Procedure III.3010.A.a, Information Security Program

Associated Policy
Policy III.3010.A, Information Resources

1. Purpose

The College's Information Resources are vital academic and administrative assets that require appropriate safeguards. Computer systems, networks, and data are vulnerable to ever increasing cybersecurity threats. These threats have the potential to perpetrate financial fraud and compromise the integrity, availability, and confidentiality of the information used by the College to conduct its day-to-day business. To combat these threats, Federal and State Laws require the College to take measures to protect Information Resources against unauthorized access, disclosure, modification, or destruction, whether accidental or deliberate. This Procedure describes these requirements and expected responsibilities of the College and serves as a master Procedure to be referenced by other Procedures under the associated policy.

2. Applicability

This Procedure applies to all Users of Information Resources, in any form, and is intended to be broad enough to include all Users.

3. Laws, Regulations, and Standards

The College is required to comply with Federal and Texas State Laws and Regulations. In the 86th legislative session, the Texas Legislature enacted policy that requires the College to designate an Information Security Officer (ISO) and comply with state information security standards, shared services, and projects, including mandatory cybersecurity training for elected officials, employees, and contractors. Furthermore, in the 87th legislative session, the Texas Legislature enacted policy that requires the College to designate a Data Management Officer (DMO) to establish a data governance program to identify data assets, establish processes and Procedures to oversee the College's data assets, and implement practices and controls for managing and securing the College's data.

The NIST Cyber Security Framework (CSF) is an overarching standard used to implement Federal and State Laws and Regulations and is defined by the National Institute of Standards and Technology (NIST) within the U.S. Department of Commerce. To implement Texas state requirements, the College is required to comply with the standards defined by Texas Administrative Code §202 (TAC 202).

Texas state requirements should satisfy other Federal Laws and Regulations given that Texas Department of Information Resources (Texas DIR) control standards are based on NIST 800-53 standards.

4. Texas State Information Security Program

Pursuant to Texas State Laws, the College is required to adopt the state's Information Security Program that establishes formal cybersecurity governance, testing, controls, enforcement, and regular assessment and reporting to Texas DIR.

5. Program Governance

Described below are the roles and responsibilities as defined by the Information Security Program.

a. **Chancellor.** The Chancellor is responsible for the security measures that protect the College's Information Resources.

b. **Designee.** The Designee is the executive that oversees the implementation and adoption of the Information Security Program. The Designee appointed by the Chancellor is the College's Chief Technology Information Officer (CTIO).

c. **Information Security Officer (CISO).** The CISO is the College's Chief Information Security Officer who reports to the Designee and is the executive authorized with explicit authority to administer the information security requirements under Texas Law, as designated by the Chancellor. The CISO coordinates with Texas DIR, the College's Data Management Officer (DMO), and with the College's leadership, employees, students, Vendors, and other third parties as defined by TAC 202.72. CISO responsibilities are outlined in TAC202.21.

d. **Data Management Officer (DMO).** The DMO reports to the Designee and is responsible for the College's Information Security Assessment Report and implementing data management governance, processes, and controls. The DMO is regarded as the Information Resource Manager (IRM). The IRM is the executive responsible for Information Resources across the whole of the institution as defined in Chapter 2054, Subchapter D, Texas Government Code. The DMO coordinates with the College's ISO, the College's Records Management Officer (RMO), the Texas State Chief Data Officer, the State Library and Archives Commission, and with the College's leadership, employees, students, Vendors, and other third parties.

e. **Strategic Leadership Team (SLT).** The SLT is the College's executive steering committee. The SLT is required to evaluate and recommend approval to the Chancellor of the Annual Program Review, risk acceptance, and any changes to controls that are escalated to the SLT.

6. Data Governance

The DMO shall establish data governance and controls at the College. The DMO shall design and develop classifications of data produced by the College's Technology Resources and determine appropriate data security requirements and applicable record retention schedules as outlined in Texas Government Code Section 441.185 for each classification.

7. Program Controls

The CISO shall design and develop processes and controls to ensure that the Information Security Program is adopted at the College. The Information Security Program shall establish appropriate security controls to protect the confidentiality, integrity, and availability of College's Information

Resources. These controls shall be based upon the NIST Cyber Security Framework (CSF), and in accordance with respective laws, regulation, and compliance requirements. Documentation of the College's Information Security Program Controls as required by Policy III.3010.A, Information Resources.

7.1 Mandatory Controls

Texas Administrative Code 202 mandatory security controls shall be defined by Texas DIR in the Security Controls Standards Catalog (DIR CC). The controls shall include minimum information security requirements for all state information and information systems and standards to be used by all institutions of higher education to provide levels of information security according to risk levels. The mandatory control families implemented at the College are as follows:

AC Access Control
AT Awareness and Training
AU Accountability, Audit, and Risk Management
CA Security Assessment and Authorization
CM Configuration Management
CP Contingency Planning
IA Identification and Authentication
IR Incident Response
MA Maintenance
MP Media Protection
PE Physical and Environmental Protection
PL Planning
PM Program Management
PS Personnel Security
RA Risk Assessment
SA System and Service Acquisition
SC System and Communication Protection
SI System and Information Integrity
SR Supply Chain Risk Management

7.2 Optional Controls

The Chancellor or Designee may employ standards for the cost-effective information security of information and information resources within or under the supervision of the College that are more stringent than the standards Texas DIR prescribes if the more stringent standards:

a. Contain at least the applicable standards issued by Texas DIR; and

b. Are consistent with applicable Federal Law, policies, and guidelines issued under Texas state rule, industry standards, best practices, or are deemed necessary based on a Risk Assessment to adequately protect the information held by the institution of higher education.

8. Enforcement

The Chancellor shall designate responsibility for enforcing this Procedure as described by College policies and procedures. Compliance with this Procedure and Program Controls shall be strictly enforced. Violations may result in disciplinary action, up to and including termination. Violations of Federal State or Local Laws may also result in criminal prosecution.

Information Resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under Federal and State Laws. Moreover, attempting to circumvent security or administrative access controls for Information Resources and/or assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of College Policy and this Procedure.

Violations of this Procedure and applicable guidelines shall be immediately reported to the CISO and or Technical Support.

9. Regular Program Reviews

The College's Information Security Program is expected to be continually updated given the evolving maturity level of the program's adoption at the College and the ever-changing cybersecurity threat landscape. As such, the College is required to perform regular reviews of its program.

a. **Annual Program Review and Approval**. The Designee shall annually review no later than June 1 of each year with the Chancellor and Strategic Leadership Team (SLT) an Information Security Program in accordance with Texas State Law by the CISO designed to address the security of the Information Resources owned, leased, or under the custodianship of the College against unauthorized or accidental modification, destruction, or disclosure. The program shall include processes for risk management and for information security awareness education for employees when hired, and an ongoing program for all Users.

b. **Biennial Program Review**. In addition to the Annual Program Review, the Information Security Program must be reviewed biennially by an individual who is independent of the program to determine if the program complies with the mandatory security controls defined by Texas DIR and any controls developed by the College in accordance with Texas Law. A review of the College's Information Security Program for compliance with these standards will be performed at least biennially, based on business risk management decisions, by individual(s) independent of the information security program and as designated by the Chancellor or designated representative(s).

10. Regular Testing of Online and Mobile Applications

The College shall adopt processes addressing the privacy and security of the College's internet-facing technology resources, websites, and mobile applications. The Information Resource Custodian shall subject the website or application to a vulnerability and/or penetration test and address any vulnerability identified in the test before deployment and mitigate according to the College's risk management procedures. Ongoing vulnerability tests will be conducted as described by the RA Risk Assessment control family in DIR's CC.

11. Texas State Cloud Computing State Risk and Authorization Management Program

The College shall require each Vendor contracting with the agency to provide cloud computing services for the agency to comply with the requirements of the state risk and authorization management program. A state agency shall require a vendor contracting with the agency to provide cloud computing services for the agency that are subject to the state risk and authorization management program to maintain program compliance and certification throughout the term of the contract.

12. Reporting

Federal and Texas State Laws require the College to submit regular and ad-hoc reports to Texas DIR and other Federal Departments and Agencies. These reports are outlined below:

a. **Information Security Plan**. Not later than June 1 of each even-numbered year the CISO shall submit an Information Security Plan on behalf of the College to Texas DIR in accordance with Texas Law.

b. **Incident Report**. The CISO shall assess the significance of a security incident and, if applicable, report urgent incidents to the CTIO, Federal Departments or Agencies, Texas DIR, and law enforcement as required by Federal, Texas State, and Local Laws. Furthermore, The College shall include within any Vendor or third-party contract the requirement that the Vendor or third-party report information security incidents to the College in accordance with the College's Policies and Procedures and as required by Federal and Texas State Laws.

c. **Security Breach Notification**. Upon discovering or receiving notification of a breach of system security, the CISO shall assess the significance of the breach and report the breach to the CTIO. Depending on the severity of the breach, the College shall disclose the breach to affected persons or entities in accordance with the time frames established by Federal and State Laws. The College shall give notice by using one or more of the following methods:

   - Written notice.
   - Electronic mail if the College has electronic mail addresses for the affected persons.
   - Conspicuous posting on the College District's website.
   - Publication through broadcast media.

13. Expected User Responsibilities

It is the shared responsibility of all Users to comply with designated security controls, programs, guidelines, and practices to ensure the confidentiality, integrity, and availability of College Information Resources. Information Resource Owners, Information Resource Custodians, and other Users of Information Resources shall, in consultation with the College's CTIO, CISO, and DMO be identified, and their responsibilities defined and documented by the College. The distinctions below among Information Resource Owners, Information Resource Custodians, and other Users should guide determination of these roles.

a. **Information Resource Owner (IRO)** is a role assigned by Texas Administrative Code (TAC) 202.72 to Users who are College leaders and designated employees either responsible for the business function that is supported by the Information Resource or whom responsibility rests for carrying out the program that uses the resources. Furthermore, the Owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared. The owner or his or her designated representative(s) are responsible for:

- Classifying information under their authority, with the concurrence of the Chancellor or designee(s), in accordance with the College District'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.
- Providing authority to custodians to implement security controls and processes.
- 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 institution of higher education information security officer.
- Participating in risk assessments as provided under Texas Administrative Code 202.75.
- The IRO coordinates with the College's ISO, DMO or their delegates to ensure that processes are documented and implemented as required by Texas State Laws.

b. **Information Custodian (IC)** is a User who is an employee, department, other institution, third party agent acting on behalf of the College, or Vendor responsible for supporting and implementing Information Resource controls as defined by the IRO. Custodians include information security administrators, institutional Information Technology Services/Systems departments, faculty or staff, vendors, and any third-party acting as an agent of or otherwise on behalf of the College. Custodians of information resources, including third-party entities providing outsourced information resources services to the College District, shall:

- Implement controls required to protect information and information resources required by this chapter based on the classification and risks specified by the information owner(s) or as specified by the Policies, Procedures, and standards defined by the College District's security program.
- Provide owners with information to evaluate the cost-effectiveness of controls and monitoring.
- Adhere to monitoring techniques and processes, 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.

c. **Information Resource User** is a User of Information Resources and has the responsibility to:

- Use the resource only for the purpose specified by the institution or Information-Owner

- Comply with information security controls and institutional policies to prevent unauthorized or accidental disclosure, modification, or destruction.
- Formally acknowledge that they will comply with the College Information Resource Policy and Procedures in a method determined by the institution head or their designated representative.
- College Information Resources designated for use by the public shall be configured to enforce the College's Information Resource Policy and Procedures without requiring user participation or intervention. Information Resources must require the acceptance of a banner or notice prior to use.

14. Definitions

This section includes a list of terms referenced in this and other Procedures associated with Policy III.3010.A, Information Resources.

Availability: means ensuring timely and reliable access to and use of information.

Breach (or suspected breach): means an unauthorized acquisition of data that compromises the security, confidentiality, or integrity of sensitive personal information maintained by a person, including data that is encrypted if the person accessing the data has the key required to decrypt the data. As defined by Texas Business and Commerce Code Section 521.053. Good faith acquisition of sensitive personal information by an employee or agent of the person for the purposes of the person is not a breach of system security unless the person uses or discloses the sensitive personal information in an unauthorized manner.

Cardholder: Individual who owns and benefits from the use of a membership card, particularly a payment card.

Cardholder Data (CHD): Elements of payment card information that must be protected including primary account number (PAN), cardholder name, expiration date, and the service code.

Cardholder Name: The name of the individual to whom the card is issued.

CAV2, CVC2, CID, or CVV2 data: The three- or four-digit value is printed on or to the right of the signature panel or on the face of a payment card and is used to verify card-not-present transactions.

College: means San Jacinto College District.

College Business: means activities that include teaching, learning, administration, safety, maintenance, business development, support, and project services.

Confidentiality: means reserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Confidential Data: means data that is collected and maintained by an agency that must be protected against unauthorized disclosure and is not subject to public disclosure under the provisions of applicable Federal and State Laws.

Cybersecurity Governance, Risk Management, and Compliance (GRC) Team: means individuals who are knowledgeable about the organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, technical security controls, and who are responsible for the Cybersecurity Risk Management processes and procedures.

Data: means elemental units, regardless of form or media, includes both digital and physical, that are combined to create information used to conduct College business. Data may include but are not limited to physical media, digital, video, and audio records, photographs, and negatives.

Digital Content: means Data that is digital that includes information, data files, image files, video files, templates, project files, software code, and other digital products stored and made available through Technology Resources, along with any related materials, modifications, and updates, if any, provided by Licensor to the User and or the College.

Disposal: means the disposal of data in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media, including computers, hard drives, magnetic tapes, and USB storage devices, in accordance with Procedure III.3001.J.a, Records Management. The approved PCI DSS disposal methods include cross-cut shredding, incineration, and approved shredding and disposal service. Records may not be destroyed prior to authorized disposal date.

Electronic Protected Health Information (ePHI): means any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

Event: means an identified issue, alert, or error which resulted in no adverse effect on an asset or user. For example, an event can be a user who receives a phishing email but does not click on any link, reply or execute an attachment.

Expiration Date: means the date on which a card expires and is no longer valid. The expiration date is embossed, encoded, or printed on the card.

Federal Law(s): means federal privacy, information, and other data protection laws including, but not limited to, the Family Educational Rights and Privacy Act (FERPA), Gram-Leach-Bliley Act (GLBA), Personal Credit Information (PCI), Health Insurance Portability and Accountability Act (HIPAA), and Children's Online Privacy Protection Act (COPPA).

Information Resources: means the collective of the College's Technology Resources, Protected Data, and Digital Content. This is the term used in Texas Law.

Information Systems: means an interconnected set of Information Resources under the same direct management control that shares common functionality. An Information System normally includes hardware, software, Network Infrastructure, information, data, applications, communications, and people.

Information Technology Services (ITS): means the department within the College responsible for the delivery, support, and security of Technology Resources.

Information User(s): means employees, contractors, third parties, and or any individual provided privileged access to Protected Data.

Integrity: means the accuracy and completeness of information and assets, and the authenticity of transactions. information.

License Agreement(s): means a legal contract between the licensor and the purchaser of a software or service which establishes the purchaser's rights to use the software. A license agreement details how and when the software or service can be used and provides any User restrictions imposed on the software by the licensor. A license agreement also defines and protects the rights of both parties. In general, the College licenses software and services on behalf of College Users and College Users are bound to the terms and conditions of the license agreement.

Magnetic Stripe Data: means data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.

Merchant: means a department(s) or unit(s) approved to accept payment cards and are assigned a merchant identification number.

NPI: means non-public personal information that is (1) provided by a consumer to a financial institution, (2) resulting from any transaction with the consumer or any service performed for the consumer, or (3) otherwise obtained by the financial institution.

Office of Cybersecurity (OCS): means the department within the College that provides data security services, vendor evaluation, (IR) incident response, and GRC compliance efforts. OCS drives the cybersecurity maturity of the College.

Payment Card Industry Data Security Standard (PCI DSS): means regulations as administered by the Payment Card Industry Security Standards Council (PCI SSC) to decrease payment card fraud across the internet and increase payment card data security. This includes sensitive data that is presented on a card or stored on a card, and personal identification numbers entered by the cardholder.

Personal Device(s): means devices, operating systems, software, hardware, systems, and services that are owned by the User. Includes but not limited to personal computing devices such as smartphones, tablets, and laptops; personal Internet Service Providers (ISP); mobile applications and software; storage devices such as USB drives; access to digital resources and services made available by any third-party platforms such as Google Drive and Dropbox; personal communications systems such as phone, email, text, instant messaging, and other collaboration tools.

Personal Identifying Information (PII): means any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information:

- That directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or
- By which the College intends to identify specific individuals in conjunction with other data elements, such as indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors. Additionally, information permitting the physical or online contacting of a specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

PII includes the first name or first initial and last name in combination with and linked to any one or more of the following data elements about an individual:

- Social security number
- Driver's license number or state identification card number issued in lieu of a driver's license number
- Passport number
- Financial account numbers, and/or credit card or debit card number
- Academic records
- Financial records
- Medical Records
- Disciplinary records
- Placement office records
- Personal names
- Address
- Telephone and fax numbers
- Electronic mail addresses
- Dates directly related to an individual, including birth date, admission date, discharge date, date of death
- Medical record numbers
- Health plan beneficiary numbers
- Full face photographic images and any comparable images

PII can also be reidentified in such a manner as to contain PII. The Federal Trade Commission also considers information that can reasonably be used to contact or distinguish a person as PII. This includes electronic identification such as IP addresses.

Texas Senate Bill 475 specifically prohibits the College from using, retaining, or disseminating data from global positioning system technology, individual contact tracing, or technology designed to obtain biometric identifiers to acquire information that alone or in conjunction with other information identifies an individual or the individual's location without the individual's written or electronic consent. Exceptions to this restriction include if such use, retention, and dissemination is required or permitted by a federal statute or by a Texas State statute other than Chapter 552; or made by or to a law enforcement agency for a law enforcement purpose.

PIN or PIN block: means personal identification number entered by the cardholder during a card-present transaction, or encrypted PIN block present within the transaction message.

Primary Account Number (PAN): means the number code of 14-16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account and includes a check digit as an authentication device.

Protected Data: means data that includes elemental units that include Personal Identifying Information (PII), financial, educational, and/or health-related information protected by Federal and State Laws and regulations. Subject to applicable Laws, the College also considers College email addresses as Protected Data insofar as they can be used in combination with IP address discovery, other external discovery information, or through fraudulent methods such as phishing to obtain passwords to gain unauthorized access to the College's Technology Resources which process and stores other Protected Data.

Ransomware: means a computer contaminant or lock that restricts access by an unauthorized person to a computer, computer system, or computer network or any data in a computer, computer system, or computer network under circumstances in which a person demands money, property, or a service to remove the computer contaminant or lock, restore access to the computer, computer system, computer network, or data, or otherwise remediate the impact of the computer contaminant or lock as defined by Section 22.023, Penal Code.

Risk(s): means a function of the likelihood that a threat will exploit a vulnerability and the resulting impact to the College's missions, functions, image, reputation, assets, or constituencies if such an exploit were to occur.

Risk Acceptance: means an agreement between data owner, stakeholders, and advisors that the risk is understood but due to resource constraints, the College is not able to implement security controls that mitigate or transfer the risk.

Risk Assessment: means the identification of the risks to people, processes, or technology, and determines the probability of occurrence and the resulting impact for each threat/vulnerability pair identified given the security controls in place; Prioritizes risks; and Results in recommended possible actions/controls that could mitigate, transfer, or accept the determined risk. Assessments may be Quantitative or Qualitative.

Risk Mitigation: means a process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk assessment process to satisfactory levels within an organization given its mission and available resources.

Risk Transference: means the process that prioritizes, evaluates, and leverages security controls that transfer the risk to a third party at a cost to the College.

Sensitive Data: means data that is collected and maintained by an organization that must be protected against unauthorized disclosure, except for public release under the provisions of applicable Federal or State Laws.

Security Incident: means the actual or suspected, unauthorized access, disclosure, exposure, modification, or destruction of sensitive personal information, confidential information, or other information the disclosure of which is regulated by law, per SB 271. For example, an incident can be a compromise of a user's account, execution of malware on a College-owned asset, or a user clicking on a malicious link in a phishing email that results in the compromise of the user's account.

Sensitive Authentication Data: means additional elements of payment card information required to be protected but never stored. These include magnetic stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data, and PIN or PIN block.

Software Intake Form (SIF) Self-Assessment Questionnaire: means a security questionnaire/ form used to collect information on technology and software solutions requested for use within the organization. This form is to be completed by the requestor's department and submitted to Tech Support with additional input from the vendor and ITS. This questionnaire/form intends to collect information about the security controls and technology requirements built into the technology in use or planned to be used by the department/ institution.

Service Code: means a code that tells merchant terminals and acquiring networks about usage restrictions the issuer has placed on this card, defining where the card is used and for what purposes.

Technology Resources: means identity access systems, devices, software, hardware, systems, and services that are provided by the College to the User to conduct College Business. Includes but not limited to authenticated systems access; computing devices; access to internal and external networks and Internet; business services, database and reporting systems; student Information Systems; learning management systems; access to digital resources and services made available via the Intranet and internal servers and any third-party platforms used to conduct College business such as social media accounts; communications systems such as email, instant messaging, collaborations tools, telephone systems, broadcasting systems, and other information technology tools, systems, and infrastructure. This associate term used in Texas legislation in "Information Resources Technologies".

Technical Support: means ITS Technical Support can be contacted by email at TechSupport@sjcd.edu or by phone at (281) 998-6137.

Texas State Law(s): means Texas state privacy, information, and other data protection laws including, but not limited to, Texas Senate Bill 64, House Bill 3834, Texas Senate Bill 475, Texas Identity Theft and Protection Act (TITEPA), and Texas Administrative Code Chapter 202 (TAC §202).

Threat: means the potential for a threat source to successfully exercise a particular vulnerability, intentionally or unintentionally. Threats are commonly categorized as:

> Environmental – external fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation, etc.

Human – cyber threat-actors, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism, etc.

Natural – fires, floods, electrical storms, tornados, etc.

Technological – server failure, software failure, ancillary equipment failure, etc. and environmental threats, such as power outages, hazardous material spills.

Other – explosions, medical emergencies, misuse of resources, etc.

Threat Source: means any circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental, which can impact the organization's ability to protect ePHI, financial NPI, protected cardholder data, and student education records.

Threat Action: means the method by which an attack might be carried out, such as hacking or system intrusion.

Threat Actor: means any entity, nation-state actor, or hacktivist that poses a threat or seeks to exploit a vulnerability in the College's Information Resources or Users.

Regulation(s): means standards and rules adopted by administrative agencies that govern how laws are enforced.

User(s): means an individual, automated application, or process that is authorized by the College to access an Information Resource. Includes, but is not limited to, all College students, faculty, staff, contractors, guests, departments, and any individual, application, or process that accesses and or uses the College's Information Resources.

Vendor(s): means any third-party that contracts with San Jacinto Community College District to provide goods and/or services to San Jacinto Community College District.

Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, i.e., resulting in a security breach or violation of policy.

Date of SLT Approval	February 15, 2024
Effective Date	February 15, 2024
Associated Policy	Policy III.3010.A, Information Resources
Primary Owner of Policy Associated with the Procedure	Chief Technology Innovations Officer

Secondary Owner of Policy Associated with the Procedure	Chief Information Security Officer