities for information systems operation; assisting in the installation and support of application software; network operations; installation, upgrade, and maintenance of network systems; installation, upgrade and maintenance of all information technology; and user support and training.

**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.