Procedure III.3010.A.f, Acceptable Use of Information Resources

Associated Policy

Policy III.3010.A, Information Resources

Other Associated Procedures:

Policy VI.6000.B, Confidentiality of Student Records
Policy VI-K: Policy Regarding Appropriate Use of Copyrighted Materials
Policy VI.6004.A, Compliance with Health Insurance Portability and Accountability Act (HIPAA)

1. Purpose

The purpose of this Procedure is to describe the conditions for Acceptable Use of Information Resources provided by the College to the User. The College maintains control, insofar as is practicable, over its Information Resources to ensure a secure and efficient operation of such Information Resources to support College Business and further the College's mission. In general, use of such Information Resources to conduct College Business is regarded as Acceptable Use.

2. Applicability

This Procedure applies to all Users of College Information Resources, in any form, and is intended to be broad enough to include all Users. Specific clauses applicable to a particular category of User are identified as such within this procedure.

3. Consent

The College provides Information Resources to the User for the purpose of conducting College Business. The User should read the terms of this Procedure carefully before using Information Resources. By using Information Resources, the User consents, accepts, and agrees to be bound and abide by the conditions of College Policy and this Procedure. The User understands that access to Information Resources is a privilege and not a right. With this privilege, the User is expected to properly use and protect Information Resources and respect the rights of other Users and third parties to their privacy, intellectual property, and other rights. Furthermore, the User understands that the College is a public junior college and governmental entity subject to specific Federal, State and Local Laws. The User agrees to be bound by and follow College Policy and this Procedure and all relevant Federal, State and Local Laws and Regulations. If warranted, the misuse of Information Resources and Digital Content by the User will result in the revocation of that User's access to Information Resources and may include disciplinary and or legal action. For all Users, documented acknowledgement of this Procedure is accomplished by completing San Jacinto Annual Cyber Awareness Training and/or clicking the checkbox on the Notice and Consent Banner when logging-in to the College's systems.

4. 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 comply with

state information security standards, including mandatory cybersecurity training for elected officials, employees, and contractors. Furthermore, Chapter 620 of Texas Government Code Title 6 Subtitle A provides specific guidance for the use of certain social medial applications and services. Sec.620.001(1)(A) specifies the social media service TikTok or any successor application or service developed or provided by ByteDance Limited, or an entity owned by ByteDance Limited. The College is also required to comply with Federal Laws and Regulations that include but are 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).

5. Associated Program Controls

The following Program Controls associated with this Procedure are:

PL Planning Control Family
- PL-4 Rules of Behavior
- PL-4(1) | Rules of Behavior | Social Media and External Site/Application Usage
- Restrictions

AT Awareness and Training Control Family
- AT-2 | Literacy Training and Awareness
- AT-3 | Role-Based Training
- AT-4 | Training Records

CM Configuration Management Control Family
- CM-10 | Software Usage Restrictions
- CM-11 | User-Installed Software

6. Roles and Responsibilities

The roles and responsibilities as defined by the Information Security Program are described in Procedure III.3010.A.a, Information Security Program. Described below are additional roles and responsibilities that pertain to this Procedure.

a. **Users Responsibility to Cooperate.** The User is expected to fully cooperate in any investigation of Information Resource abuse. The User agrees to follow all directives from the Chancellor or designee, whether communicated verbally, in writing, or other media.

b. **Users Responsibility to Complete Annual Cybersecurity Training Program**. Users who are elected officials, employees, and contractors that use a computer to complete their College job responsibilities are required to complete an annual cybersecurity training program as certified by Texas Department of Information Resources (Texas DIR). Such Users agree and understand that access to College Information Resources is subject to their completion of annual cybersecurity training.

7. Disclaimer of Liability

The User agrees and understands that the College shall not be liable for the User's inappropriate use of Information Resources; the User's violations of Federal, State and Local Laws and Regulations, or License Agreements; and or the User's mistakes or negligence and costs as incurred by User. Furthermore, the College shall not be responsible for ensuring the availability of Information Resources or the accuracy, age appropriateness, or usability of any information found on the Internet.

8. Privacy

The College makes no warranties or representations as it relates to the User's privacy in use of Information Resources. The User should have no general expectation of privacy when using Information Resources. The User understands the following:

a. The College routinely monitors Digital Content and Protected Data, software, and communications contained within its Information Resources.

c. Digital Content and Protected Data stored on Technology Resources and on Personal Devices used to access Information Resources to conduct College Business, such as but not limited to email, text messages, documents, or other data relating to College Business, belongs to The College insofar as allowed by Federal, State and Local Laws or Regulations.

d. While The College attempts to provide a secure environment for Information Resources, Digital Content and Protected Data, the User should be aware that the Internet and Personal Devices contain many security risks that the User may be exposed to when using Personal Devices and or accessing Information Resources when using Personal Devices. As such, the User should have no expectation of privacy when using the Internet and or Personal Devices to access Information Resources.

9. College-owned Devices and Prohibited Technologies

The use or download of Prohibited Technologies is prohibited on all College-owned devices, except where approved exceptions apply. Refer to **Procedure III.3010.A.d, Prohibited Technologies.**

a. **Personal Use of Information Resources**. The User may use Information Resources to conduct limited and reasonable personal use insofar as such use does not interfere with the User's duties and or College business or pose a security risk to the College.

b. **Personal Devices and Prohibited Technologies**. Personal Devices may be used by all College Users to conduct College Business insofar as allowed by College Policy and Procedures, Federal, State and Local Laws, Regulations, and License Agreements. The College will include security considerations to protect the College's network and data from traffic related to Prohibited Technologies. The following limitations apply to this granted use:

- Access to Information Resources when using a Personal Device is limited to Information Resources protected by Multi-factor Authentication (MFA) and defense in depth.
- Students are restricted to only use a Personal Device that is privately owned or leased by the Student or a member of the Student's immediate family or the Student's ISD or Academy.

- Users employed or contracted by the College must not install or operate Prohibited Technologies on any Personal Device that is used to conduct College Business.

The User understands and agrees that their Personal Devices and the Digital Content and any Data stored on such Personal Devices are subject to College Policies, Federal and State Laws, Regulations, and License Agreements.

10. Student Access to Information Resources

a. **Web Content Filtering.** The College considers access to Information Resources such as networks, the Internet, productivity and instructional software, and computers in lab spaces by Users who are students as an extension of the classroom environment. The College also considers all Users who are students as adults. As such, the College does not place age-based restrictions on User activities, nor does it filter web content.

b. **Dual Credit Students**. Access to College Information Resources is provided to Users who are High School students, including Minors, enrolled in any College sponsored class or program and who have been issued valid College login credentials. The College requires such Users to comply with applicable College Policies and Procedures. As such, Dual-Credit partner institutions and their students are responsible for ensuring compliance with their institution's policies and procedures.

c. **Minors not enrolled at the College.** Minors not enrolled at the College are not authorized Users of Information Resources and therefore require parent or guardian's consent to the College's Policies and this Procedure to access the College's network, computer labs or other computer use areas.

11. Unacceptable and Prohibited Use

Described as follows are activities regarded as Unacceptable and Prohibited uses of Information Resources by all Users.

a. **Unauthorized Access to Information Resources.** The User must not gain unauthorized access or enable or cause unauthorized access to Information Resources. The User with an authorized password or access to protected system accounts is prohibited from disclosing the User's password and or other forms of authentication identification, or otherwise make available protected accounts to any other User both within and outside of the College. The College will never ask for a User's username or password. Any issues discovered by the User with system security must be reported immediately to Technical Support.

b. **Unauthorized Access to Digital Content.** The User must not intentionally seek or provide information on, obtain copies of, or modify data files, programs, passwords, or other digital materials protected by Federal, State and Local Laws and Regulations, License Agreements and or belonging to other Users or third parties, without the specific, written permission from those Users or third parties.

c. **Unauthorized use of Digital Content or Data Protected by Intellectual Property and Privacy.** The User is required to comply with intellectual property and other Federal, State and

Local Laws and Regulations. The User must not use peer-to-peer file sharing networks, such as but not limited to BitTorrent and Usenet, unless such use is deemed legitimate College Business and does not violate intellectual property or other laws. Any Digital Content protected by copyright may not be copied except as specifically stipulated by the owner of the copyright in writing or otherwise permitted by copyright law. Protected Digital Content may not be copied into, from, or by using any College facility or Information Resource without a valid license or as otherwise permitted by copyright law. Unauthorized duplication, distribution, or use of someone else's intellectual property, including computing software, is prohibited.

d. **Use of College Information Resources for Personal Business.** The User must not use Information Resources for commercial purposes that are not considered College Business. The User is reminded that the "EDU" domain on the Internet has rules restricting or prohibiting most commercial use. Specifically,

- **College email for personal business.** Users who are College employees and contractors to include persons working in an "intern" position are prohibited from using their sjcd.edu email account for personal use and business. Accounts are to be used strictly for College-related business. Examples of personal use: mailing lists, news groups, and personal purchase confirmations that are not related to College or educational price discount programs. Exceptions may be granted if specifically related to area of instruction and job function. The introduction of non-College Business-related emails increases the likelihood of SPAM and malware infected emails that pose a risk to the College's Information Resources.
- **Advertising.** The User must not use the College's email system or any other Information Resources to transmit commercial or personal advertisements, solicitations, or promotions.
- **Off-site Personal Use of Information Resources.** College-owned computing devices, equipment, and any other Information Resources taken by the User off-site must be used for College Business and must not be used for any personal or personal business use, including the use by family members or friends. Furthermore, the User is responsible for the protection and security of Digital Content protected by laws and regulations, that is stored on or accessed by College-owned and Personal Devices.

e. **Non-compliance with the terms of License Agreements.** By using Information Resources, such as software and online services, the User agrees and understands the terms and conditions as described in License Agreements of the licenses that are granted for their use. The number and distribution of copies and access to copyrighted software and services must be handled in such a manner that the number of simultaneous Users does not exceed the number of original copies or licenses purchased by that User, unless otherwise stipulated in the purchase contract or as otherwise permitted by Federal and State Laws and Regulations.

f. **Theft of Computing Devices and other Information Resources.** The User must protect College-owned computing devices and any other Information Resources and equipment from theft, loss, or damage.

g. **Modification or Removal of Information Resources.** The User is prohibited from attempting to modify Information Resources or remove equipment including but not limited to computer devices and equipment, software, or peripherals.

h. **Use of Unauthorized or Destructive Programs and Digital Content.** The User is prohibited from intentionally using or developing programs, processes, Data or Digital Content that are disruptive to other Users, damage software or hardware components of a system, or access, store, process or transmit personal, private, or restricted information and Digital Content. The User is prohibited from breaching security, including but not limited to creating or propagating viruses or other malware, key logging, denial of service attacks, ransomware, hacking, and use of another User's password.

i. **Threats, Harassment, Libel, or Slander.** The User must not use the College's email system or any other Information Resource to send, view, or download fraudulent, threatening, harassing, obscene, or other messages or material that are a violation of applicable College Policies and Procedures, and Federal, State and Local Laws and Regulations, such as under circumstances that might contribute to creating a hostile academic or work environment.

j. **Mass Communications and unsolicited material.** The User must not send mass messages such as texts or emails to internal College accounts unless approved by the College. The User must not send mass messages such as texts or emails to external non-College accounts unless approved by the College's Marketing or Student Services Department. Mass communications are protected by laws and regulations. Furthermore, the User understands that subscribing to an outside electronic mailing/list will be viewed as having solicited material delivered by the list. Materials which are not consistent with conducting College Business will be considered as unsolicited material and may be restricted from delivery to the College's email system or other Information Resources.

k. **Child Pornography.** Child pornography is material that depicts minors in a sexually explicit way. Intentionally uploading, downloading, or viewing child pornography by the User violates Laws and is explicitly forbidden.

l. **Political Use.** The User must not use Information Resources for partisan political activities as prohibited by Federal, State and Local Laws and Regulations.

m. **Excessive use of Information Resources**. The User must not intentionally excessively use Information Resources, including but not limited to excessive, unnecessary, or wasteful usage of bandwidth, storage usage, CPU usage. Furthermore, the User must not intentionally print excessive copies of documents, files, or programs when more efficient alternatives are known. The use of College printers for personal business is prohibited.

n. **Gambling or illegal activities.** The User must not use Information Resources for gambling or other illegal activities. The User who receives any communication or materials with illegal content from any other User or third-party should report the matter immediately to campus police, Technology Support, and their immediate leader.

12. Auditor Access

Personnel of the Internal Audit Departments have access to all College activities, records, property, and employees in the performance of their duties.

a. For non-investigative audits, access requests for Information Resources, including information Services and data files, will be made to the User, as appropriate. Requests to access data subject to privacy laws and regulations must be submitted to the College's Chief Information Security Officer (CISO).

b. For investigative audits, access requests for Information Resources, including information Services and data files will be made to the appropriate College leader. Requests to access data subject to privacy laws and regulations must be submitted to the College's Chief Information Security Officer (CISO).

c. Internal Audit access to data files will be provided as specifically requested by Internal Audit; however, whenever practical, Internal Audit will utilize hard copy output or data file copies.

d. Read-only access will be granted, unless specific instructions are provided, to ensure proper safeguards for continued integrity and availability of data files.

e. State, Federal and Supervisory Authority auditors will be granted access to Information Services and data files on an as-needed basis after coordination with the Internal Auditors and area supervisor, and after proper training requirements are met.

13. Amendment and Complaints

Given the unique nature of Information Resources and the ever-evolving security threats that impact the College's operations related to the same, this procedure may be amended or modified at any time and will continue to apply to all Users of Information Resources. Users continued use of Information Resources consent to any modifications, but such use shall not be necessary for this policy to apply to all Users as amended. Complaints related to the application of this policy should be directed to a User's leader or the College's Chief Information Security Officer (CISO).

14. Definitions

The terms referenced in this Procedure are outlined in **Procedure III.3010.A.a, Information Security Program**, Section 14. Definitions**.**

Date of SLT Approval	May 29, 2024
Effective Date	May 30, 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