STC
South Texas College

INFORMATION SECURITY OFFICE

Information Resources Security Guidelines

1. General

These guidelines, under the authority of South Texas College *Policy #4712- Information Resources Security*, set forth the framework for a comprehensive Information Security Program as required under Texas Administrative Code and other applicable regulatory requirements.

2. Scope

Information Resources Security Guidelines apply to all individuals that have, or may require, access to the college's information resources and those with responsibility for maintaining the information resources.

Information Resources are: Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network-attached and computer-controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers. Additionally, included are the procedures, equipment, facilities, software and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

3. Responsibilities

3.1 Information Resource Manager (IRM)

The chief information officer (CIO) is designated as the college's information resources manager (IRM) as required in the Texas Administrative Code §211.20(b). The IRM is responsible for management of the college's information resources. The designation of a college IRM is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the college's information activities, and ensure greater visibility of such activities within and between institutions.

3.2 Information Security Officer (ISO)

The chief information security officer (CISO) is designated as the college's Information Security Officer (ISO) as required in Texas Administrative Code §202.71(b) to document and maintain an up-to-date information security program for the college. It is the duty and responsibility of the CISO, under the authority of the vice president for information services and planning, to:

1. Cultivate, review, and interpret new sources of information on current and emerging laws, rules, regulations, and industry practice in relation to information technology security. Liaison with local, state and federal authorities requiring information and reports on security incidents.

2. Develop and recommend policies and establish procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information resources assets against unauthorized or accidental modification, destruction, or disclosure.

3. Monitor the effectiveness of defined controls for mission critical information and report, at least annually, to the vice president for information services and planning the status and effectiveness of information resources security controls.

4. Design, implement, and provide training policies, standards, guidelines, and security monitoring processes in relation to general control, security programs, privacy regulations, and development and operation of the college’s technology infrastructure.

3.3 Owner of an Information Resource (Data Owner)

The owner of an information resource is a person responsible for a business function and for determining controls and access to information resources supporting that business function. Owners are responsible for and authorized to approve access and to formally assign custody of an information asset, judge the asset’s value, specify data control requirements and convey them to users and custodians, and ensure compliance with applicable controls. College owners will, typically, be South Texas College administrators.

3.4 Custodian of an Information Resource (Data Custodian)

A custodian of an information resource is a person responsible for implementing owner-defined controls and access to an information resource. Custodians also provide physical and procedural safeguards for information resources, assist owners in evaluating the cost-effectiveness of controls and monitoring, and implement monitoring techniques and procedures for detecting, reporting and investigating breaches in information security.

Because custodians, by virtue of their system responsibilities, have access to information resources that are generally outside the scope of their positions, they also have additional ethical and procedural responsibilities, shown in the Administrative and Privileged Access Users section 3.6 below. College custodians, typically, will have database management and server administration responsibilities.

3.5 User of an Information Resource

All individuals accessing information resources at South Texas College must formally acknowledge and abide by the Guidelines for the Acceptable Use of Information Resources. Formal acknowledgement by all individuals accessing information resources is a requirement of the Texas Administrative Code §202.72(3) and serves as a compliance and enforcement tool. Devices designated for public access shall be configured to enforce security policies and procedures without the requirement for formal acknowledgement. Users of information resources have the following responsibilities:

1. Individuals authorized to use college computing resources are prohibited from attempting to violate the security of other computer users on any system accessible via the college computer network. The violation or attempted violation of system security is grounds for revocation of computer access privileges, suspension or discharge of employees, suspension or expulsion of students and possible prosecution under federal or state law.

2. Individuals are responsible for the security of any computer account issued to them and will be held accountable for any activity that takes place in their accounts. Any discovered violation or attempted violation of system security must be reported immediately to the CISO.

3. Each faculty and staff member (including student staff) who has access to the college's central computer systems or any terminal or workstation device connected to the college computer network is responsible for using only those resources and materials required to fulfill his or her job functions. Moreover, such use must be appropriate and consistent with those job functions and must not violate or compromise the privacy or security of any data and/or systems accessible via the college computer network.

4. Users must follow recommended security procedures for machines under their control, including, but not limited to, the use of virus scanning software and application of software and operating systems updates, and will be held accountable for any activity that takes place on those machines.

5. Users are responsible for ensuring that backup copies of essential data and software used on personal computers under their control are made frequently enough to prevent unacceptable loss of such data and software.

6. Each person having access to an administrative database is responsible for ensuring the privacy and security of any information accessible to him/her in the normal course of his/her work.

7. Each person is responsible for the security of any terminal or workstation device accessible to him/her in the normal course of his/her work.

3.6 Administrative and Privileged Access Users

Certain designated persons are given broader access to information resources because their job responsibilities require such access. Typically, such persons are responsible for providing administrative service such as system maintenance, data management, and user support. The term "broader access" covers a range from wider access than given to an ordinary system user, up to and including complete access to all resources on the computer system. These responsibilities are considered additions to the responsibilities acknowledged by all ordinary computer users and by the authorizers of computer privileges.

1. Not to "browse" through the computer information of system users while using the powers of privileged access unless such browsing: is a specific part of their job description; is required during file system repair, management, or restoration; is necessary to investigate suspicious or system-impairing behavior or possible violations of college policy; or is specifically requested by, or has the approval of, the person who authorized their privileged access.

2. Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.

3. Not to copy any computer information for any purpose other than those authorized under their defined job responsibilities or pursuant to an authorized investigation or review.

4. Not to do any special favors for any user, member of management, friend, or any other person regarding access to college computers. Such a favor would be anything that circumvents prevailing security protections or standards.

5. Not to tell or disclose to any unauthorized person the information required to gain privileged access, or to engage in careless practices that would reveal that information to unauthorized persons.

6. Not to attempt to gain or use privileged access outside of assigned responsibility (e.g., on other machines) or beyond the time when such access is no longer required in assigned job functions.

7. Not to change or develop any computer software in a way that would disclose computer information to persons not authorized to have it, or make it possible to retain any special access privilege once that authorized privilege has been terminated by management.

8. Not to make arrangements on computer system(s) under their charge that will impair the security of other systems. In order to comply with this restriction, a system administrator setting up authorized networking connections should make use of available controls and protections as fully as reasonably possible.

Furthermore, all other persons given broader-than-normal access privileges on college computer systems agree that they will:

1. Report all suspicious requests, incidents, and situations regarding a college computer to an appropriate member of local management, CISO, CIO, or IS&P Client Services.

2. Use all available software protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.

3. Take steps to the best of their ability to comply with all computer security standards and policies in force and furthermore, advise management and/or designated computer security representatives of deficiencies in these standards.

4. Conduct themselves in a manner that will foster security awareness and understanding among users.

4. Classification and Management of Electronic Data

Information resource security safeguards must be applied based on the confidentiality requirements of the data and systems. Information containing any confidential data must be identified, documented, and adequately protected. Data Classification Guidelines shall be used to identify and manage electronic data. All data owners are responsible for classifying electronic data processed by systems under their purview based on data sensitivity and risk so that the appropriate security controls can be applied.

5. Risk Management

Risk management is intended to ensure that reasonable steps have been taken to prevent situations that can interfere with accomplishing the college's mission. To that end, the following measures shall be taken:

1. In accordance with Texas Administrative Code §202.75 a security risk analysis of information resources shall be performed and documented. The frequency of the risk analysis shall be dependent upon the criticality of the resource and the magnitude of any changes to the information resource infrastructure.

2. The performance and frequency of both internal and external information resource security audits and vulnerability assessments shall be consistent with all regulatory and non-regulatory requirements applicable to the college, such as the Payment Card Industry Data Security Standard (PCI-DSS).

3. The vice president for information services and planning, acting as the president's designated representative, shall make the final security risk management decisions and must approve the security risk management plan.

6. Change Management

Change management ensures that changes do not introduce any new vulnerability to systems or processes, and that changes do not negatively impact the availability of information resources. Change control management procedures must be implemented, at a minimum, for systems handling confidential information, to monitor and control hardware and software configuration changes.

The CIO shall develop and implement change control procedures. All college units shall adhere to the change control procedures prescribed.

7. Information Resources Security Safeguards

1. All computer systems, networks connections, hardware, and software are the property of South Texas College.

2. Every information resource must have an owner responsible for the security of the resource. The owner must as a minimum address information security issues related to planning, implementing, maintaining, and disposing of the information resource.

3. Information resources systems which use passwords shall be based on industry best practices on password usage and documented security risk management decisions.

4. When confidential or sensitive information from another college or state agency is received by South Texas College in connection with the transaction of official business, the confidentiality or sensitivity of the information shall be maintained in accordance with the conditions imposed by the providing agency or college.

5. Appropriate audit trails shall be maintained to provide accountability for updates to mission critical information, hardware and software and for all changes to automated security or access rules.

6. A sufficiently complete history of transactions shall be maintained to permit an audit of the college's mission critical information resources system by logging and tracing the activities of individuals through the system.

7. Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless the data has been declassified or unless all personnel involved in testing are otherwise authorized access to the production data.

8. Supervisors are responsible for ensuring that access privileges are revoked or modified as appropriate for any employee in their charge who is terminating, transferring, and/or changing duties. Supervisors should provide notification to the appropriate custodian of an information resource whenever an employee's access privileges should be revoked or changed as a result of the employee's change in status. The custodian of each information resource shall establish procedures to ensure that all security privileges associated with an employee's job function are revoked once it is known that the employee has ceased employment with the college. The separating employee shall cease to have any further access to confidential and sensitive information via college computing resources.

9. Appropriate information security and audit controls shall be incorporated into new systems. Each phase of systems acquisition shall incorporate corresponding development or assurances of security controls.

8. Network & Telecommunications

Technology Resources is designated the responsibility for the networking infrastructure at South Texas College, which includes all cabling, wireless signaling, and connected electronic devices, to ensure reliability of operations, proper accessibility to resources, and protection of data integrity.

Technology Resources is required to approve all access methods, installation of all network hardware connected to the local-area network, and methods and requirements for attachment of any computer systems or devices to any college network to ensure that access to the network does not compromise the operations and reliability of the network, or compromise the integrity of use of information contained within the network.

9. Portable Computing and Remote Access

To preserve the confidentiality, integrity, and availability of college information, users accessing the college's networking infrastructure remotely must do so in accordance with these guidelines and all college policies, standards, and/or procedures regarding acceptable use of information resources. All college and non-college owned portable computing devices storing college data must also comply with the college's Wireless Access Guidelines.

10. Business Continuity

The college shall develop and maintain a written business continuity plan in accordance with the Texas Administrative Code §202.74 so effects of a disaster are minimized and to provide for the timely resumption of mission-critical functions. For the purposes of this rule, the authority and responsibility for reviewing and approving South Texas College's business continuity plan has been delegated by the president to the chief project administrator.

As part of the college business continuity plan, the CIO shall be responsible for maintaining a written disaster recovery plan for information resources. The disaster recovery plan will:

1. Contain measures which address the impact and magnitude of loss or harm resulting from an interruption;

2. Identify recovery resources and a source for each;

3. Contain step-by-step instructions for implementing the Plan;

4. Be tested either formally or informally at least annually. Information learned from tests conducted will be used to update the existing plan.

Backups are a business requirement to enable the recovery of data and applications in the case of events such as natural disasters, system disk drive failures, espionage, data entry errors, human error, or systems operations errors.

Backup practices shall be commensurate with the risk and value of the system and data in accordance with risk management decisions implemented by the Data Owner. Mission critical data shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized college personnel.

11. Physical Controls

Without physical control over the access to information resources, there can be no security from unauthorized use of those resources because malicious or inexperienced persons could obtain access to the operating system of servers and/or desktop machines and thereby view, copy, delete, or otherwise cause harm to the files on the system. Therefore, the following procedures are critical to protecting the college's information resources:

1. All college information processing areas must be protected by physical controls appropriate for the size and complexity of the operations and the criticality or sensitivity of the systems operated at those locations.

2. Managers shall conduct reviews of physical security measures annually, as well as whenever facilities or security procedures are significantly modified.

3. Physical access to centrally administered computer facilities is restricted to individuals having prior authorization from Technology Resources. Authorized visitors shall be supervised.

4. The responsibility for securing departmentally administered computer facilities and/or equipment from unauthorized physical access and/or improper use rests with the manager responsible for the facility and/or equipment.

5. Information resources shall be protected from environmental hazards. Designated employees shall be trained to monitor environmental control procedures and equipment and shall be trained in appropriate responses in case of emergencies or equipment problems. Emergency procedures shall be developed and regularly tested at least annually.

6. No terminal or workstation logged in to a current job session capable of accessing confidential or sensitive information shall be left unattended unless appropriate measures, such as password protected keyboard locking, have been taken to prevent unauthorized use. The owner of the logged-in account is responsible for any activity that occurs during a job session logged-in under that account.

7. Data and software essential to the continued operation of critical college functions will be backed up. The security controls over the backup resources will be as stringent as the protection required of the primary resources. Backup of data and software stored on centrally administered computer systems is the responsibility of Technology Resources. Mission critical data shall be backed up on a scheduled basis and stored off site in a secure, environmentally safe, locked facility accessible only to authorized personnel.

12. Vendor Access

Vendors serve an important function in the support of hardware and software and in some cases even the operations of computer networks, servers, and/or applications. Those responsible for the third party service procurement activities and other affected departments must be aware of security implications of the service, and must institute methods for selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for the information resources to which they will have access.

Contracts must require that vendors comply with all applicable college rules associated with these guidelines, practice standards and agreements, and address all federal and state laws to which South Texas College must adhere to ensure that the college remains in compliance with such law.

The college shall control vendor access to its data based on data sensitivity, confidentiality, and risk (as determined in accordance with Section 5 of these guidelines). Any deviation from these standard provisions will require the approval of the college president.

13. Security Training

New employee orientation will be used to introduce information awareness and inform new employees of information security policies and procedures. The college shall also provide an ongoing information security awareness education program for all users. The CISO is responsible for oversight of the training program to ensure compliance with the training requirements set forth in Texas Administrative Code §202.71.

14. Security Monitoring

Pursuant to Texas Administrative Code §202.72(2) and to ensure compliance with these guidelines and state laws and regulations related to the use and security of information resources, Technology Resources personnel have the authority and responsibility to monitor network traffic and use of information resources to confirm that security practices and controls are adhered to and are effective.

15. Incident Management

Incidents involving computer security will be managed by the chief information security officer and will be reported as required by federal or state law or regulation. The CISO is required to establish and follow Incident Management Procedures to ensure that each incident is reported, documented and resolved in a manner that restores operation quickly and if required, maintains evidence for further disciplinary, legal, or law enforcement actions.

16. Software Licensing

All software used on college computers will be used in accordance with the applicable software license. Unauthorized or unlicensed use of software is regarded as a serious violation subject to disciplinary action and any such use is without the consent of the college.

Systems administrators have the right to remove software from college computers for cause. For example, if a user is unable to show proof of license, or if the software is not required for college business purposes, or causes problems on the college-owned computer.

All departments or individuals managing college-owned computers will periodically audit all computers to inventory and document all installed software. All departments are responsible for the accurate accounting of software purchased by the department and must ensure that the installation of the software complies with the license agreement of the software. For audit purposes, departments must maintain proof of purchase and/or original installation media for each software package.

17. Violations

Machines on the campus data communications network will be disconnected if they are deemed by the chief information security officer to be dangerous to the remainder of campus or to the Internet in general.

Penalties for violation of this procedure range from loss of computer resource usage privileges to dismissal from the college, prosecution, and/or civil action. Each case will be determined separately on its merits and in accordance with existing college disciplinary policies and procedures. Violations will be reported to the CIO or the vice president for information services & planning**.**

18. References

Texas Administrative Code, Chapter 202
FTC Safeguards Rule and the Gramm-Leach-Bliley Act (“GLBA”)
Texas Government Code, Section 441
Payment Card Industry (PCI) Data Security Standard
IRM Act, 2054.075(b)
The State of Texas Penal Code, Chapters 33 and 33A
DIR Practices for Protecting Information Resources Assets
Copyright Act of 1976
Computer Fraud and Abuse Act of 1986
Computer Security Act of 1987

19. Change History

Date	Name	Description
10/29/2009	Steven Bourdon	Minor grammatical edits, edited last sentence of section 17.
11/09/2009	Steven Bourdon	Removed Data Stewards, corrected sentence spacing.
01/25/2010	Steven Bourdon	Section 3.5 – minor grammatical edits.
02/16/2016	Victor Gonzalez	Adjusted references to TAC 202 to match the revised version of the document.