ACC Alvin Community College	**ADMINISTRATIVE PROCEDURE MANUAL**	
Section Title: **Information Security Program**	Number: cs-01	Page: 1 of 18
BASED ON BOARD OF REGENTS POLICY		
Policy Title: **INFORMATION SECURITY**	Policy Number: CS	
Local	Date Adopted by ELT: 12/12/17	

Purpose

The purpose of this document is to provide the structure of the Information Security Program for Alvin Community College.

1. Background

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* ". Current regulations do not require ACC to maintain compliance with TAC§202. However, TAC§202 defines an outstanding security program that follows closely with the federal requirements defined in NIST 800-53. Following these codes will provide security for the college's important data. The guidelines established in this statute will ensure that ACC data is compliant with current state and federal regulations and will prepare ACC for future compliance requirements by the THECB.

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, as well as to assure the availability, integrity, utility, authenticity, and confidentiality of information. Unauthorized modification, deletion, or disclosure of information technology resources can compromise the mission of ACC, violate individual privacy rights, and possibly constitute a criminal act (TAC§202.70).

The purpose of the ACC Information Security Program is to provide the college community with a description of the college standards for information security. The Information Security Program process combines multiple security elements into a management framework that supports the objectives of confidentiality, integrity, and availability. Additionally, the framework of this plan is designed to document the controls used to meet the information security program objectives by:

- Identifying system data owners, providing the data classification standard and identifying 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, standards, and procedures.
- Creating a security effectiveness report to the president.
- Reviewing the current process and implement changes as necessary.

The ACC 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.

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

a. Authority

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

2. Scope

This program applies equally to all individuals granted access privileges to any Alvin Community College information technology resource, to include the following:

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

3. Information Security Roles and Responsibilities

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

a. Data Owner

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

- classifying information under their authority, with the concurrence of the ACC President or his/her designated representative(s), in accordance with ACC's established information classification categories;
- approving access to information resources and periodically review 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;
- providing 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 ACC information security officer; and
- participating in risk assessments as provided under §202.75 of the Texas Administrative Code.

i. **ACC Data Owners:** Data Owner roles are defined in Appendix A of this document.

b. Data Custodian

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

- 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 ACC 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 information is recoverable in accordance with risk management decisions.

i. **ACC Data Custodians:** Data Custodian roles are defined in Appendix A of this document.

c. Users

The user of an information resource has the responsibility to:

- use the resource only for the purpose specified by ACC or 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 ACC President or his/her designated representative.

d. Public Use of ACC systems (Guest on campus)

ACC 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 prior to use.

4. Roles and Responsibilities

a. College President

The president of Alvin Community College, as the institution head, is ultimately responsible for the security of the information resources. The president or his/her designated representative shall:

- designate an Information Security Officer (ISO) 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 ACC 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 ACC has trained personnel to assist the college in complying with the requirements of this program and related policies;
- ensure that ACC senior officials support the ISO in developing, at least annually, a report on the ACC 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 ACC 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 and operational processes and policies.

b. Information Security Officer (ISO)

Alvin Community 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:

- developing and maintaining a college-wide information security plan as required by §2054.133, Texas Government Code;
- developing and maintaining information security policies, standards 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 with respect to such responsibilities;
- providing guidance and assistance to ACC senior officials, data owners, data custodians, and end users concerning their responsibilities under this program;
- ensuring that annual information security risk assessments are performed and

documented by data owners;

- reviewing the ACC inventory of information systems and related ownership and responsibilities;
- developing and recommending policies and standards, establishing procedures and practices, in cooperation with the ACC Information Resources Manager, 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, and/or share confidential data;
- 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;
- reporting, at least annually, to the ACC President the status and effectiveness of security controls; and
- informing the parties in the event of noncompliance with this chapter and/or with ACC's information security policies and standards.

The Information Security Officer, with the approval of the ACC 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.

i. **ISO Role Assignment:** The roles and responsibilities of the Information Security Officer are assigned to the Network Security Administrator.

c. Information Resources Manager (IRM)

The ACC 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 information resources management activities, provide for greater coordination of ACC'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 ACC 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.

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

  - a senior official within the organization,
  - reports directly to a person with a title functionally equivalent to executive director or deputy executive director, and
  - has been vested with the authority necessary to fulfill his/her duties as the

Information Resources Manager.

ii. Statutory IRM Responsibilities

Per the Information Resources Management Act, the IRM will:

- oversee the Biennial Operation Plan (BOP) preparation, subject to instructions from the Legislative Budget Board (LBB);
- provide input into the Alvin Community College Five Year Strategic Plan;
- comply with IRM continuing education requirements provided by DIR;
- oversee the implementation of the organization’s project management practices; and
- demonstrate in the organization’s strategic plan the extent to which the organization uses its project management practices.

iii. Other IRM Responsibilities

Other IRM responsibilities for this organization include

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

iv. The roles and responsibilities of the Information Resources Manger are assigned to the Director, Information Technology.

5. Program Framework

This section defines the Information Security Program elements that will ensure the continuity, performance and security of ACC's information systems. This framework is based on the main objective of the information security program: confidentiality, integrity, and availability.

The following elements are designed to create a framework for the information security program (ISP), help Alvin Community College adopt a controls catalog, and comply with Texas Administrative Code (TAC). The description of each element includes a definition, description of primary activities, and assignment of responsibility.

The elements of the information security program are:

- Asset / Data Classification
- Risk Assessment and Management
- Identity and Access management
- Disaster Recovery / Business Continuity Plan
- Incident Response
- Security awareness training
- Physical Security
- Required Controls (DIR Security Controls Catalog)

a. Asset / Data Classification

An inventory of information systems assets is required. These include critical networking assets, high value systems, and all locations of confidential and sensitive data at rest and in transit. Each year, the assigned data owners and their selected data custodians will be reviewed by the IRM and the ISO. The data owners will review and/or identify their datasets and identify the categories of data stored as confidential, protected or public according to the Data Classification Standard. 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 to include personnel, equipment, hardware and software, as well as define information classification categories. (TAC§202.72(1A) (2A)).

Activity Description	Assigned Responsibility
Inventory of systems, data owners, data custodians	ISO
Periodic review of access and authorization granted	Data Owners
Develop and maintain data classification standard	ISO
Develop and maintain applicable control standards	ISO
Classify data	Data owner

Implement Controls	Data custodians
Respond to audits and inquiries	Data owners and custodians
Acknowledge policies and confidentiality	Authorized users

b. Risk Assessment and Management

Data risk management is the process of aligning information resource risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures. The risk management cycle includes assessment, review, mitigation and reporting. It includes the following activities:

i. Risk assessment is the process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. 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’, ‘moderate’, or ‘low’ based on TAC§202.75 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 as a result of evaluating the information collected.

ii. Risk review is the process of evaluating the results of risk assessments and recommending activities to mitigate the risks.

iii. Risk mitigations are technical and/or procedural activities designed to reduce or eliminate the risks identified during assessment and review.

iv. Risk reporting is the process of reporting residual risks to the President and executive administration.

Activity Description	Assigned Responsibility
Coordinate risk assessment activities	ISO
Participate in risk assessment	Data owners and custodians
Review assessment results and recommend remediation requirements	ISO
Mitigate identified risks	Data custodians

Grant exemptions to controls requirements based on risk assessments	ISO, IRM
Residual risk reporting	ISO

c. Identity & Access Management

Identity and access management ensures accurate identification of authorized users and provides secure authorized access to the use of information resources. The purpose of identity management is to:

- ensure unique identification of users;
- assign access privileges based on identity; and
- maintain effective identity mechanisms through evolving technologies and regulations.

Access control refers to the process of controlling access to systems, networks, and information based on business and security requirements. The objective is to prevent unauthorized disclosure of Alvin Community College's information assets. Access control measures include secure and accountable means of identification, authentication and authorization. These measures include the following:

- assign access privileges to authenticated users;
- allow user access to information resources granted only by authorized individuals;
- ensure periodic review of users and their access; and
- maintain effective access mechanisms through evolving technologies and regulations.

Activity Description	Assigned Responsibility
IAM technology standards development and maintenance	IRM or designee
IAM procedure development and maintenance	IRM or designee

d. Disaster Recovery/Business Continuity Plan

ACC Information Technology Services (ACC-ITS) is responsible for developing and maintaining a Business Continuity Plan (BCP) designed to address the operational restoration of ACC'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 ACC to resume the minimum required levels of essential services. The plan is located in strategic areas and available to all Information 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 ACC-ITS Business Continuity Plan described above does not address the needs of individual departments beyond the restoration of 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 catastrophic.

Activity Description	Assigned Responsibility
Develop and maintain BCP	ISO, Data custodians
Develop and maintain applicable standards, process, and procedures	ISO, Data custodians
Coordinate Distribution of BCP	ISO
Mitigate identified risks	Data custodians
Implement and test BCP	IRM or designee

e. Incident Response

An information security incident is defined as an event that impacts or has the potential to impact the confidentiality, availability or integrity of ACC information resources. Having an effective incident response plan is essential in mitigating damage and loss. Proper handling of such incidents protects Alvin Community College's information resources from future unauthorized access, misuse or damage.

Activity Description	Assigned Responsibility
Develop and maintain incident response standard	ISO
Coordinate incident response activities	ISO
Develop and maintain incident response plan	ISO
Develop and maintain incident response procedures for: • Incident management • User reporting • State reporting (TAC§202.73)	ISO

f. Security Awareness Training

All employees with access to the ACC information technology resources must participate in information security awareness training (TAC§202.71(b)(4)).

The training promotes awareness of:

- ACC 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 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 college executive management are responsible for and will be provided status of training compliance.

Activity Description	Assigned Responsibility
Maintain and operate an ongoing security awareness program	ISO
Coordinate development and effective maintenance of communication and internal marketing strategies for information security awareness	ISO
Participate in security awareness program	All users

g. Physical Security

Physical security controls and secure areas are used to minimize unauthorized access, damage, and interference to information resources. This includes providing environmental safeguards and controlling physical access to equipment and ACC data consistent with TAC and State Office of Risk Management rules and guidelines.

Activity Description	Assigned Responsibility
Develop and maintain physical security standards and procedures	IRM or designee
Implement physical security procedures	Data custodians

h. Required Controls (DIR Security Controls Catalog)

Defined controls provide a system of checks and balances intended to identify irregularities, prevent abuse from occurring, and assist in resolving discrepancies that are introduced into the operation of the business. Control activities and mechanisms help ensure remediation requirements are carried out to reduce risks identified during the risk assessment process.

The Texas Department of Information Resources (DIR) has published a Security Controls Standards Catalog (SCSC) for the purpose of providing state agencies and higher education institutions specific guidance for implementing security controls in a format that easily aligns with the National Institute of Standards and Technology Special Publication 800-53 Version 4 (NIST SP 800-53 Rev. 4). The control catalog specifies the minimum information security requirements that state organizations must use to provide the appropriate levels of information security according to risk levels. (TAC§202.74)

Activity Description	Assigned Responsibility
Develop and maintain information security plan that tracks adoption of appropriate security controls	ISO

Report effectiveness of security controls	ISO
Submit information security plan to DIR biennially	ISO
Coordinate data security control requirements with the data owners and convey them to data custodians	ISO
Implement controls	Data custodians

i. 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 ACC IT Policies and standards. The ISO and IRM will report the status and effectiveness of ACC's information security controls and will present recommended revisions and improvements based on the information collected (TAC§202.73).

The report will include:

- Description and/or narrative of any security incident that resulted in a significant impact to the university.
- Status of the Risk Assessments noting any significant changes.
- Status of the Vulnerability Assessments noting any major findings and corrections.
- Status of the IT Information Security Program review.
- Status of the IT Security Awareness Training Program.
- Anticipated changes in the next fiscal year.

6. Compliance References

ACC's information security practices must comply with a variety of federal and state laws, as well as ACC 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.

There are many individual laws, regulations, and policies that 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 ACC's information technology resources are listed below.

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

Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of ACC's information technology resources.

- Texas State University System Rules and Regulations
- The Federal Family Educational Rights and Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Federal Information Security Management Act (FISMA)
- Texas Administrative Code, Title 1, part 10, Chapter 202, Subchapter C
- Security Controls Standards Catalog published by Texas Department of Information Resources
- Texas Administrative Code, Title 1, part 10, Chapter 203
- Texas Government Code, Chapter 2054 – Information Resources
- Texas Government Code, Chapter 2059 – Texas Computer Network Security System
- Texas Business and Commerce Code, Chapter 521 – Unauthorized Use of Identifying Information
- Texas Penal Code, Chapter 33 – Computer Crimes
- Digital Millennium Copyright Act
- Copyright Act of 1976

7. Failure to Comply (Enforcement)

Consistent with ACC policies, the ISO is authorized by the ACC 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 program 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, a written request for exception must be approved by the ISO. Approved requests will be reviewed annually to determine if an exception is still warranted.

ACC 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 in order to protect the confidentiality, integrity, availability or functionality of ACC information technology resources; to protect ACC from liability; or to enforce this program and its related standards and practices.

Failure to adhere to the provisions of this program may result in:

- suspension or loss of access to ACC 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 in a manner consistent with applicable laws and regulations, and ACC 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 in accordance with 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 ACC.
Appeals of college actions resulting from enforcement of this program will be handled through existing disciplinary/grievance processes for ACC students and employees.

a. Obtaining a Program Exemption

Exemptions to policies are granted on a case-by-case basis and must be reviewed and approved by the college designated IRM. The IRM will mandate the documentation and additional administrative approvals required for consideration of each program exemption request. TAC§202.71(c).

8. Definitions

Alphabetized listing of both common and specific terms that are used in this Information Security Program. The words and terms, when used in this program, shall have the following meanings, unless the context clearly indicates otherwise.

Access
The physical or logical capability to view, interact with, or otherwise make use of 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 of ensuring timely and reliable access to and use of information.

Cloud Computing
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 agreement.

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

Control
A safeguard or protective action, device, , 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 that 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 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, organizational 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 major damage to organizational assets;
- result in major financial loss; or
- result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

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

Information Custodian
A department, agency, or third-party service provider 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 that are 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 who 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 common functionality. An Information System normally includes, but is not limited to, hardware, software, network Infrastructure, information, applications, communications and people.

Integrity
The security objective of guarding 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 loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational

assets, or individuals. Such an event could:

- cause a degradation in mission capability to an extent and duration that the organization is able to 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 loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. Such an event could:

- cause a significant degradation in mission capability to an extent and duration that the organization is able to 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 as 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 level of 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 provided by planned or in-place security controls.

Risk Management
The process of aligning information resources risk exposure with the organization's risk tolerance by either accepting, transferring, or mitigating risk exposures.

Security Incident
An event which results in the 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 as defined by §521.002(a)(2), Business and Commerce Code.

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

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 in accordance with federal and state law, agency , and the information-owner's procedures and rules.

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

ACC ALVIN COMMUNITY COLLEGE	**ADMINISTRATIVE PROCEDURE MANUAL**	
Section Title: **Information Security Program** **Appendix A – Data Owners and Custodians**	Number: CS-01	Page: 1 of 18
BASED ON BOARD OF REGENTS POLICY		
Policy Title: **Information Security**	Policy Number: CS	
Local	Date Adopted:	

Data Owners

ACC Position (Pending ELT Approval)	**Department**	**Data**	**Name**
Vice President, Administrative Services	Administrative Services	Colleague – CF, ST, CORE, UT All Administrative Services “S: Drive” Data	**Karl Stager**
Director, Fiscal Affairs, Business Office	Administrative Services	Colleague – CF Fiscal Affairs “S: Drive” data	Deborah Kraft
Director, Purchasing	Administrative Services	Colleague – CF:PU Purchasing “S: Drive” data	Randi Faust
Director, IT	Administrative Services	Colleague – CORE Colleague – other misc modules IT “S: Drive” data	Kelly Klimpt
Vice President, Instruction	Instruction	All Instruction Data Instruction “S: Drive” Data	**Cynthia Griffith**
Vice President, Student	Student Services	Colleague – ST	**Marilyn Dement**

Services		Student Services “S: Drive” Data	
Registrar	Student Services	Colleague – ST Enrollment	Irene Robinson
Director, Financial Aid	Student Services	Colleague ST – FA	Dora Sims
Executive Director, Human Resources	Human Resources	Colleague – HR Human Resources “S: Drive” data	**Karen Edwards**
Executive Director, Continuing Education & Workforce Development	Continuing Education / Workforce Development	Colleague – ST: XCE CE “S: Drive” data	**James Simpson**

Data Custodians

ACC Position	**Department**	**Data**	**Name**
Director, Information Technology	Information Technology	Colleague All Non-ERP data	Kelly Klimpt
Network Manager	Information Technology	All Non-ERP data Non-ERP Hardware All File Shares	Steve Cabrera
Senior Programmer	Information Technology	Colleague	Benjamin Deadwyler
Database Administrator	Information Technology	ERP Hardware Colleague	Frederick Bellows