

# University Computing and Telecommunications

## SECURITY GUIDELINE

APPLICABILITY: San José State University

---

### 1. PURPOSE

The purpose of this guideline is to:

- Ensure that the University complies with state laws and regulations regarding the use of and security of electronic and computer based Information Resources.
- Establish prudent and reasonable practices for the protection and security of Information Resources.
- Educate employees, students, faculty, and others who may use Information Resources about the responsibilities associated with such use.
- Protect automated information resources against accidental or unauthorized disclosure, contamination, modification or destruction, as well as to ensure the security, reliability, integrity and availability of information.

It is the practice of San Jose State University to protect all electronic data and computer based information technology resources.

### 2. GENERAL GUIDELINES

- Access to University information resources must be controlled. State law requires that state owned information resources be used only for official state purposes.
- Sensitive or confidential information, must be protected from unauthorized access or modification.
- Data, that is essential to critical University functions, must be protected from loss, contamination, or destruction.
- Risks to information resources must be managed. The expense of security safeguards must be appropriate to the value of the assets being protected, considering value to both the University and potential intruder.
- The integrity of data, its source, its destination, and processes applied to it, are critical to its value. Changes to data must be made only in authorized and acceptable ways.
- In the event a disaster or catastrophe disables information processing and related telecommunication functions, the ability to continue critical University services must be assured.
- Security needs must be considered and addressed in all phases of development or acquisition of new information processing systems.
- Security awareness of employees must be continually emphasized and reinforced at all levels of management.

All individuals must be responsible for their actions relating to information resources.

- The University information security program must be responsive and adaptable to changing vulnerabilities and technologies affecting information resources.
- The University must ensure adequate separation of functions for tasks that are susceptible to fraudulent or other unauthorized activity.

### 3. RESPONSIBILITIES FOR INFORMATION RESOURCE SECURITY

Various classes of persons have responsibilities for the security of data, software, hardware and other information resources at SJSU:

- The AVP of UCAT has designated the Computer Center's Network Security Officer to be responsible for coordinating the University's information security function. The information security function is charged with:
  - Recommending guidelines and establishing procedures and practices, in cooperation with owners and custodians, necessary to ensure the security of information assets against unauthorized or accidental modification, destruction or disclosure.
  - Documenting and maintaining an up-to-date information security program.
  - Monitoring the effectiveness of defined controls for critical information.
  - Reporting, at least biennially, to the President or his/her designated representative on the effectiveness of information resources security controls.
- Owner of an Information Resource - A person responsible for a business function and for determining controls and access to information resources supporting that business function. Owners are responsible and authorized to approve access and 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.
- Custodian of an Information Resource - The 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 System Administrator Code of Ethics in section 4, below.
- User of an Information Resource - An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules. Users of information resources have the following responsibilities:
  - Individuals authorized to use University computing resources are prohibited from attempting to violate the security of other computer users on any system accessible via the University computer network.
  - 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 Network Security Officer.
  - Each SJSU faculty and staff member (including student staff) that has access to the University's

central computer systems or any terminal or workstation device connected to the University 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 University computer network.

- 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.
- Users are responsible for insuring 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.
- Each person having access to an administrative database is responsible for insuring the privacy and security of any information accessible to him/her in the normal course of his/her work.
- 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. Any ID or Password information will be safeguarded for these terminals/workstations.

## 4. SYSTEM ADMINISTRATOR CODE OF ETHICS

Certain designated persons are given broader access to the resources of computer systems because their job responsibilities require such access. Typically, such persons are responsible for providing administrative services on the designated computer(s), services 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. Persons with the broadest (complete) access are sometimes called "super users".

This code of ethics applies to all persons given broader-than-normal access to any resources on SJSU multi-user computer systems. It also applies to persons who authorize such access. The points contained in this code are considered additions to the responsibilities acknowledged by all ordinary computer users and by the authorizers of computer privileges.

### Responsibilities of Privileged Access Users

Super users (individuals with full access to files) and all other persons given broader-than-normal access privileges on SJSU computer systems agree:

- 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 (e.g., a university computer auditor); is required during file system repair, management, or restoration; is necessary to investigate suspicious; or system-impairing behavior or possible violations of SJSU guideline; or is specifically requested by, or has the approval of, the person who authorized their privileged access. Browsing should never be done unless it is in the best interest of SJSU.
- Not to disclose, to any unauthorized person, computer information observed while operating with privileged access.
- 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.
- Not to intentionally or recklessly damage or destroy any SJSU computing resources.

- Not to accept favors or gifts from any user or other person potentially interested in gaining access to SJSU computer systems.
- Not to do any special favors for any user, member of management, friend, or any other person regarding access to SJSU computers. Such a favor would be anything that circumvents prevailing security best practices or guidelines.
- 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.
- 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.
- 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.
- 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, super users and all other persons given access privileges on SJSU computer systems agree that they will:

- Report all suspicious requests, incidents, and situations regarding a SJSU computer to an appropriate member of local management, Internal Audit, SJSU Police, Offices of Human Resources or Student Development, as applicable.
- Use all available software protections to safeguard computer system(s) under their charge from unauthorized access by any person or another computer.
- Take steps to the best of their ability to comply with all computer security best practices and guidelines at SJSU and furthermore, advise management and/or designated computer security representatives at SJSU of deficiencies in these guidelines.
- Conduct themselves in a manner that will foster security awareness and understanding among users.

## Responsibilities of Management

Management should restrict the number of persons granted privileged access to a minimal practicable number. Management should tell the person who is responsible for overall administration of a system the names of all other persons who have been granted privileged access and what functions those persons have been assigned. Persons who are to be given privileged access to a SJSU computer system should be selected (or approved) by the Head of the department that owns or manages the operation of the computer system or by another member of management to whom this responsibility has been delegated.

## 5. RISK ANALYSIS PROCEDURES

Risk analysis is the vehicle for systematically evaluating the vulnerabilities of an information system and its data to the threats facing it in its environment. It's an essential part of any security and risk management program. Although absolute security against all threats is unachievable, risk analysis provides a framework for weighing losses which may be expected to occur, in the absence of an effective security control, against the costs of implementing such a control. Risk management is intended to ensure that reasonable steps have been taken to prevent situations that may interfere with accomplishing the University's mission. To that end, the following measures shall be taken:

- An internal audit of the information security function shall be performed periodically, based on risk assessment, as directed by the President or the Associate Vice President for University Computing and Telecommunications Services acting on delegated authority for risk management decisions.
- Owners of information resources shall periodically complete and/or commission a risk analysis of all information resources in their custody. The degree of risk acceptance (i.e. the exposure remaining after implementing appropriate protective measures, if any) must be identified and documented.
- The Associate Vice President for University Computing and Telecommunications shall biennially complete and/or commission a risk analysis of information resources considered essential to the University's critical mission and functions. He or she shall also prepare or commission and maintain a written and cost-effective Disaster Recovery Plan that provides for the prompt and effective continuation of critical University systems in the event of a disaster. The Disaster Recovery Plan will be tested and updated periodically to assure that it is valid and remains current.

## 6. PERSONNEL PRACTICES

- People are the most important components of an information security program. People also represent the greatest threats to information security; therefore, maintaining employee awareness and motivation is an integral part of the security program. Managers are responsible for taking all measures necessary to insure that departmental staff maintain an appropriate level of confidentiality for information retrieved from University information sources. Examples of such information may include personnel and payroll records, transcript and grade records, financial aid information, and other sensitive data. Use of such information for unauthorized purposes is prohibited; as is access to such information in any form whatsoever by unauthorized individuals.
- The Network Security Officer will develop and maintain an Information Security Best Practices Document that details specific steps that should be taken to protect information resources at SJSU. The use of University information resources implies that the user has knowledge of and agrees to comply with the best practices and guidelines contained and referenced in the document. Managers are responsible for insuring that all faculty, staff, and student members of their respective departments, including part-time or temporary employees, read and agree to the best practices and guidelines as outlined in this document and the Information Resources Security Practice Document.
- The Security Department at University Computing and Telecommunications shall provide literature and/or training to emphasize security awareness and the importance of individual responsibility with respect to information security. Supervisors must continually reinforce the value of security consciousness in all employees whose duties bring them into contact with confidential or sensitive information resources.
- Supervisors are responsible for insuring 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 insure 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 University. The separating employee shall cease to have any further access to confidential and sensitive information via University computing resources.

# 7. PHYSICAL SECURITY, EQUIPMENT, AND POWER PROCEDURES

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 University's information resources:

- All University 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.
- Managers shall conduct reviews of physical security measures annually as well as whenever facilities or security procedures are significantly modified.
- Each individual entering a monitored door must use the appropriate processes to enter protected doors. Tailgating (multiple people entering using a single security device) at Biometric, Card-key, or Omni-lock doors is strictly prohibited.
- Doors shall not be propped open and left unattended.
- 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.
- 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.
- 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 enabled to prevent unauthorized use.
- Data and software essential to the continued operation of critical University 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 the University Computing and Telecommunications Department. Departments administering networks are responsible for establishing regular schedules for making backup copies of all mission-critical data and software resident on their networks and for ensuring that the backups are stored in a safe location.
- No one other than the Network Security Officer shall grant access to the premises. The Network Security Officer MUST clear individuals who do not have their own individual access regardless of their relationship to the individual, personal or professional.
- Floor tiles may never be removed by anyone other than Data Center Personnel.
- Any technicians, vendors or any other personnel will run no network cables of any sort, unless authorized by and under direct supervision of the Director of Network Services.
- Equipment may only be installed after prior written approval of the Change Management Committee.

- Physical access to centrally administered computer facilities is restricted to individuals having prior authorization from the Computing Center. Authorized visitors shall be supervised.

## 8. INFORMATION SAFEGUARDS

- The University Computing and Telecommunications Department will purchase and maintain virus protection software for use on all University-owned or operated computers.
- Each University department shall, as part of its contingency plan, provide for an alternate means of accomplishing its program objectives in case the system or its communication network becomes unavailable. Alternative procedures shall be established that enable University personnel to continue critical day-to-day operations in spite of the loss of the communication network.
- When confidential or sensitive information from another university or state agency is received by SJSU in connection with the transaction of official business, SJSU shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing agency or university.
- Except for public users of systems where such access is authorized, or for situations where risk analysis demonstrates no need for individual users, each user of a multiple-user automated system shall be assigned a unique personal identifier or user identification. User identification shall be authenticated before the system may grant that user access to automated information. E.g. SJSUONE
- Mission-critical University systems which use passwords for authentication shall conform to the federal standard on password usage contained in the Federal Information Processing Standard Publication 112 ([FIPS PUB 112](#)), which specifies minimum criteria and provides guidance for selecting additional password security criteria when appropriate.
- Appropriate audit trails shall be maintained to provide the ability for changes to confidential or sensitive information, software and automated security or access rules.
- Encryption techniques for storage and transmission of information shall be used based on documented agency security risk management decisions.
- Test functions shall be kept either physically or logically separate from production functions. Copies of production data shall not be used for testing unless all personnel involved in testing are authorized access to the production data.
- 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.
- Public access systems must authenticate the identity of any individual retrieving, creating, and/or updating sensitive or confidential information about themselves.
- Public access systems must have security procedures in place to protect the privacy and confidentiality of individuals who access those systems, in accordance with federal and state laws.
- Any individual who connects a machine to the campus network is responsible for maintaining security on that machine system (including password security) and for performing appropriate security updates so as to prevent security breaches to the campus network.
- The custodian of an information resource must take steps where possible, such as using an encryption system, to ensure that passwords cannot be obtained by interception of data communications transmissions or access to a storage device.
- Network access to an application containing confidential or sensitive data, and data sharing between

applications, shall be as authorized by the application custodians and shall require authentication of any user of the application.

## **9. SECURITY BREACHES**

The owner of the information system, assisted by the San Jose State University Information Security Officer if such assistance is requested, shall investigate breaches to information resource security controls promptly.

## **10. SANCTIONS**

- Machines on the campus data communications network will be disconnected if they are deemed by the Network Security Analyst to be dangerous to the remainder of campus or to the Internet in general.