SOUTHWESTERN COMMUNITY COLLEGE	INFORMATION TECHNOLOGY **INFORMATIONS SYSTEMS OPERATIONS SECURITY**	Procedure 8.17.01

I. SCOPE

This policy applies to all College faculty and staff, whether full- or part-time, paid or unpaid, temporary or permanent, volunteers, as well as to all other members of the College community. This policy applies to all information collected, stored or used by or on behalf of any operational unit, department and person within the community in connection with College operations. If any particular information at College is governed by more specific requirements under other College policies or procedures the more specific requirements shall take precedence over this policy to the extent there is any conflict.

II. ACRONYMS/DEFINITIONS

Availability - The degree to which information and critical College services are accessible for use when required.

Confidentiality - The degree to which confidential College information is protected from unauthorized disclosure.

Information Owner - An Information Owner has primary responsibility for overseeing the collection, storage, use, and security of a particular information resource. In cases where an Information Owner is not identified for any information resource, the cognizant Vice President or Dean shall be deemed the Information Owner

Information Resource - Data, information, and information systems used by College to conduct College operations. This includes not only the information or data itself, but also computer, network, and storage systems used to interact with the information.

Information Security - The protection of information against unauthorized disclosure, transfer, modification, or destruction, whether accidental or intentional. The focus is on the confidentiality, integrity, and availability of data.

Information Security Office/Officer (ISO) - The Information Security Office/Officer has authority and responsibility for operation and management of College's Information Security Program.

Integrity - The degree to which the accuracy, completeness, and consistency of information is safeguarded to protect the business of the College.

Risk - A probability or threat of damage, loss, or any other negative occurrence that is caused by external or internal vulnerabilities, and that may be avoided through preemptive action**.**

Security Incident - An attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; interference with information system operation; or violation of information security policy.

Segregation of Duties - The concept of having more than one person required to complete a task, which is intended to prevent fraud or error.

Vulnerability - A weakness in the College's operating environment that could potentially be exploited by one or more threats.

III. PROCEDURE

A. OPERATIONAL PROCEDURES AND RESPONSIBILITIES

- Procedures for the correct and secure operation of College information resources shall be documented, regularly reviewed and maintained, and communicated to all individuals with a need to know.
- Duties and areas of responsibility shall be segregated, also known as Segregation of Duties, to reduce opportunities for unauthorized or unintentional modification or misuse of College information resources.
- Procedures shall be implemented to ensure satisfactory control of all changes and ongoing compliance with information security requirements:
    - Changes must be documented.
    - Changes must have management approval at the relevant level.
    - Development, test, and production information resources shall be separated to reduce the risks of unauthorized access or changes to the production system.
    - Migration to production status should not occur until:
        - Acceptance requirements are clearly defined, agreed, and documented.
        - Adequate capacity of resources is confirmed.
        - Thorough testing of the development system has been demonstrated.
        - Fallback plans to the previous version or system have been defined.
- Procedures shall be defined to control the development or implementation of all operational software. Systems developed for or within the College must follow a formalized development process.
- Procedures for the reporting of security incidents and suspected vulnerabilities in College information resources shall be documented. Please reference Policy 8.15 - Information Security Incident Response for more details regarding incident response.

B. PROTECTION FROM MALWARE

Malicious software (malware) such as viruses, spyware, adware, and other software installed without a user's consent are designed to infiltrate and damage computers without the user's knowledge or permission. Systems can be infected through:

- Infected email attachments
- Infected removable or portable storage media
- Downloaded software
- Links in email, websites, or instant messages

Effective protection against malware requires a multi-layered defense comprised of technical capabilities and end user awareness and behavior.

INFORMATION RESOURCE REQUIREMENTS

- All College information resources connected to the College network or otherwise using IT facilities must run an approved and up-to-date anti-malware product that continually monitors for malware where technically feasible.
- Regular virus scans must be scheduled and executed.
- College email systems must scan all email attachments and message bodies for the presence of malicious software. Any messages found to contain malware must be removed and the user must not be allowed to retrieve the message. This scanning must be implemented for inbound and outbound email messages.
- College email systems must scan all email messages for indicators of SPAM. This includes not only malicious content (or links to web pages containing malicious content), but also unsolicited or junk messages.
- Devices suspected to have been compromised or infected by malware must be removed from use and isolated from the College network until confirmed virus-free. Contact the IT Help Desk for assistance.
- If a system is infected with malware, it must be re-installed from a known good image and data restored from a known good backup.
- Information resources must be monitored to ensure they are running the most current version of approved anti-malware software. Systems found to be non-compliant must be remediated as soon as possible.
- Information resources and networks must be monitored for indicators of compromise or malicious behavior.

USER BEHAVIOR

End users play a critical role in protecting against malware. End users must follow these practices:

- NEVER open any files or click on any links sent from unknown, suspicious, or untrustworthy sources. Delete these files or messages immediately.
- Delete SPAM, chain messages, and other junk email without forwarding, as described in College Policy 8.02 - Acceptable Use of Information Resources.
- Never download files from unknown or suspicious sources.
- Be sure to scan removable media (USB memory sticks, external hard drives, etc.) to ensure it is free from malware before use.
- Be sure to scan any file shared with you to ensure it is free from malware before use.
- Ensure critical data and system configurations are routinely backed up.
- The deliberate distribution, infection, or propagation of malware on the College network is strictly prohibited and may result in disciplinary and/or

legal action.

C. BACKUP AND RESTORE

The College maintains data backups to provide for the continuity, restoration, and recovery of critical information and information systems. These backups are designed to allow for the recovery of important information resources in the event of an equipment failure, intentional destruction of data, or other type of disaster.

The following requirements apply to data backups:

- Information Owners and the College IT Division are responsible for determining which College information resources are critical and therefore require data backup. A list will be maintained that inventories the systems for which backups are maintained. At a minimum, this list must include systems providing critical business functions to College faculty, staff, and students and systems containing important College business information, etc. This may include file servers, web servers, application servers, network infrastructure systems, security systems, etc.
- Backups must be accurately labeled and accurate backup records must be maintained.
- Daily backups will be taken of critical systems, the backup retention period may vary by system, but will be at least 30 days.
- At minimum, network device configuration backups are to be performed at least once per day for each network system (some backups will occur more frequently).
- Backups are performed utilizing an automated backup system. This system automatically performs backups of specified systems on the defined backup interval and will report any failures or detected anomalies to designated IT Division staff. The IT Division staff will investigate any reported backup issues and document the resolution of the issue.
- A copy of system backups will be maintained in a secure, remote location, at a sufficient distance from the College to escape any damage from a disaster at the primary site.
- The IT Division will test data backups at least once per month to confirm data can be restored and/or retrieved from the backup copies. These tests and their results must be documented and maintained for future review.
- All backup media must be properly disposed of when the end of useful life is reached.
- The IT Division will work with individual departments and users to determine the appropriateness and methods for backups of individual user workstations. Any workstation backups to removable or portable media must be encrypted to protect confidential data.
- College faculty, staff, or students who require data to be restored from a system backup must submit a support request to the IT Division. The request should include information about the data in question including

creation date, file name(s), last update date, and the date and time it was modified or deleted.

D. LOGGING AND MONITORING

- All information resources that handle confidential information, accept remote access network connections, or make or enforce access control (authentication and authorization) decisions, must record and retain audit-logging information.
- Information resource audit logs must be protected from unauthorized access or modification.
- Any individual engaging in monitoring activity (including accessing audit logs) without proper authorization is subject to disciplinary action.
- The recorded information must be sufficient to answer the following questions:
    - What activity was performed?
    - Who or what performed the activity, including where or on what system the activity was performed from?
    - What was the activity performed on?
    - When was the activity performed?
    - What tool(s) was used to perform the activity?
    - What was the status, outcome, or result of the activity?
    - Did the activity complete successfully or not?

- Audit logs should be recorded when a system performs any of the following activities:
    - Create, read, modify, or delete any confidential or restricted information, including confidential authentication information such as passwords.
    - Initiates, accepts, or terminates a network session providing remote access to College systems.
    - User authentication and authorization for activities covered in the above bullet points, such as user login and logout.
    - Changes to access rights to College information resources, including adding or deleting user accounts or group members, changing user privilege levels, modifying file permissions, changing database object permissions, modifying firewall rules, etc.
    - Modifications to user credentials, including password changes.
    - Changes to system, network, or service configurations, including installation of software patches and updates, or other installed software changes o Application process startup, shutdown, or restart
    - Application process abort, failure, or abnormal end, especially due to resource exhaustion or reaching a resource limit or threshold (such as for CPU, memory, network connections, network bandwidth, disk space, or other resources).
    - Failure of network services such as DHCP or DNS.

- Hardware faults or failures.
- Detection of suspicious/malicious activity such as from an Intrusion Detection or Prevention System (IDS/IPS), anti-virus system, or anti-spyware system.

- Where possible, log files must contain the following elements:
  - Type of action - examples include authorize, create, read, update, delete, and accept network connection.
  - System or component performing the action - examples include process or transaction name, process or transaction ID, etc.
  - Identifiers (as many as available) for the subject requesting the action - examples include user name, computer name, IP address, and MAC address. Note that wherever possible, such identifiers should be standardized in order to facilitate log correlation.
  - Identifiers (as many as available) for the object the action was performed on - examples include file names accessed, unique identifiers of records accessed in a database, query parameters used to determine records accessed in a database, computer name, IP address, and MAC address. Note that wherever possible, such identifiers should be standardized in order to facilitate log correlation.
  - Before and after values when action involves updating a data element. Do not record confidential information in logs such as passwords, etc.
  - Date and time the action was performed, including relevant time-zone information if not in Coordinated Universal Time
  - Whether the action was allowed or denied by access-control mechanisms. If the action was denied, the log should include a description for why the action was denied.
  - The result of the action (success, failure, etc.)
  - Any applicable error codes or descriptions for why an action was not completed successfully.

E. CONTROL OF OPERATIONAL SOFTWARE

All College authorized applications and software shall be installed by IT Services staff. IT Services will only provide technical support for software authorized by the College prior to its installation. Any software that is installed without prior authorization of IT Services will not be supported.

F. TECHNICAL VULNERABILITY MANAGEMENT

- The College will maintain a system to automatically scan its networks and endpoints for the presence of vulnerabilities related to missing software patches, as well as configuration issues that may expose systems to compromise.
- The College must scan all networks and systems that comprise the College operating environment at least once per month. The IT Division team responsible for the network or endpoint in question is required to verify and

remediate vulnerabilities in a timely manner. Reviews and subsequent outcomes must be documented and available for inspection.

- The College will engage a third-party security assessment firm at least once per year to perform an external security assessment. Any security issues discovered in this assessment must be remediated in a timely manner (or the risk must be accepted by College senior management).

G. PATCH MANAGEMENT

- The College will evaluate the status of managed endpoints to confirm they are running software that does not contain known vulnerabilities. This includes firmware, operating systems, service packs, support rollups, application software, and other programs or services that run on the system. Systems found to be running vulnerable software must be updated in a timely manner to address the noted vulnerabilities.
- As software manufacturers release new updates, these updates will be evaluated for relevance to College systems. Once an update has been determined to be required, the relevant system owners must update their systems accordingly.
- The College will maintain a system to automatically evaluate the status of managed endpoints to determine if software patches are required to address known vulnerabilities. College systems that require software updates must be updated in a timely manner to address the missing patches.
- The IT Division team responsible for the managed endpoint is required to verify and remediate patch compliance issues on a routine basis. The Information Security Office / Officer will provide oversight to the process to confirm that the operations teams are keeping systems updated as required.
- If the system owner or IT Service staff member responsible for a given system cannot (or feels they should not) comply with the vulnerability management requirements listed above, an exception request should be raised to the ISO. The ISO will review the request and make a recommendation based on overall security risk to IT Services senior management. IT Services senior management will review the request and recommendation and the appropriate College information resource owners will be responsible for making a decision based on overall risk and College objectives.

H. ENCRYPTION

- The College will utilize encryption technologies, where appropriate, in order to promote confidentiality and integrity of information, both in transit and at rest.
- Encryption performed on College systems must use proven, standard algorithms and must permit properly designated IT Services staff to decrypt the data when required.
- The use of proprietary encryption algorithms is not allowed for any purpose.
- Encrypting data at rest must ensure information availability and compliance with applicable laws and regulations. Procedures must be established to ensure that data can be decrypted when access to data is necessary. This requires backup or other strategies to enable decryption, to ensure data can

be recovered in the event of loss or unavailability of cryptographic keys. Procedures must also consider handling the compromise or suspected compromise of encryption keys.

- Data will be encrypted in transit where confidential information risks unacceptable exposure if intercepted or misrouted. A secure method will be used to convey the decryption measure to the recipient.
- All certificates used for encryption or authentication by College systems must be generated, or signed as trusted, by a Certificate Authority (CA) verified and approved by the IT Service and ISO. It is important College systems not present certificate errors or warnings to users.
- Self-generated or self-signed certificates must not be utilized by production College systems.
- The College will establish and maintain a certificate management system to ensure that:
    - Certificates used by College systems are valid and appropriately trusted by user systems.
    - Certificates can be revoked if compromised.
    - Certificate expiration and renewal are effectively managed to prevent service outages and other operational issues.

IV. SANCTIONS/ENFORCEMENT

Any College faculty, staff, or student found to have violated this policy may be subject to disciplinary action. Sanctions will be proportionate with the severity and/or frequency of offense and may include termination of employment or expulsion. In addition, violators may be subject to criminal and/or civil action.

V. EXCEPTIONS

No approved exceptions exist at this time.

Legal References

- CIS Controls v8 Control 13 (Network Monitoring and Defense)

Cross References

- Policy 8.02 - Acceptable Use of Information Resources
- Policy 8.15 - Information Security Incident Response

Adopted: September 2025

Revised: N/A