Procedure 2-3-b: Computer Security

Procedures Applicability

All users of the San Jacinto College computing resources will follow the Computer Security Procedures.

The San Jacinto College Security Procedures apply to information resources owned by others in those cases where a contractual or fiduciary duty exists to protect the resources while in the custody of San Jacinto College District. In the event of a conflict, the more restrictive security measures apply.

Procedures Statements

- Information Resources are valuable assets and unauthorized use, alteration, destruction, or disclosure of these assets is a computer-related crime, punishable under Texas statues and federal laws.
- Attempting to circumvent security or administrative access controls for information resources is a violation of these guidelines. Assisting someone else or requesting someone else to circumvent security or administrative access controls is a violation of these guidelines.
- Use of college computing resources should be limited to the intended purpose. Use of college-owned computers (offices and computer labs) shall be limited to college-related business or incidental personal use. The San Jacinto College District has determined that employees may use computing resources for personal reasons as long as that use does not result in additional costs or damages to the college and generally does not hinder the day to day operations of college offices and facilities. Use of e-mail to solicit sales or conduct business, setting up a web page to advertise or sell a service all constitute commercial use and are prohibited. In addition, use of computing resources for commercial, religious or political purposes or personal gain is prohibited.
- Person using Information Resources will acknowledge compliance with the Computer Security Guidelines when logon-ids and passwords are assigned, and in some cases, when an administrative application is accessed.
- Violations of the Computer Security Guidelines will be reported to the San Jacinto College District Information Technology Services.
- Violations of the Computer Security Guidelines that may be violations of state and federal laws will be reported to the appropriate legal authority.
- Persons violating the Computer Security Guidelines will be subject to appropriate administrative and criminal sanctions.
- All employees will receive the Computer Security Guidelines Summary Statement from the Human Resources Department.
- Logon-ids and passwords must control access to all information resources except for those specific resources identified as having public access such as the On-Line Public Access Catalog Library System.
- Passwords must be changed periodically by the logon-id owner as determined to be necessary by Information Technology Services.
- The logon-id owner is responsible to manage their password.
- The logon-id owner is responsible for all actions and functions performed by their logon-id.

- All Information Resources used for mission critical applications should provide a notice at logon time stating that the computer system is protected by a computer security system; that unauthorized access is not permitted; and that usage may be monitored.
- Information, which by law is confidential, must be protected from unauthorized access or modification. Data, which is essential to critical functions, must be protected from loss, contamination, or destruction.
- Confidential information shall be accessible only by personnel who are authorized on a basis of strict "need to know" in the performance of their duties. Data containing any confidential information should be readily identifiable and treated as confidential in its entirety.
- An audible, continuous chain of custody shall record the transfer of confidential information. When confidential information from a department is received by another department, the receiving department, the receiving department shall maintain the confidentiality of the information in accordance with the conditions imposed by the providing department.
- All employees accessing a mission critical administrative application must receiving appropriate training and must acknowledge the security and privacy requirements for the date contained in the application.
- When an employee terminates employment, their access to information resources will be terminated.
- All information resources used for mission critical applications shall have a cost effective, written contingency plan that will provide for prompt and effective continuation of critical missions in the event of a disaster.
- End-user workstations used in sensitive or critical tasks must have adequate controls to provide continued confidentiality, integrity, and availability of data stored on the system.
- All end-user workstations will have virus protection software installed.
- Computer software purchased using college funds is San Jacinto College property and shall be protected as such.
- Physical access to all areas that house the facilities providing information resources shall be restricted to authorized personnel. Authorized visitors should be supervised and their entry and exit recorded in a log.
- Individuals who believe they have experienced computer generated harassment or illegal discrimination are encouraged to contact the appropriate administrative office to file a complaint.
- Internet access to the San Jacinto College Network will be controlled as appropriate under guidelines determined by Information Technology Services.

Procedures Administration

The Computer Security Procedures is administered by Information Technology Services. The Director of Information Technology Services, or their designee, has responsibility to:

- Monitor computer security issued
- Maintain records on computer security issues
- Monitor compliance with these guidelines

These guidelines will be reviewed annually and updated as appropriate.

Management Responsibility

Administrators are responsible for the security of information resources in all offices under their jurisdiction and for implementing information security requirements on an office-wide basis.

Administrative Data Ownership

Administrative data is owned by the administrative unit(s) having primary responsibility for creation and maintenance of the data content.

Data Custodian Responsibilities

The data custodian is the unit assigned to supply services associated with the data.

The custodian is:

- The Information Technology Services for centrally supported administrative applications,
- The end-user of an individual microcomputer workstation.

The custodian provides services in accordance with the directions from the area supervisor and is responsible for:

- Implementing specific controls over the data,
- Providing a general security access system,
- Insuring compliance of its employees with security guidelines.

Data User Responsibilities

The data user is the person who has been granted explicit authorization to access the data by the District. This authorization must be granted according to established guidelines. The user must:

- Use the data only for purposes specified by the area supervisor,
- Comply with security measures specified by the area supervisor,
- Not disclose information in the data nor the access controls over the data unless specifically authorized in writing by the area supervisor.

Electronic Mail

Electronic mail is provided to faculty, staff, and students as part of the Information Resources of San Jacinto College to conduct the business of San Jacinto College.

Electronic mail is intended to be a convenient way for the faculty and staff to communicate with one another and colleagues at other locations. The information in electronic mail files may be subject to disclosure under certain circumstances; for example, requests filed under the Texas Open Records Act, or during audit or legal investigations.

No user shall alter electronic communications to hide their identity or impersonate another person. These actions are considered forgery. All e-mail, news posts, chat sessions, or any other form of electronic communication should contain your name and/or user name. Forgery includes using another person's identity or using a fake identity. Similarly, you must not conceal your identity, except when anonymous access is explicitly provided.

The propagation of chain e-mail using San Jacinto College resources is prohibited. In most cases, first offense results in a warning. Subsequent offenses result in referral to the appropriate San Jacinto College District authority for disciplinary action.

Additionally, the only appropriate uses of mass public distribution lists are notification of official college-related activities. When using a public distribution list, text that reflects the content of the message must be placed in the subject line. This way a message that is not of interest can be deleted with being read. The use of personal group distribution lists (that is, those created and maintained by an individual) must follow these guidelines.

Auditor Access

There will be occasions when auditors require access to Information Resources and data files. The access will be permitted according to these guidelines:

Internal Auditors from San Jacinto College District

- Personnel of the Internal Audit Departments have access to all College activities, records, property, and employees in the performance of their duties.
- For non-investigative audits, access requests for Information Resources and data files will be made to the area supervisor and the administrative management of the organization operating the computers and information resources, as appropriate.
- For investigative audits, access requests for information resources and data files will be made to the appropriate administrative management level of the organization operating the computers and information resources.
- 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.
- Read only access will be granted, unless specific instructions are provided, to ensure proper safeguards for continued integrity and availability of data files.

External Auditors

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

Activities Prohibited by Law

Any computing activity that violates local, state or federal law is a violation of San Jacinto College District Computing Guidelines. Upon receiving a report of alleged violation, the appropriate SJCD authority may refer the incident for possible investigation and/or prosecution by the appropriate local, state, or federal authorities.

Illegal activities include, but are not limited to

Threats and Hoaxes

It is illegal to send a message via e-mail that threatens other persons or property. Federal authorities may investigate these messages.

Child Pornography

Child pornography is material that depicts minors in a sexually explicit way. Under federal child pornography statutes anyone under the age of 18 is a minor. Intentionally uploading or downloading child pornography violates these laws. It is also illegal to advertise or seek the sale, exchange, reproduction, or

distribution of child pornography. Exhibition of any files containing images of naked children could violate child pornography statutes. It is also illegal to distribute pornography to minors.

Copyright Infringement

Reproducing copyrighted material without permission of the author or their agent is considered illegal. In response to the recently enacted Digital Millennium Act, the San Jacinto College District has appointed an agent to receive statutory notices from copyright owners about infringements and to send statutory notices to affected subscribers. Upon receiving notification that a user of the San Jacinto College District computing resources has used sources inappropriately, they will notify the SJCD Chancellor, President of the appropriate campus, and the user accused of the infringement. If it is determined that an infringement has taken place, necessary steps will be taken to correct the situation. The user will also be provided with additional information explaining the appropriate use and reproduction of copyrighted material. Any user repeatedly found to infringe on the copyrights of others will lose access privileges to the San Jacinto College District computing resources.

Software Piracy

Unauthorized duplication, distribution or use of someone else's intellectual property, including computing software, is illegal and subject to both civil and criminal penalties.

Defamation/Invasion of Privacy

Defamation can occur in two forms-libel and slander. Slander is a fleeting form, like speech. Libel occurs in a physical, longer-lasting form. Defamation is conveying false information that injures a person's reputation or holds them up to ridicule or humiliation such that lowers their standing in the community or deters others from associating with them. Invasion of privacy may occur when a person's likeness is used without permission, especially for commercial purposes, or when personal or private information about a person is communicated to other persons who have no need to know the information.

Sexual Harassment

Use of a computer system to engage in sexual harassment, as defined in the District's sexual harassment guidelines is in violation of federal discrimination laws.

Scams and Pyramid Schemes

Pyramid schemes and chain e-mail involving the collection of money are illegal under federal laws.

Procedure #:	**2-3-b**
Procedure Name:	**Computer Security**
Pages:	**3**
Adopted Date:	
Revision/Reviewed Date:	**February 5, 2008**
Effective Date:	**February 5, 2008**
Associated Policy:	**VI-V**