SAN JUAN COLLEGE

Information Security Documentation

Doc. #		Effective Date	Email
Version	1.0	Contact	Phone

TABLE OF CONTENTS

APPROVAL, REVIEW AND REVISION HISTORY

Date	Version	Description of Revision	Author	Approval Date	Approved by Name & Title
7/24/23	5	Refined Language and added language for cybersecurity insurance	Roy Lytle		

EXCEPTIONS

Only the Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the “Request for Policy Exception” form and a copy maintained by the CIO.

PURPOSE

The purpose of this policy is to establish the rules for the use of San Juan College technology resources.

SCOPE

The scope of this policy applies to all members of the San Juan College community and any contractors or third-parties using San Juan College’s technology resources or data. It also supports San Juan College in their Family Educational Rights and Privacy Act (FERPA), Payment Card Industry (PCI), Protected Health Information (PHI), and Personally Identifiable Information (PII) compliance efforts.

VIOLATIONS

Any violation of this document may result in disciplinary action, up to and including termination of employment. San Juan College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS STATEMENT

Please see the ITC Security Definitions for a list of all Information Technology (IT) definitions.

RELATED REGULATIONS

This policy is a component of the San Juan College information security program that is intended to comply with the Payment Card Industry-Data Security Standards (PCI-DSS), FERPA, Gramm Leach Billey Act and other regulations.

POLICY DETAILS

The same principles of academic freedom and privacy that have long been applicable to written and spoken communications in the College community also apply to electronic information. The College cherishes the diversity of perspectives represented on this campus and, accordingly, does not condone either censorship or the casual inspection of electronic files. The College employs various measures to protect the security of its technology resources and user accounts. Users shall therefore comply with the following policies:

1. SJC TECHNOLOGY USE

1.1. San Juan College reserves the right to monitor and inspect all network traffic and retrieve and read any data composed, sent, received, saved, or accessed via college technology resources and/or the SJC network. Since some communications over the network involve matters of academic freedom and sensitive or protected communications, this policy shall uphold the privacy of such communications.

1.2. College technology resources shall not be used to transmit, receive, or download any materials that may be ruled as malicious or judged as objectionable based on SJC policies, procedures and generally applied standards; and all applicable local, state and federal laws and regulations. Expressly prohibited is the deliberate transmission, receipt, or download of materials that contain gratuitous violence, sexual activity or depictions, obscene language, and computer codes or programs intended to negatively affect the operation of computers or College networks.

1.3. Use of San Juan College's technology resources are provided for users to conduct business or academic work in their assigned duties/course work on behalf of San Juan College. Unless specifically authorized, College technology resources shall not be used for non-College business or commercial purpose. Incidental personal use of college technology resources is permitted provided that this use does not interfere with college operations; violate college policies; create an inappropriate atmosphere for students and employees in violation of federal, state, and local law or College policy; generate incremental identifiable costs to the College; and/or negatively impact the user's job performance.

1.4. Access is available in designated areas for public use for the community. This community access may not violate local, state and federal law, or College policy.

1.5. San Juan College reserves the right to block access to certain malicious content, Internet/Web services, and other "addresses" which are not specifically related to academics, college business, and community public use. This could include legitimate services that may have been compromised.

1.6. In accordance with FERPA regulations and SJC policies, users shall not disclose any sensitive and/or confidential student or College-related information (i.e., credit card numbers, PINs, SSN, Date of Birth, etc.). If this information shall be shared externally, please contact IT for guidance on secure methods.

1.7. Personal devices used to access SJC technology resources must be password protected and have end-point protection (e.g., Anti-virus, Anti-Malware, etc.) installed and enabled. Devices discovered without such protection may be removed from the SJC network by IT.

2. EMAIL USE

2.1. Use of San Juan College's email system is provided to users to perform assigned duties and to support academic work. Unless specifically authorized, College email shall not be used for non-College business, non-academic work, or commercial purpose. Incidental personal use of email is permitted provided that this use does not interfere with college operations; violate College policies; create an inappropriate atmosphere for students and employees in violation of federal, state, and local law or College policy; generate incremental identifiable costs to the College; and/or negatively impact the user's job performance.

2.2. Unless specifically authorized, personal email should not be used for College business. Incidental use of personal email is permitted provided that this use does not interfere with college operations; violate College policies; create an inappropriate atmosphere for students and employees in violation of federal, state, and local law or College policy; generate incremental identifiable costs to the College; and/or negatively impact the user's job performance.

2.3. San Juan College email shall not be used as the account name for personal use accounts. For example, using your SJC email to create a personal social media account is not allowed. If you are creating a social media account that is for a San Juan College department or program, you shall not use the same password as your SJC password. Do not reuse passwords.

2.4. Upon voluntary separation from San Juan College, the user's identity, email account, access to MySJC, OneDrive, and other Microsoft 365 data, etc. shall be disabled after 210 days. Accounts inactive for 210 days and the associated access to SJC resources, shall be disabled. Accounts disabled for 30 days or more will have their data deleted (unless legally retained required). We do retain, although disabled, the SJC ID numbers and account IDs, i.e. doej,

2.5. Involuntary termination will result in immediate deactivation of the user account and access to College technology resources. Any exception must be documented and approved by appropriate personnel.

2.6. When emailing sensitive, confidential, or PII information, such as Social Security Numbers, Date of Birth, Student ID, Bank Account numbers, credentials, etc., the email must be encrypted, and the recipient should have information security safeguards and policies in place. Contact IT at (505) 566-3266 for more information.

2.7. College data may only reside on College-owned equipment. Users are prohibited from copying documents or files containing copyrighted information, sensitive, confidential, or PII College data to non-College owned equipment.

2.8. Non-College data may not be stored on College-owned equipment.

2.9. The deliberate receipt or transmission of materials on the Internet or via College e-mail in violation of any local, state and federal law, or San Juan College policy is prohibited.

2.10. College e-mail resources shall not be used to transmit, receive, or download any materials that may be ruled as malicious or judged as objectionable based on SJC policies and procedures, and all applicable local, state and federal laws and regulations, and generally applied standards set by the College. Expressly prohibited is the deliberate transmission, receipt, or download of materials that contain gratuitous violence, sexual activity or depictions, obscene language, or intentionally malicious computer codes or programs, such as malware or ransomware.

3. EQUIPMENT AND SOFTWARE

3.1. Users are required to comply with commercial software license agreements. Modifying, selling, or duplicating commercial software packages may be illegal and is expressly prohibited. Please contact IT at (505) 566-3266 with questions.

3.2. Installation or modification to classroom and lab software or operating system configurations may only be done by Information Technology (IT) staff. Please contact IT at (505) 566-3266 with software requests.

3.3. Software and/or documentation relating to the use of software shall not be duplicated. Please contact IT at (505) 566-3266 with these requests.

3.4. Any unauthorized duplication may result in a termination of access, authorization, or other disciplinary measures.

3.5. IT must be consulted prior to purchasing software. College employees using software agree to use the software in compliance with the licensing agreement.

3.6. Each authorized user agrees that they transfer all licensing rights in and to any legally purchased personal software that is installed onto the College system.

3.7. Any unauthorized installation of software onto unauthorized, non-College systems may be a violation of the licensing agreement and the user will be liable for any costs or liabilities associated with the unauthorized installation.

3.8. If unauthorized software is discovered, the College will, at its option, remove the software or require the owner to obtain a multiple use license for the software.

3.9. The College will, in any event, retain ownership of software installed on its technology resources. Anyone who violates or is suspected of violating this policy may have their privileges suspended or terminated. If the violator or suspected violator is a member of the general public, the violation of this policy may subject them to a civil action to recover any financial losses.

4. MOBILE COMPUTING (SJC OWNED DEVICES)

4.1. Mobile computing devices shall be password protected.

4.2. Mobile computing devices shall be kept in the user's possession or in a secure location at all times. For example, do not leave your laptop or phone unattended in a public area.The individual to whom the device is issued is responsible for its physical protection.

4.3. Lost or misplaced mobile computing devices shall be immediately reported to IT and the Department of Public Safety (DPS).

4.4. IT is responsible for wiping user's device when: 1) the device is lost, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of the College's data and technology infrastructure.

5. BRING YOUR OWN DEVICE (BYOD)

5.1. San Juan College grants the use of personal devices to its staff and faculty to access select College resources. The College reserves the right to revoke this privilege if users do not abide by the rules outlined in this policy.

5.2. The College Community may use their personal devices to access select College-owned resources to which they have permissions.

5.3. The College has a zero-tolerance policy for using personal devices while driving for official College purposes. Only hands-free talking while driving is permitted.

5.4. Users may be blocked from accessing malicious websites while connected to the College network.

5.5. To prevent unauthorized access, devices must be password protected using the features of the device.

5.6. External storage devices (USB, thumb drive, etc) containing College data shall remain secure, in the possession of the user/owner at all times, and scanned for viruses, malware, ransomware, etc. upon connection to SJC technology resources.

6. SECURITY AND ENDPOINT PROTECTION

6.1. Users of San Juan College technology are responsible for protecting College information and resources and shall not deactivate protections such as endpoint protection software (e.g., anti-virus, anti-malware, anti-ransomware, etc.).

6.2. Users shall take appropriate measures to avoid introducing a virus or malware into San Juan College computers or computer system networks.

6.3. All SJC employees are required to complete annual cybersecurity training.

6.4. Users of San Juan College technology are expected to use the standard College procedures to obtain authorized access to any College or non-College system. Unauthorized access to any system is strictly prohibited. If you find that you have access to systems that you should not have access to or no longer need access to, please submit an IT ticket.

6.5. Users granted access to a College system shall retain exclusive control of their password. It must not be written down anywhere. It must not be shared with anyone, including IT staff. IT staff will not ask for your password. Users who share passwords may be subject to disciplinary action. Users who suspect their password has been compromised shall notify IT immediately.

6.6. Users must secure technology devices when leaving their device unattended, including when leveraging office spaces, labs, or classrooms. This includes signing off the application or ensuring your device is password protected and locked.

6.7. Printed documents containing PII, PCI, FERPA, HIPAA data, or other protected, sensitive information shall be stored securely when not actively in use and securely destroyed when no longer needed. These documents may not be left out and unattended,

7. VENDOR AND THIRD-PARTY USE

7.1. Non-College employees requiring access to San Juan College's technology resources must first be approved by IT. This includes vendor staff, consultants, and regulators.

8. MONITORING

8.1. IT is authorized to observe, log, monitor and track the use of San Juan College technology resources and data. In the event that potential improper activity is suspected or discovered, IT, in coordination with Human Resources, Student Services, and/or the Department of Public Safety (DPS) may provide any evidence obtained to the College and/or law enforcement personnel. If the activity disclosed is criminal, the College may request that prosecution be undertaken by the appropriate authorities. An individual's right to use SJC systems may be suspended until a determination has been made as to whether or not the use was

improper. If improper use has occurred access will be terminated and the individual will be notified.

8.2. Users with access to confidential or sensitive information may be monitored to assure that credentials (usernames, passwords, etc.) are not shared.

8.3. Users assume full responsibility for any use of SJC resources and recognize that their assigned resources may be suspended or terminated for improper use by themselves or by someone utilizing their credentials. Account sharing is strictly prohibited.

ACKNOWLEDGEMENT OF POLICY

This document is a statement of San Juan College policy. The College will post this policy in appropriate locations and generally make copies available to everyone who uses or may use College technology resources. All provisions of this policy are implicitly accepted by all College technology users even if they have not received and/or signed a copy of this document.
In addition, each college employee or student, upon application for authorization to use College technology resources shall be required to acknowledge the following statement:

I hereby certify that I have received a copy of the San Juan College technology resources Acceptable Use Policy and agree to the terms and conditions set forth therein. I understand that any violation of the terms of this policy may result in suspension or termination of my access privileges, and disciplinary action in accordance with the faculty, staff, or student handbooks. I further understand that the installation of any proprietary software may result in an assignment of the software to the College. In the event that my conduct exposes the College to civil liability or monetary loss, I acknowledge that I may be required to indemnify the College for the same.

Name: _____

Signature: _____ Date: _____