Standard: Access Control

Executive Summary

Access control is a critical information security process that forms the basis of the authority used to determine access to confidential information, is limited only to authorized users and those who need such access to complete their work as a faculty member, staff member, or student. The basis for implementation of campus access control is a coordinated implementation of a campus-wide identity management system, wherein the identities, roles, and authorities of all users are maintained using consistent standards and policies. The Access Control Standard defines the access control requirements surrounding the management of access to information on SJSU's computer and communication systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of SJSU's business information, as it is stored, processed, and transmitted.

Information Security Standards

Access Control

Standard #	**IS-AC**	**Effective Date**	**11/1/2015**	**Email**	**security@sjsu.edu**
Version	**6.1**	**Contact**	**Information Security Team**	**Phone**	**408-924-1530**

Revision History

Date	Action
4/23/2014	Draft sent to Mike
5/14/2014	Reviewed, left in comments. Added comments.
12/1/2014	Reviewed, left in comments. Content suggestions. Added comments. Hien Huynh
3/2/2015	Minor Edits – Cleaned up for Draft Standard Posting on Web, removed multiple sections for length – Mike Cook
11/1/2015	Incorporated changes from campus constituents – Distributed to Campus.
1/13/2017	Incorporated workstation administrative privileges information – Hien Huynh
11/18/2020	Reviewed. Nikhil Mistry
10/19/2021	Reviewed. Cole Gunter
11/30/2022	Reviewed. Cole Gunter

Table of Contents

Introduction and Purpose

This standard defines the access control requirements surrounding the management of access to information on San Jose State University (SJSU) computer and communications systems. The purpose of this standard is to define security protection controls that will help minimize the loss of confidentiality, integrity, and availability of SJSU business information as it is stored, processed, and transmitted.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities, with a target audience of SJSU Information Technology employees and partners.

Standard

This Access Control Standard establishes, documents, and formalizes review based on SJSU business requirements for access to level 1 and level 2 data, as defined in the Information Classification Standard. This standard should be reviewed on a periodic basis for necessary updates to each campus department business requirement.

Access Control System

An Access Control System will be implemented that will control access to Level 1 and Level 2 data based on roles and privileges that restrict information on a need to know basis.

Regulating Software

All software installed on SJSU campus multi-user systems must be regulated by an approved access control system that will control a user's session prior to passing control to separate application software.

Password Based Access Control

Any system that stores, processes, or transmits Level 1 or Level 2 information must utilize a properly maintained version of an approved password based access control system.

User ID Creation Date

Access control systems must be configured to capture and maintain the creation date for every user ID.

Last Logon Date

Access control systems must be configured to capture and maintain the date and time of the last logon for every user ID.

Last Logoff Date

Access control systems must be configured to capture and maintain the date and time of the last logoff for every user ID.

Password Change Date

Access control systems must be configured to capture and maintain the date and time of the last password change for every user ID.

User ID Expiration Date
Access control systems must be configured to capture and maintain an expiration date or every user ID that represents the last date that the user ID is active for use.

Malfunctioning Access Control
Where possible, if a computer or network access control system is not functioning properly, it must default to denial of privileges to end-users.

Access Control System Modification
The functionality of all access control systems must not be altered, overridden or bypassed via the introduction of additional code or instructions.

Access Control Registers
Departments are required to create and maintain unambiguous, organized, and current records of all information system access privileges to Level 1 and Level 2 protected information systems. Access Control Registers are to be reviewed annually as part of the CMS/Separations of Duties Audit by department management and sign-off provided to the Information Security Office.

Every User ID Reflected in a Centralized Access Database
Every User ID on every multi-user computer system within all SJSU campuses must be reflected in the centralized database maintained by Human Resources.

Circumventing Access Control
Programmers and other technically-oriented staff must refrain from installing any code that circumvents the authorized access control mechanisms found in operating systems or access control packages.

Authorization and Privilege Management
Each campus department Information Owner should develop privilege profiles based on user profiles needing access to Level 1 or Level 2 information. The granting of privileges based on standard profiles should be authorized through a formal authorization process.

Sensitive Information Access
Access to campus Level 1 or Level 2 information must be provided only after express management authorization has been obtained.

Granting Access to Organization Information
Access to campus Level 1 or Level 2 information must always be authorized by a designated Information Owner of such information, and must be limited on a need-to-know basis to a reasonably restricted number of people.

Information System Privilege Usage
Every information system privilege that has not been specifically permitted by the campus department Information Owner must not be employed for any campus department business purpose until approved in writing.

Need To Know Privilege Restriction
The computer and communications system privileges of all users, systems, and programs must be restricted based on the need to know. Access to all Level 1 and Level 2 information, as specified in the Information Classification Standard, must be restricted based on the need to know.

Granting Access to Campus Information
Access to campus Level 1 or Level 2 information must always be authorized by a designated Information Owner or via formal approval process, and must be limited on a need-to-know basis to a reasonably restricted number of people.

User ID and Privilege Approval
Whenever user IDs, business application system privileges, or system privileges involve capabilities that go beyond those routinely granted to general users (i.e. administrative access to workstations), they must be approved by the user's department manager (MPP) or department chair. The department must keep these approvals on file for future review. Campus Desktop Technicians are responsible for ensuring that administrative accounts, if created locally, area disabled upon employee separation. Departments may elect to utilize the Request for Workstation Administrative Privileges form.

System Access Request Authorization
All requests for additional privileges on campus multi-user systems or networks must be submitted on a completed system access request form that is authorized by the user's immediate manager.

Default User Privileges
Without specific written approval from management, administrators must not grant any privileges, beyond electronic mail and word processing, to any user.

Information Security Awareness Training
All campus users must complete an approved information security training and awareness class before they are granted access to any campus department Level 1 or Level 2 information or within 30 days of hire.

Personal Information Access
All identifying information about customers and student record data, must be accessible only to those campus department personnel who need such access in order to perform their jobs.

Separation of Activities and Data
Management must define user privileges such that ordinary users cannot gain access to, or otherwise interfere with, either the individual activities of, or the private data of other users.

Read Access to Sensitive Information
Users who have been authorized to view information classified at a level 1 or 2 sensitivity level must be permitted to access only the information at this level and at less sensitive levels.

Role-Based Access Control Privileges
The information systems access privileges of all users must be defined based on their officially assigned roles within the campus department, as specified by the Information Owner for the respective campus.

Special Privileged Users
All multi-user computer and network systems must support a special type of user ID that has broadly-defined system privileges, which will enable authorized individuals to change the security state of the system.

Special System Privileges
With respect to ICSUAM8105, special system privileges, such as the ability to examine the files of other users, must be restricted to those directly responsible for system management and/or systems security.

Third Parties
Access granted to third parties such as vendors, auditors, and consultants, shall be done so after the completion of a Vendor-Confidentiality Agreement. Departments shall maintain copies of confidentiality agreements for all third parties accessing sensitive data.

Number of Privileged User IDs
The number of privileged user IDs must be strictly limited to those individuals who absolutely must have such privileges for authorized business purposes.

User Access Management
Formal procedures should be in place to control the allocation of access rights to information systems and services. The procedures should cover all stages in the life-cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

User Registration
There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services. Users will be required to accept the Responsible Use Policy prior to receiving an account and on every password reset where possible.

Non Anonymous User IDs
All individual user IDs on campus computers and networks must be constructed by matching the individual's EMPLID or must otherwise clearly indicate the responsible individual's name, and under no circumstances are such user IDs permitted to be generic, descriptive of an organizational title or role, descriptive of a project, or anonymous.

Unique User ID and Password
Every user must have a single unique user ID and a personal secret password for access to campus multi-user computers and computer networks.

Non-Employee User ID Expiration
Every user ID established for a non-employee must have a specified expiration date, with a default expiration of 365 days when the actual expiration date is unknown.

User ID Expiration
Expiration dates must be set for all user IDs on multi-user systems at SJSU. When user IDs expire, privileges for user IDs must be automatically revoked, and the files linked to these user IDs must be retained for at least a two-week period.

Unique User ID
Each computer and communication system user ID must uniquely identify only one user. Shared or group user IDs must not be created or used wherever possible.

Generic User ID
User IDs must uniquely identify specific individuals and generic user IDs based on job function must not be created or used.

Re-Use of User IDs
Each SJSU campus computer and communication system user ID must be unique, connected solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with SJSU.

User ID Naming Standard
Campus worker user IDs must be the same on every production computer system and comply with the user ID naming standards specified by the IT Department.

Access Privileges Termination
All campus information systems privileges must be promptly terminated at the time that a worker ceases to provide services to the SJSU campus department.

Access Privilege Review
All campus information systems privileges should be promptly reviewed for necessary changes or revoked promptly after a user's role has changed.

Record of Access
The campus information owner is responsible for maintaining a current record of all users authorized to use a particular application or system that has access to Level 1 information. Each user's access will be confirmed by their supervisor that their access is consistent with the business purpose.

User Password Management
Creation, distribution, and management of passwords must follow a formal management process established by the Information Security Office. Specific guidelines and procedures for user password management will be established.

Password Complexity Guidelines
As determined by the Information Security Office, campus users will be required to adhere to the password strength and complexity specifications for initial passwords, expiration, and reset in compliance with NIST Level 2 Password Complexity Requirements. For more information on password complexity refer to the Password Assurance Calculator.

Password Lockout
The Information Security Office will enforce thresholds for account lockout in the event of incorrect passwords entered in compliance with NIST Level 2 Password Complexity Requirements. For more information on password complexity refer to the Password Assurance Calculator.

Initial Password Distribution
As specified by the campus Password Standard, an initial password distribution mechanism should be reasonably secure for temporary, initial use passwords. Users should be forced to change initial password.

Password Reset
As specified by the campus Password Standard, procedures will be followed to properly verify a user's identity before a replacement password or reset.

Password Expiration
As specified by the campus Password Standard, campus user passwords will expire after 180 days.

Reuse of Authentication Credentials on Public Websites
SJSU workers must never use their internal network credentials (userid and password) on a public internet site which requires authentication.

User Responsibilities

Password Use
Users will be responsible for protecting the confidentiality of their password. Users will undergo Awareness Training and comply with the campus Password Standard. Users must not share their password for any reason. Users aware of the use of shared passwords shall notify the Information Security Office.

Clear Desk
Outside of regular working hours, unless they are working at the time, all workers must clean their desks and working areas such that all sensitive or valuable data is properly secured. Unless information is in active use by authorized personnel, desks must be absolutely clear of confidential data during non-working hours with all information locked away.

Clear Screen
When computers are left unattended, users shall lock their computers to prevent unauthorized viewing of confidential data.

Covering Sensitive Information
All workers who handle campus Level 1 or Level 2 information must adequately conceal this information from unauthorized disclosure to nearby non-authorized parties.

Network Access Control
Access to both internal and external networked services should be controlled. User access to networks and network services should not compromise the security of the network services by ensuring that appropriate interfaces are in place between campus network resources, student networks, and public networks. Security standards for network access control are specified in the Network Security Standard.

Operating System Access Control
Security facilities should be used to restrict access to operating systems to authorized users. The facilities should be capable of the following:

- Authenticating authorized users, in accordance with a defined access control policy.
- Recording successful and failed system authentication attempts.
- Recording the use of special system privileges.
- Issuing alerts when system security policies are breached.
- Providing appropriate means for authentication.
- Where appropriate, restricting the connection time of users.

Password Attempts
After five unsuccessful attempts to enter a password, the involved user ID must be suspended until reset by a Systems Administrator, temporarily disabled for no less than five minutes, or disconnected if dial-up or other external network connections are involved.

Password on Login Requirements for Workstations
All University owned workstations including, but not limited to, personal computers, portable computers, transportable computers, and handhelds, must employ an access control system which requires a password at the time the device is powered on either at boot or within the Operating System. Exceptions shall be granted where appropriate compensating controls exist, or risk is low (i.e. Kiosks, Police Dispatch). Exceptions shall be approved/documented by the Information Security Office.

Logon Information
Wherever possible, when logging into a SJSU computer or data communications system, if any part of the logon sequence is incorrect, the user must be given only feedback that the entire logon process was incorrect. Specific diagnostic feedback is prohibited.

Incorrect Logon Feedback
When logging on to a SJSU computer or data communications system, if any part of the logon sequence is incorrect, the system must terminate the session and wait for the correct logon information.

System Logon Banner
Where desired, each logon screen for multi-user computers must include a special notice which must state that the system may only be accessed by authorized users, users who logon represent that they are authorized to do so, unauthorized system usage or abuse is subject to criminal prosecution, and system usage will be monitored and logged.

Logon Banner Information
Where possible, all logon banners on network-connected SJSU computer systems must direct the user to log on, and must not provide any identifying information about the organization, operating system, system configuration, or other internal matters until the user's identity has been successfully authenticated.

Portable Identification Credentials
All portable identification credentials that work with computers must require the provision of a fixed password to operate each time they are used, and must be automatically disabled if they have experienced five consecutive incorrect attempts to enter that same password. These systems include, but are not limited to, smart cards, identity tokens, and photo ID badges with magnetic stripes.

Operating System User Authentication
SJSU campus application systems developers must consistently rely on the access controls provided by operating systems, commercially-available access control systems that enhance operating systems, gateways or firewalls. Where possible, these developers must not construct other mechanisms to collect or manage access control information, and they must not construct or install other mechanisms to identify or authenticate the identity of users, without first having obtained the permission of the Information Security Office.

Null Passwords Always Prohibited
At no time, may any Systems Administrator or Security Administrator enable any user ID that permits password length to be zero (a null or blank password).

Password Characters
All user-chosen passwords less than 16 characters in length must contain at least one alphabetic and one non-alphabetic character.

Password Case
All user-chosen passwords less than 16 characters in length must contain at least one lower case and one upper case alphabetic character.

Password History
Where possible, authentication systems must be used to maintain an encrypted history of previously chosen fixed passwords (i.e. Active Directory). This history must contain at least the previous 5 passwords for each user ID.

System-Generated Passwords
All system-generated passwords for end users must be pronounceable.

System-Generated Password Issuance and Storage
If passwords or personal identification numbers are generated by a computer system, they must always be issued immediately after they are generated and must never be stored on the involved computer systems.

Password Display and Printing
Where possible, display and printing of passwords, when end users enter them, must be masked, suppressed, or otherwise obscured so that unauthorized parties will not be able to observe or subsequently recover them.

Masking Password Changes
Whenever user-chosen passwords or encryption keys are specified, they must be entered twice and masked such that the user cannot see what was typed.

Required Password Changes
Where possible, all users must be automatically required to change their passwords at least once every 180 days.

Password Change Interval Synchronization
Where possible, the fixed password change interval must be synchronized across all computer and network platforms at SJSU campus locations.

Passwords in Readable Form
Fixed passwords must never be in readable form outside a personal computer or workstation.

Password Encryption
Passwords must always be encrypted when held in storage for any significant period of time or when transmitted over networks.

Password Retrieval
SJSU computer and communication systems must be designed, tested, and controlled to prevent any type of retrieval of stored passwords, whether the passwords appear in encrypted or unencrypted form.

System Access Control Passwords
Computer and communication system access control must be achieved through passwords that are unique to each individual user. Access control to files, databases, computers, and other system resources via shared passwords (also called lockwords) is prohibited. Local and Service Account passwords used to log on to University Systems outside of the Password Management System, must be changed whenever a party who has knowledge of or access to the password separates from the University.

Vendor Default Passwords
All vendor-supplied default passwords must be changed before any computer or communications system is used for SJSU business.

Control Override Facilities
Management must establish override facilities to be used in those exceptional circumstances where controls must be compromised to maintain on-going business operations. The ability to use override facilities must be severely restricted, and these facilities must be used only when absolutely necessary.

File Restoration Access Control
If end users are given the ability to restore their own files, they must not be given privileges to restore other users' files or to see which files other users have backed-up.

Automatic Log Off or Lock
Wherever possible, if there has been no activity on a computer terminal, workstation, or personal computer for 30 minutes, the system must automatically blank the screen, suspend the session, and require a password for the re-establishment of the session. Exceptions shall be granted where appropriate compensating controls exist, or risk is low (i.e. Kiosks, Police Dispatch). Exceptions shall be approved/documented by the Information Security Office.

Time-Dependent Access Control
All multi-user computer systems must employ positive user identification systems to control access to both information and programs. Beyond this basic access control, user activities must be restricted by time of day and day of the week.

Application and Information Access Control
Security facilities should be used to restrict access to and within application systems. Logical access to application software and information should be restricted to authorized users. Application systems should:

- Control user access to information and application system functions, in accordance with a defined access control policy.
- Provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or bypassing system or application controls.
- Not compromise other systems with which information resources are shared.

Records

Production Application System Log Contents
Where possible, all computer systems running SJSU production application systems must include logs that record additions and changes to the privileges of users.

User ID Records
Records reflecting all the computer systems on which users have user IDs must be kept current.

Access Review of User Access Rights

Review of Accounts Used in Applications and Middleware
SJSU must annually review the privileges of special accounts used for production applications, system accounts, or middleware.

Reauthorization of User Access Privileges
The system privileges granted to every user must be reevaluated annually by the user's immediate manager annually to determine whether currently-enabled system privileges are needed to perform the user's current job duties.

Mobile Computing and Telecommuting
A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing, communication facilities, and telecommuting.

Small Portable Computer Usage
Personal digital assistants, handheld computers, and smart phones must not be used for SJSU business information unless they have been configured with encryption and passcodes for all mobile devices which access University systems, including email and calendar.

Confidential Information on Transportable Computers
Workers possessing a portable, laptop, notebook, handheld, or other transportable computer containing confidential Level 1 SJSU information must not leave these devices unattended at any time unless the information contained therein is exclusively stored in encrypted form.

Sensitive Information on Personal Computers
If sensitive information is to be stored on the hard disk drive or other internal components of a personal computer, it must be protected by either a password access control package or encryption. When sensitive information is written to a flash drive, floppy disk, magnetic tape, smart card, or other storage media, the media must be suitably marked with the highest relevant sensitivity classification. Unless encrypted, when not in use, this media must be stored in locked furniture.

Lending Computers Containing Sensitive Information
A personal computer, handheld computer, transportable computer, personal digital assistant, smart phone, or any other computer used for business activities that contains sensitive information must not be lent to anyone.

Organization Property at Alternative Work Sites
The security of SJSU property at an alternative work site or campus is just as important as it is at the central office. At alternative work sites, reasonable precautions must be taken to protect SJSU hardware, software, and information from theft, damage, and misuse.

Information Stored In Organization Portable Computers
SJSU provides selected members of its workforce with portable computer equipment so that they can perform their jobs at remote locations including hotel rooms and personal residences. The information stored in SJSU portable computer equipment is SJSU property, can be

inspected or used in any manner at any time by SJSU and, like the equipment, it must be returned to SJSU at the time workers are no longer employed by SJSU.

Storage of Remote Access credentials In Portable Computers

Users must never store remote access information (such as fixed passwords and user-IDs) in their portable computer, or the accompanying case, because this could allow a thief to readily gain unauthorized access to SJSU data.

Portable Computers, PDAs, and Smart Phones Out Of Sight

When stored in a motor vehicle or in another unattended public place, users must keep all portable computing devices covered and out of sight. For example, when left in a locked car or in an unattended hotel room, these devices must be covered and out of sight. These devices include machines such as laptops, tablets, personal digital assistants, and smart phones.

Physical Protection of Wireless Handheld Devices and Network Interface Cards

Wireless handheld devices, and any other device containing wireless network interface cards (NICs), must be physically protected by the user from loss, theft, and tampering.

Mobile Device Usage with SJSU Information

All computing devices used to conduct any SJSU business must be properly configured with necessary antivirus/antimalware software. This policy does not apply to cellular phones or pagers that are not used for text messages dealing with SJSU business.

Sensitive Information Not Accessed from Public Terminals

Employees must not use public web terminals to access sensitive SJSU information.

Telecommuter Working Environments

To retain the privilege of doing off-site work, all telecommuters must structure their remote working environment so that it is in compliance with all SJSU policies and standards.

Telecommuter Information Security Procedures

Telecommuters must follow all remote system security policies and procedures including, but not limited to, compliance with software license agreements, performance of regular backups, and use of shredders to dispose of sensitive paper-resident information.

Remote Workers Required to Sign Specific Policy

All SJSU employees who are approved to work from remote locations must sign an agreement to abide by specific remote worker policies. The agreement should be reviewed annually.

Clock Synchronization of Telecommuting Systems

Telecommuting workers must diligently keep their remote computers' internal clocks synchronized to the actual date and time.

Teleworker Third-Party Network Access Control

When accessing a SJSU computer or communications system through a third-party network teleworkers must use the secure remote access solution provided by the organization.

Teleworker Connections to Internet Service Providers

Any remote device used to communicate with a SJSU computer or communications system must be protected by a broadband router or firewall when directly connected to the teleworker's Internet service provider.

Teleworker Software Updates
Teleworkers must check for updates and apply them periodically, as explained in the manufacturer's documentation, either automatically or manually, for all equipment used to communicate with SJSU computer and communications systems.

Anti-Malware Controls on Personally-Owned Equipment
Regardless of Operating System, workers must install and properly maintain anti-malware software and controls on all personally-owned equipment used to access a SJSU computer or communications system. For more information on Anti-Malware visit the Antivirus Web Site.

Definitions

Account (User ID or Username)
A unique string of characters assigned to a user by which a person is identified to a computer system or network. A user commonly must enter both a user ID and a password as an authentication mechanism during the logon process.

Confidential Information (Sensitive Information)
Any SJSU information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by SJSU from a third party under a non-disclosure agreement.

Partner
Any non-employee of SJSU who is contractually bound to provide some form of service to SJSU.

Password
An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

System Privileges
Advanced powers or authorities within a computer system, which are significantly greater than those available to the majority of users. Such persons will include, for example, the system administrator and network administrator who are responsible for keeping the system available and may need powers to create new user profiles as well as add to or amend the access rights of existing users.

Users
Any SJSU employee or partner who has been authorized to access any SJSU electronic information resource.

More Information

[1] San Jose State University: "SJSU Antivirus".

< https://antivirus.sjsu.edu/>

[2] Request for Workstation Administrative Privileges
<http://its.sjsu.edu/services/info-security/security-forms/index.html>

References

ISO/IEC 27002 – 11 Access Control