Clarendon COLLEGE

Information Security Program

2025

TABLE OF CONTENTS

Overview

Introduction

The Texas Administrative Code Chapter 202 (TAC§202) is written for state agencies and institutions of higher education. TAC §202 defines an institution of Higher Education as; "*A university system or institution of higher education as defined by §61.003, Education Code, except for public junior colleges unless otherwise directed by the Higher Education Coordinating Board* ". Clarendon College is a comprehensive, two-year community college – a public junior college. Current regulations do not require Clarendon College to maintain compliance with TAC§202. However, TAC§202 defines an outstanding security program closely following the federal requirements specified in NIST 800-53. Following these codes will provide security for the college's essential data. The guidelines established in this statute will ensure that Clarendon College data complies with current state and federal regulations and will prepare Clarendon College for future compliance requirements by the THECB.

This document defines an Information Security Program for Clarendon College (Clarendon College). It provides direction for managing and protecting Clarendon College's information technology resources' confidentiality, integrity, and availability. Much of the content has been borrowed from TAC §202, adopted to be effective March 17, 2015. The general requirements have been made specific to Clarendon College to more easily understand the roles and responsibilities of the Clarendon College constituents.

The Information Security Program contains administrative, technical, and physical safeguards to protect College information technology resources. Actions have been taken to protect these resources against accidental or unauthorized access, disclosure, modification, or destruction and to assure information availability, integrity, utility, authenticity, and confidentiality. The Clarendon College Information Security Program appropriately manages access to Clarendon College information technology resources. Unauthorized modification, deletion, or disclosure of information technology resources can compromise the mission of Clarendon College, violate individual privacy rights, and possibly constitute a criminal act. (TAC§202.70).

This framework represents the basis of the institutional information security program. The Clarendon College Information Security Program and security standards are not intended to prevent or impede the authorized use of information technology resources as required to meet the college mission.

Clarendon College's information technology resources may be limited or regulated by Clarendon College, as needed, to fulfill the primary mission of the college. Usage of Clarendon College information technology resources may be constrained as required to assure adequate capacity, optimal performance, and appropriate security of those resources.

Purpose

The purpose of the Clarendon College Information Security Program is to provide the college community with a description of the college policies for information security. Additionally, the framework of this plan is designed to document the controls used to meet the information security program objectives by:

- Identify system data owners, provide the data classification standard, and identify the category of its data.
- Reviewing all authorized users and their security access for each system.
- Providing security awareness training for all employees.
- Performing the risk assessment process and developing the risk mitigation plan.
- Reviewing and updating the disaster recovery plan.
- Reviewing current policies and training programs.
- Create a security effectiveness report for the president.
- Review the current process and implement changes as necessary.

The Information Security Program process combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability.

Authority

1 Texas Administrative Code (TAC) §202
Texas Higher Education Coordinating Board (THECB)

Scope

This program applies equally to all individuals granted access privileges to any Clarendon College information technology resource, including the following:

- Central and departmentally managed college information technology resources.
- All users employed by Clarendon College, contractors, vendors, or anyone with access to Clarendon College's information technology resources.
- Non-Clarendon College-owned computing devices that may store protected Clarendon College information.
- All categories of information, regardless of the medium in which the information asset is held or transmitted (e.g., physical or electronic).
- Information technology facilities, applications, hardware systems, and network resources owned or managed by Clarendon College. This includes third-party service providers' systems that access or store Clarendon College's protected information.
- Auxiliary organizations, external businesses, and organizations that use college information technology resources must operate those assets in conformity with the Clarendon College Information Security Program.

Information Security Roles and Responsibilities

The following distinctions among owner, custodian, and user responsibilities guide the determination of the roles (TAC§202.72).

Data Owner

The owner or their designated representative(s) are responsible for:

- classifying information under their authority, with the concurrence of the Clarendon College President or their designated representative(s), by Clarendon College's established information classification categories;
- approving access to information resources and periodically reviewing access lists based on documented risk management decisions;
- formally assigning custody of information or an information resource;
- coordinating data security control requirements with the ISO;
- conveying data security control requirements to custodians;
- provide authority to custodians to implement security controls and procedures;
- 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
- participating in risk assessments as provided under §202.75 of the Texas Administrative Code.

Clarendon College Data Owners:

- Finance and Operations: Comptroller
- Student: Vice President of Student Affairs
- Academic Affairs: Vice President of Academic Affairs
- ERP General: Designated IRM

Data Custodian

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

- implement controls required to protect information and information resources needed for this program based on the classification and risks specified by the information owner(s) or as determined by the policies, procedures, and standards defined by the Clarendon College Information Security Program;
- provide owners with information to evaluate the cost-effectiveness of controls and monitoring;
- adhere to monitoring techniques and procedures approved by the ISO for detecting, reporting, and investigating incidents;
- provide information necessary to provide appropriate information security training to employees and
- Ensure that information is recoverable following risk management decisions.

Clarendon College Data Custodians:

- Admissions: Associate Dean of Enrollment Services
- Purchasing: Accounts Payable Clerk
- Student Records: Registrar
- ERP General: Vice President of Information Technology
- Financial Aid: Associate Dean of Financial Aid
- Residence Life: Vice President of Student Affairs
- Human Resources: Comptroller
- Payroll: Benefits and Payroll Coordinator
- Accounting: Cashier, Accounts Payable Clerk, Controller

Users

The user of an information resource has the responsibility to:

- use the resource only for the purpose specified by Clarendon College or the information owner;
- comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction; and
- formally acknowledge that they will comply with the security policies and procedures in a method determined by the Clarendon College President or their designated representative.

Public Use of Clarendon College Systems (Guest on campus)

Clarendon College information resources designated for use by the public shall be configured to enforce security policies and procedures without requiring user participation or intervention. Information resources must require the acceptance of a banner or notice before use.

College President

As the institution's head, the president of Clarendon College is ultimately responsible for the security of the information resources. The president or their designated representative shall:

- designate an Information Security Officer who has the explicit authority and the duty to administer the information security program institution-wide;
- allocate resources for ongoing information security remediation, implementation, and compliance activities that reduce risk to a level acceptable to the institution head;
- ensure that Clarendon College senior officials and information owners, in collaboration with the information resources manager and information security officer, support the provision of information security for the information systems that support the operations and assets under their direct or indirect (e.g., cloud computing or outsourced) control;
- ensure that Clarendon College has trained personnel to assist the college in complying with the requirements of this program and related policies;
- ensure that Clarendon College senior officials support the college education Information Security Officer in developing, at least annually, a report on the Clarendon College information security program, as specified in §202.71(b)(11) and §202.73(a) of the Texas Administrative Code;
- approve high level risk management decisions as required by §202.75(4) of the Texas Administrative Code;
- review and approve at least annually the Clarendon College Information Security Program required under §202.74 of the Texas Administrative Code; and
- ensure that information security management processes are part of the institution of higher education strategic planning, operational processes, and policies.

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 the training and experience required to administer the functions described below.
The ISO is responsible for:

- developing and maintaining a college-wide information security plan as required by §2054.133, Texas Government Code;
- developing and maintaining information security policies and procedures that address the requirements of this program and the institution's information security risks;
- 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;
- providing for training and direction of personnel with significant responsibilities for information security concerning such responsibilities;
- Provide guidance and assistance to Clarendon College senior officials, information owners, information custodians, and end users concerning their responsibilities under this program;

- ensuring that annual information security risk assessments are performed and documented by information owners;
- reviewing the Clarendon College inventory of information systems and related ownership and responsibilities;
- 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;
- 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;
- verifying that security requirements are identified and risk mitigation plans are developed and contractually agreed and obligated before 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;
- reporting, at least annually, to the Clarendon College President the status and effectiveness of security controls; and
- informing the parties of noncompliance with this chapter and/or Clarendon College's information security policies.

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

Information Resources Manager (IRM)

The Clarendon College Information Resources Manager (IRM) is responsible to the State of Texas for managing the college's information resources. The designation of the college's 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.
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 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 the executive director or deputy executive director and
3. has been vested with the authority necessary to fulfill their 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's 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 it 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 requirements provided by the DIR and approve them by the DIR board. The President of Clarendon College ensures their appointed IRM remains qualified to serve as IRM §211.21 (2).

Program Framework

This section defines the Information Security Program process to ensure Clarendon College's information systems' continuity, performance, and security. This framework is based on the main objective of the information security program: confidentiality, integrity, and availability (The CIA Triad).

A review of Clarendon College's Information Security Program for compliance with the TAC§202 standards will be performed biennially based on business risk management decisions by individual(s) independent of the Information Security Program (TAC§202.73.3).

The following processes will ensure that the appropriate safeguards are applied to Clarendon College's information systems and will continue to mature with the growing needs of the college's mission.

1. Establish Responsibility

At the beginning of each fiscal year, the IRM and the ISO per Data Access Review Policy will review the assigned data owners and their selected data custodians. The data owners will review/identify the related data stored on their system and the categories stored as confidential, protected, or public according to the data classification standards in the Data Classification Policy. The data owners will then review the list of authorized users for each system and make the necessary changes using the least privileged model.
The IRM will review and approve information ownership and responsibilities, including personnel, equipment, hardware, and software, and define information classification categories. (TAC§202.72(1A)(2A)).

2. Security Awareness Training

All employees with access to the Clarendon College information technology resources must participate in information security awareness training (Technology Security Training Policy) (TAC§202.71(b)(4)).
The training promotes awareness of the following:

- Clarendon College's information security policies, standards, procedures, and guidelines.
- Potential threats against college-protected data and information technology resources.
- Appropriate controls and procedures to protect the confidentiality, integrity, and availability of protected data and information technology resources.

New employees will sign a non-disclosure agreement and be provided individual access to the Information Security Awareness Training Program.
Employees are expected to complete the training within 30 days of receiving their access to the program and then annually.
Department heads and college executive management are responsible for and will be provided training compliance status.

3. Risk Assessment and Planning

Risk Planning

The principal reason for managing risk in an organization is to protect the mission and assets of the organization. Understanding risk, especially the magnitude of the risk, allows organizations to prioritize resources.
Security must be a consideration from the very beginning of any project at the college rather than something that is added later. A control review should be performed before implementing information technology resources that store or handle confidential, sensitive, and/or protected information. This may include:

- A technical security evaluation to ensure appropriate safeguards are in place and operational.
- A risk assessment, including a regulatory, legal, and policy compliance review.
- A contingency plan, including the data recovery strategy.
- Review ongoing production procedures, including change controls and integrity checks.

Risk Assessment

Clarendon College annually assesses its information risks and vulnerabilities (Risk Assessment Policy). Risk assessments may be aimed at particular types of information, areas of the organization, or technologies. Risk assessments provide the basis for prioritization and selection of remediation activities and can be used to monitor the effectiveness of college controls. Risk assessments shall:

- assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information;
- evaluate the sufficiency of existing policies, procedures, information systems, internal controls, and security practices, in addition to other safeguards in place to control risks;
- be classified and updated based on the inherent risk. Risk and frequency will be ranked 'high,' 'medium,' or 'low' based on TAC§202.72 criteria;
- design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of state and federal laws;
- monitor the effectiveness of those safeguards;
- analyze data collected to identify control objectives, risk exposures, mitigation strategies, and action plans for addressing each risk with timelines and
- support the annual report to the president and substantiate any changes to the information security program that may be needed due to evaluating the information collected.

4. Disaster Recovery/Business Continuity Plan

Clarendon College-IT is responsible for developing and maintaining a Disaster Preparedness/ Recovery/ Business Continuity Plan (see Business Continuity and Disaster Recovery Policy) designed to address the operational restoration of Clarendon College's critical computer processing capability. This plan identifies the strategy to recover centrally administered data storage, programs, and processing capability in the event of a disaster. The plan identifies the minimum acceptable recovery configuration, which must be available for Clarendon College to resume the minimum required levels of essential services. The plan is in strategic areas and available to all Computer Services personnel through a shared network resource. The plan contains proprietary and confidential information, is not intended for public distribution, and will not be published online. (TAC§202.74) (Texas Government Code, Sec. 552.139)
The Clarendon College-Business Continuity and Disaster Recovery Policy described above does not address individual departments' needs beyond restoring access to their critical centrally administered applications. All major college divisions/departments develop individual plans for protecting their information resource assets and operating capability. Each departmental plan will address losses ranging from minor temporary outages to catastrophes.

5. Annual Review

At the end of each fiscal year, the Information Security Officer (ISO) will review the risk assessment results, Security Awareness Training Program, Information Security User Guide, Information Security Program, and all Clarendon College IT Policies.

The ISO and IRM will report Clarendon College's information security controls' status and effectiveness and present recommended revisions and improvements based on collected information. The report will include: Description and/or narrative of any security incident that resulted in a significant impact on the university.

- Status of the Risk Assessments, noting any significant changes.
- Status of the Vulnerability Assessments, noting any significant findings and corrections.
- Status of the IT Policy review.
- Status of the IT Security Awareness Training Program.
- Anticipated changes in the next fiscal year.

Compliance References

Clarendon College's information security practices must comply with a variety of federal and state laws, as well as Clarendon College policies. These regulations are generally designed to protect individuals and organizations against the unauthorized or accidental disclosure of information that could compromise their identity or privacy. Legal regulations cover a variety of types of information, including personally identifiable information (e.g., social security number, driver's license number), personal financial information (e.g., credit card numbers), medical information, and confidential student information.

Many individual laws, regulations, and policies establish our information security requirements. While it is not possible to list all potentially applicable laws and regulations, the most relevant to the users of Clarendon College's information technology resources are listed below.

Information technology resources will be regularly tested and audited to ensure adherence to external and internal standards to avoid breaches of any law, regulation, contractual obligation, or institutional policy. Students, faculty, and staff are responsible for understanding and observing these and all other applicable policies, regulations, and laws concerning their use of Clarendon College's information technology resources.

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA) of 1996
- Federal Information Security Management Act of 2002 (FISMA)
- Texas Administrative Code, Title 1, Subchapter 203
- Texas Administrative Code, Title 1, Subchapter 211
- Texas Government Code, Title 5, Subtitle A, Chapter 552
- Texas Penal Code, Chapter 33, Computer Crimes
- Texas Penal Code, § 37.10, Tampering with Governmental Record
- United States Code, Title 18, § 1030, Computer Fraud and Related Activity of 1986
- Copyright Act of 1976
- Digital Millennium Copyright Act October 20, 1998
- Electronic Communications Privacy Act of 1986
- The Information Resources Management Act (IRM) TGC, Title 10, Subtitle B, 2054.075(b)
- Computer Software Rental Amendments Act of 1990
- ISO/IEC 27002:2005 standards jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)

Failure to Comply (Enforcement)

Consistent with Clarendon College policies, the ISO is authorized by the Clarendon College President to ensure that the appropriate processes to administer this program are in place, communicated to, and followed by the college community.
Administrators must ensure that measures are taken within their department to comply with this policy and its related standards, guidelines, and practices. Departments found to be non-compliant will be required to take specific steps to come into compliance within a specified time. If compliance cannot be achieved, the ISO must approve a written request for an exception. Approved requests will be reviewed annually to determine whether an exception is warranted.

Clarendon College reserves the right to temporarily or permanently suspend, block, or restrict access to college information technology resources, independent of such procedures when it reasonably appears necessary to do so to protect the confidentiality, integrity, availability, or functionality of Clarendon College information technology resources; to protect Clarendon College from liability, or to enforce this policy and its related standards and practices.

Failure to adhere to the provisions of this policy statement or the appropriate use policy statement may result in:

- suspension or loss of access to Clarendon College information technology resources
- appropriate disciplinary action under existing procedures applicable to students, faculty, and staff, and
- civil or criminal prosecution

Potential violations will be investigated consistent with applicable laws and regulations and Clarendon College policies, standards, guidelines, and practices (TAC§202.72)(TAC§202.73).
The Vice President for Administrative Services or designee will ensure that suspected violations and resultant actions receive the proper and immediate attention of the appropriate college officials, law enforcement, outside agencies, and disciplinary/grievance processes under due process.
Third-party service providers who do not comply may be subject to appropriate actions as defined in contractual agreements or other legal remedies available to Clarendon College.
Appeals of college actions resulting from enforcement of this policy will be handled through existing disciplinary/grievance processes for Clarendon College students and employees.

Obtaining a Policy Exemption

Policy exceptions are granted case-by-case and must be reviewed and approved by the college-designated IRM. The IRM will mandate the documentation and additional administrative approvals required to consider each policy exemption request. TAC§202.71(c).

Definitions

Alphabetized listing of common and specific terms used in this Information Security Program. When used in this program, the words and terms shall have the following meanings unless the context indicates otherwise.

Access
The physical or logical capability to view, interact with, or use information resources.

Agency Head
The top-most senior executive with operational accountability for an agency, department, commission, board, office, council, authority, or other agency in the executive or judicial branch of state government that is created by the constitution or a statute of the state or institutions of higher education, as defined in §61.003, Education Code.

Availability
The security objective is to ensure timely and reliable access to and use of information.

Clarendon College IT: The department or any company working on behalf of the Clarendon College IT Department is responsible for maintaining and supervising the Clarendon College IT infrastructure.

Cloud Computing
It has the same meaning as "Advanced Internet-Based Computing Service" as defined in §2157.007(a). Texas Government Code

Confidential Information
Information that must be protected from unauthorized disclosure or public release based on state or federal law or other legal agreements.

Confidentiality
The security objective is to preserve authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Control
A safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources. Controls may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Control Standards Catalog
The document provides state agencies and higher education institutions with state-specific implementation guidance for alignment with the National Institute of Standards and Technology (NIST) SP (Special Publication) 800-53 security controls.

Custodian
See information custodian.

Department
The Department of Information Resources.

Destruction
The result of actions taken to ensure that media cannot be reused as originally intended and that information is technologically infeasible to recover or prohibitively expensive.

Electronic Communication
A process used to convey a message or exchange information via electronic media. It includes the use of electronic mail (email), Internet access, Instant Messaging (IM), Short Message Service (SMS), facsimile transmission, and other paperless means of communication.

Encryption (encrypt or encipher
The conversion of plaintext information into a code or cipher text using a variable called a "key" and processing those items through a fixed algorithm to create the encrypted text that conceals the data's original meaning.

Guideline
Recommended, non-mandatory controls that help support standards or serve as a reference when no applicable standard is in place.

High Impact Information Resources
Information Resources whose loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, assets, or individuals. Such an event could:

- cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.

Information
Data is processed, stored, or transmitted by a computer.

Information Custodian
A department, agency, or third-party service provider is responsible for implementing the information owner-defined controls and access to an information resource.

Information Owner(s)
A person(s) with statutory or operational authority for specified information or information resources.

Information Resources
As defined in §2054.003(7), Texas Government Code. The procedures, equipment, and software employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information and associated personnel, including consultants and contractors.

Information resources technologies
As defined in §2054.003(8), Texas Government Code. Data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training.

Information Resources Manager
As defined in §2054.071, Texas Government Code. A senior official within the organization oversees the acquisition and use of information technology within a state agency or institution of higher education and ensures that all information resources are acquired appropriately, implemented effectively, and in compliance with relevant regulations and policies.

Information Security Program
The policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.

Information System
An interconnected set of information resources under the same direct management control that shares standard functionality. An Information System typically includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications, and people.

Integrity
The security objective safeguards against improper information modification or destruction, including ensuring information non-repudiation and authenticity.

ITCHE
Information Technology Council for Higher Education.

Low-Impact Information Resources
Information resources whose confidentiality, integrity, or availability loss could be expected to have a limited adverse effect on organizational operations, assets, or individuals. Such an event could:

- cause a degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is noticeably reduced;
- result in minor damage to organizational assets;
- result in minor financial loss; or
- result in minor harm to individuals.

Moderate Impact Information Resources
Information Resources whose confidentiality, integrity, or availability loss could be expected to affect organizational operations, assets, or individuals seriously. Such an event could:

- cause a significant degradation in mission capability to an extent and duration that the organization can perform its primary functions, but the effectiveness of the functions is significantly reduced;
- result in significant damage to organizational assets;
- result in significant financial loss; or
- result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.

Network Security Operations Center (NSOC)
As defined in §2059.001(1), Texas Government Code.

Personal Identifying Information (PII)
A category of personal identity information defined by §521.002(a)(1), Business and Commerce Code.

Procedure
Instructions to assist information security staff, custodians, and users in implementing policies, standards, and guidelines.

Residual Risk
The risk that remains after security controls have been applied.

Risk
The effect on the entity's missions, functions, image, reputation, assets, or constituencies considering the probability that a threat will exploit a vulnerability, the safeguards already in place, and the resulting impact. Risk outcomes are a consequence of Impact levels defined in this section.

Risk Assessment
The process of identifying, evaluating, and documenting the impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations from planned or in-place security controls.

Risk Management
Aligning information resources risk exposure with the organization's risk tolerance by accepting, transferring, or mitigating risk exposures.

Security Incident
An event that results in accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.

Sensitive Personal Information
A category of personal identity information defined by §521.002(a)(2), Business and Commerce Code.

Standards
Specific mandatory controls that help enforce and support the information security policy.

Threat
Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals.

User of an Information Resource
An individual, process, or automated application authorized to access an information resource by federal and state law, agency policy, and the information owner's procedures and rules.

Vulnerability Assessment
A documented evaluation containing the information described in §2054.077(b), Texas Government Code, which includes the susceptibility of a particular system to a specific attack.

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 17, 2025.