COLLIN COLLEGE

Information Security Plan

Contents

Overview

Introduction

The Texas Administrative Code, Title I, Part 10, 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. Beginning September 1, 2019, Senate Bill 64 modified Section 2054.0075 of the Government Code to add the requirement for "public junior colleges and public junior college districts" to be compliant with information security standards outlined within TAC §202*" Collin College is a public junior college and an institution of higher education for purposes of compliance with TAC §202 Section 202.70-202.76.

TAC§202 defines an outstanding security program that closely follows 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 Collin College (CC) data is compliant with current state and federal regulations and will prepare CC for future compliance requirements by the THECB.

This document defines an Information Security Plan for CC. It provides direction for managing and protecting the confidentiality, integrity, and availability of CC information technology resources. Much of the content is directly from TAC §202. The general requirements have been made specific to CC to understand the roles and responsibilities of the CC constituents more easily.

The Information Security Plan 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 assure information availability, integrity, utility, authenticity, and confidentiality. The CC Information Security Plan appropriately manages access to CC information technology resources. Unauthorized modification, addition, deletion, or disclosure of information technology resources can compromise the mission of CC, violate individual privacy rights, and possibly constitute a criminal act. (TAC§202.70).

This framework represents the basis of the institutional information security plan. The CC Information Security Plan and security standards are designed not to prevent or impede the authorized use of information technology resources as required to meet the college mission.

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

Purpose

The purpose of the CC Information Security Plan is to provide the college community with a description of the college Information Security Protocols (ISPs) for information security. Additionally, the framework of this plan is to document the controls used to meet the information security plan objectives by:

- Identifying system data owners, providing the data classification standard and identifying the category of its data.
- Review all authorized users and their security access for each system.
- Provide security awareness training for all employees.
- Performing the risk assessment process and developing the risk mitigation plan.
- Review and update the disaster recovery plan.
- Review current ISPs and training programs.
- Create a security effectiveness report to the District President.
- Review the current process and implement changes as necessary.

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

Authority

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

Scope

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

- Central and departmentally-managed college information technology resources
- Employees, contractors, vendors, or any other person with access to CC's information technology resources
- Non-CC-owned computing devices that may store CC information or CC-protected 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, network resources owned or managed by CC, including third-party service providers' systems that access or store CC's protected information.
- Auxiliary organizations, external businesses, and organizations that use college information technology resources must operate those assets in conformity with the CC Information Security Plan.

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 Data Owner or their designated representative(s) are responsible for:

- classifying information under their authority, with the concurrence of the District President or their appointed representative(s), per CC'sestablished 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 Chief Information Security Officer (CISO);
- conveying data security control requirements to custodians;
- providing authority to custodians to implement security controls and procedures;
- justifying, documenting, and being accountable for exceptions to security controls. The data owner shall coordinate and obtain approval for exceptions to security controls with the CC information security officer; and
- participating in risk assessments as provided under §202.75 of the Texas Administrative Code.

Data Owners are defined for these ISPs, but Collin College remains the owner of data maintained, stored, or transmitted on and through CC's information technology resources.

CC Data Owners:

- Financial Services: Chief Financial Officer
- Student and Enrollment Services: Vice President Student and Enrollment Services
- Academic Affairs: Vice President Academic Affairs
- Human Resources: Chief Human Resources Officer
- Designated Information Resource Manager (IRM): Chief Information Officer (CIO)

Data Custodian

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

- implement controls required to protect information and information resources needed by this plan based on the classification and risks specified by the information owner(s) or as prescribed by CC's ISPs, procedures, and any standards defined by the CC Information Security Plan;
- provide owners with information to evaluate the cost-effectiveness of controls and monitoring;

- adhere to monitoring techniques and procedures, approved by the CISO, for detecting, reporting, and investigating incidents;
- provide information necessary to provide appropriate information security training to employees; and
- ensure data is recoverable in accordance with risk management decisions.

CC Data Custodians:

- Purchasing: Director Purchasing/Contract Administrator
- Registration and Records: Dean Admissions/Registrar
- Technology Services Software Support: Executive Director Technology Services/Executive Directory Technology Support
- Financial Aid: Director of Financial Aid/Veterans Affairs
- Human Resources: Director HR/Benefits Compensation and HRIS
- Payroll: Director Payroll Administration
- Accounting: Director Accounting
- Bursar and Accounts Receivable: Bursar

Users

The user of an information technology resource has the responsibility to:

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

Public Use of CC systems (Guest on campus)

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

District President

The Collin College District President, as head of the institution, is ultimately responsible for the security of the college's information resources. The president or their designated representative shall:

- appoint the Chief Information Security Officer (CISO) who has the explicit authority and the duty to administer the information security plan 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 CC senior officials and data-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 CC has trained personnel to assist the college in complying with the requirements of this plan and related ISPs;
- ensure that CC senior officials support the college CISO in developing, at least annually, a report on the CC information security plan, as specified in §202.71(b)(11) and §202.73(a) of the Texas AdministrativeCode;
- approve high-level risk management decisions as required by §202.75(4) of the Texas Administrative Code;
- review and approve at least annually the CC information security plan required under §202.74 of the Texas Administrative Code; and
- ensure that information security management processes are part of strategic planning, operational processes, and ISPs.

Chief Information Security Officer (CISO)

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

The CISO is responsible for:

- developing and maintaining a college-wide information security plan as required by §2054.133, Texas Government Code;
- developing and maintaining ISPs and procedures that address the requirements of this plan 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 plan and the institution's information security risks;
- providing for training and direction of personnel with significant responsibilities for information security concerning such responsibilities;
- providing guidance and assistance to CC senior officials, information owners, information custodians, and end-users concerning their obligations under this plan;
- ensuring that annual information security risk assessments are performed and documented by data-owners;
- reviewing the CC inventory of information systems and related ownership and responsibilities;
- developing and recommending ISPs and establishing procedures and practices, in cooperation with data-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, 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, or shareconfidential data;
- reporting, at least annually, to the District President the status and effectiveness of security controls; and
- informing the parties in non-compliance with this chapter or with CC's information security ISPs.

The CISO, with the approval of the District President, may issue exceptions to information security requirements or controls in this plan. Any such exceptions shall be justified, documented, and communicated as part of the risk assessment process.

Plan Framework

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

A review of CC's Information Security Plan for compliance with the TAC§202 standardswill be performed at least biennially, based on business risk management decisions, by an individual(s) independent of the Information Security Plan (TAC§202.73.3).

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

1. **Establish Responsibility for Data**

   The assigned data owners and their selected data custodians will be reviewed by the CISO per Data Access Review ISP at the beginning of each fiscal year. The data owners will review/identify the categories of data stored on their system and designate the types of data stored as confidential, protected, or public according to the data classification standards in the Data Classification ISP.

   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 CISO will review and approve information ownership and responsibilities to include 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 CC information technology resources must participate in information security awareness training at least annually. (TAC§202.71(b)(4)).

   The training promotes awareness of:

- CC ISPs, standards, procedures, and guidelines.
- Potential threats against college-protected data and information technology resources.
- Controls and procedures to protect the confidentiality, integrity, and availability of protected data and information technology resources

New employees will sign an Employee Agreement Form and will 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 designated college leadership team members are responsible for and provided with training compliance status.

3. Risk Assessment and 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, allows organizations to prioritize resources.

Information 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, or protected information. This may include:

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

CC performs annual assessments of its information risks and vulnerabilities (DIR-Risk Assessment Guidelines). Risk assessments may target particular types of information, areas of the organization, or technologies. Risk assessments provide the basis for prioritization and selection of remediation activities and can 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 ISPs, 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 plan resulting from evaluating the information collected.

4. Disaster Recovery/Business Continuity Plan

Collin College-Technology Service (CC-TS) is responsible for developing and maintaining an information technology disaster preparedness/ recovery/ business continuity plan (Plan) designed to address the functional restoration of CC's critical computer processing capability and data protection. This Plan identifies the strategy to recover centrally administered data storage, plans, and processing capability in the event of a disaster. The Plan identifies the minimum acceptable recovery configuration, which must be available for CC to resume the minimum required essential services levels. The Plan is located in strategic areas and accessible to all Technology 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 on the Web in its entirety. (TAC§202.74) (Texas Government Code, Sec. 552.139)

The CC-TS Disaster Preparedness/Recovery Plan described above does not address the needs of individual departments beyond the restoration of access to their critical centrally administered applications. All central 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 catastrophic.

5. Annual Review

At the beginning of each fiscal year, the CISO will review the risk assessment results, Security Awareness Training Program, Information Security User Guide,Information Security Plan, and all CC-TS, Information Security Procedures (ISP).

The CISO will report the status and effectiveness of CC's information security controls to the District President and present recommended revisions and improvements based on the information collected.The report will include:

- A description and narrative of any security incident that resulted in a significant impact on the college or reported to law enforcement agencies or other reporting agencies
- Status of the Risk Assessments noting any significant changes
- Quality of the Vulnerability Assessments noting any substantial findings and mitigation status
- Status of the ISP review.
- Status of the Security Awareness Training Program.
- Anticipated changes over the next fiscal year

Compliance References

CC's information security practices must comply with a variety of federal and state laws, as well as CC ISPs. These regulations are designed to protect individuals and organizations against the unauthorized or accidental disclosure of information that could compromise their identity or privacy. Legal regulations cover various 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 information security requirements. While it is impossible to list all potentially applicable laws and regulations, the most relevant to CC's information technology resources users are listed below.

To avoid breaches of any law, regulation, contractual obligation, or Board policy, information technology resources will be regularly tested and audited to ensure adherence to external and internal standards.

Students, faculty, and staff are responsible for understanding and observing the following and all other applicable Board policies, ISPs, regulations, and laws connected with their use of CC's information technology resources, to the extent they apply:

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C (TAC 202)
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Federal Information Security Management Act of 2002 (FISMA)
- Gramm-Leach-Bliley Act of 1999 (GLBA)
- 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)
- Texas Identity Theft Enforcement and Protection Act

Failure to Comply (Enforcement)

Consistent with CC Information Security Plan, the CISO is authorized by the District President to ensure that the appropriate processes to administer this plan are in place, communicated to, and followed by the Collin College community.

CC administrators must ensure that measures are taken within their department to comply with this ISP and its related standards, guidelines, and practices. Departments found to be non-compliant will require specific steps to comply within a specified time. If compliance cannot be achieved, a written request for an exception must be approved by the CISO. Approved requests will be reviewed annually to determine if an exception is warranted.

CC 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 CC information technology resources; to protect CC from liability, or to enforce CC ISPs and related standards and practices.

Failure to adhere to CC's ISPs or Board policies addressing appropriate use of technology resources may result in:

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

Potential violations will be investigated in a manner consistent with applicable laws and regulations and CC ISPs, standards, guidelines, and practices (TAC§202.72)(TAC§202.73). The Senior Vice President Campus Operations 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 CC. Appeals of college actions resulting from enforcement of this ISP will be handled through existing disciplinary/grievance processes outlined in Board policy for CC students and employees.

Obtaining an ISP Exemption

Exemptions to ISPs are granted on a case-by-case basis and must be reviewed and approved by the CISO. The CISO will mandate the documentation and additional administrative approvals required to consider each exemption request. TAC§202.71(c).

Definitions

The words and phrases shall have the following meanings when used in this ISP unless the context indicates otherwise.

Access
The physical or logical capability to view, interact with, or otherwise 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, Texas Education Code.

Availability
The security objective is to ensure authorized users have access to the necessary systems and resources.

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 and federal laws, legal agreement, or Board policies, including, but not limited to, Board policy GCA(Legal).

Confidentiality
The security objective is to protect unauthorized access or view confidential recourses,objects, or data.

Control
Security controls are safeguards 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 state-specific implementation guidance for alignment with the National Institute of Standards and Technology (NIST) SP (Special Publication) 800-53 security controls.

Custodian
See Data Custodian.

Data Custodian

A Data Custodian is a Collin College employee with operational or technical responsibilityfor institutional data. This person usually has administrative or root equivalent access to the data and is accountable to the Data Owner.

Data Owner(s)

A Data Owner is a Collin College employee designated as accountable for specific institutional data. The Data Owner has administrative control over the dataset and is usually themost senior divisional officer. Data Owners are defined for these ISPs, but Collin College remains the owner of data maintained, stored, or transmitted on and through CC's information technology resources.

Department of DIR

The Texas 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

Any process used to convey a message or exchange data or 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 ciphertext using a variable called a "key" and processing those items through a fixed algorithm creates the encrypted text concealing the data's original meaning.

Guideline

Recommended, non-mandatory controls 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 have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause 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 substantial financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or life-threatening injuries.

Information

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

Information Resources

Defined in §2054.003(7), Texas Government Code, information resources are the procedures, equipment and software deployed, 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

Defined in §2054.003(8), Texas Government Code, information resources technologies are data processing and telecommunications hardware, software, services, supplies, personnel, facility resources, maintenance, and training.

Information Resources Manager

Defined in §2054.071, Texas Government Code, the information resource manager (IRM) is a senior official who oversees the acquisition and use of information technology. This person ensures that all information resources are acquired appropriately, implemented effectively, and compliantwith relevant regulations and ISPs.

Information Security Plan

The information security plan comprises the ISPs, 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

The information system is related to information resources under the same direct management 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 of guarding against unauthorized changes ensures the data is correct and reliable.

ITCHE

Information Technology Council for Higher Education.

Low Impact Information Resources

Information resources, whose loss of confidentiality, integrity, or availability, could have a limited adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

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

Moderate Impact Information Resources

Information Resources whose loss of confidentiality, integrity, or availability could have a moderate adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

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

Network Security Operations Center (NSOC)

As defined in §2059.001, Texas Government Code.

Personal Identifying Information (PII)

A piece of personal identity information as defined by §521.002(a)(1), Business and Commerce Code.

Procedure

Procedures are instructions to assist information security staff, custodians, and users in implementing ISPs, standards, and guidelines.

Residual Risk

The risk remains after security controls have been applied.

Risk

Risk defined in NIST 800-137 measures the extent to which a potential circumstance or event threatens an entity, and typically a function of (i) the adverse impacts that wouldarise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Assessment

Risk Assessment, defined in NIST 800-137, is the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation resulting from the operation of an information system.

Risk Management

Risk Management, defined in NIST 800-137, is the program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined, and (iv) monitoring risk over time.

Security Incident

A security incident defined in NIST 800-137 is an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of a breach of security policies, security procedures, or acceptable use policies.

Sensitive Personal Information

A piece of personal identity information as defined by §521.002(a)(2), Business andCommerce Code.

Standard

Standard defined in NIST 800-66 is a rule, condition, or requirement: (1) Describing the following information for products, systems, services, or practices: (i) Classification of components. (ii) Specification of materials, performance, or operations; or (iii) Delineation of procedures; or (2) Concerning the privacy of individually identifiable health information.

Threat

Threat is defined in NIST 800-30 as any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, or denial of service.

User

A user is defined in NIST 800-66 as a person or entity with authorized access.

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.

Implementation Information

Review Frequency:	Annually
Responsible Person:	SVP – Campus Operations
Approved By:	Abe Johnson, Ed. D.
Approval Date:	02/09/2022

Revision History

Version:	Date:	Description:
1.0	02/09/2022	Initial document
1.1	10/28/2022	Annual Review – No Changes required.
1.2	11/07/2023	Annual Review – Minor Title Changes