

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, and 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.

Table of Contents

Introduction and Purpose	5
Scope	5
Standard	5
Auditing	6
Authorization and Privilege Management	5
Local Administrative Rights	5
Default User Privileges	5
Information Security Awareness Training	6
Separation of Activities and Data	6
Role-Based Privileges	6
Third Parties	6
User Access Management	6
User Registration	6
Unique User ID and Password	6
Non-Employee User ID Expiration	7
User ID Expiration	7
Termination of Access	7
Access Privilege Review	7
Record of Access	7
Password Management	7
Initial Password Distribution	7
Password Reset	7
Reuse of Authentication Credentials on Public Websites	7
User Responsibilities	7
Password Use	7
Clear Desk	8
Clear Screen	8
Covering Sensitive Information	8
Network Access Control	8
Operating System Access Control	8
Logon Information	8
Incorrect Logon Feedback	8
System Logon Banner	8
Logon Banner Information	9
Portable Identification Credentials	9
Null Passwords Always Prohibited	9
System-Generated Password Issuance and Storage	9
Password Display and Printing	9

Password Encryption	9
Password Retrieval	9
System Access Control Passwords	9
Vendor Default Passwords	9
Control Override Facilities	10
File Restoration Access Control	10
Automatic Log Off or Lock	10
Time-Dependent Access Control	10
Application and Information Access Control	10
Auditing	10
Production Application System Log Contents	10
User ID Records	10
Definitions	11
Access Control	11
Account (User ID or Username)	11
Confidential Information (Sensitive Information)	11
Partner	11
Password	11
System Privileges	11
Users	11
More Information	12
References	12

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, staff, 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.

Auditing

Where possible, systems must record the following data for security and auditing purposes:

- User ID Creation Date
- Last Logon Date
- Last Logoff Date
- Password Change Date

Authorization and Privilege Management

Each system owner/administrator must implement and practice a process for reviewing access requests to systems housing Level 1 or Level 2 data. The request must be approved by their MPP. System owners/administrators must also review user access annually, as per CSU policy. Users/accounts no longer requiring access are to be removed.

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.

Local Administrative Rights

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 or servers), 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, are disabled upon employee separation. Departments may elect to utilize the [Admin Rights Request](#) form.

Default User Privileges

Without specific written approval from management (MPP or department chair), administrators must not grant any elevated permissions going beyond the scope of their role. This applies to

all information assets. Workstations are not to be deployed with local administrative rights, unless an [Admin Rights Request](#) form has been submitted, and approved by their MPP.

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.

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.

Role-Based 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 data/information owner for the respective campus.

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.

User Access Management

To implement the ISO Domain 9: Access Control Policy, access to campus Information Assets containing Level 1 or Level 2 Data must include a process for documenting appropriate approvals before access or privileges are granted. All changes to user accounts (i.e., account termination, creation, and changes to account privileges) on campus Information Systems or network resources (except for password resets) must be approved by appropriate campus personnel. Such approval must be adequately documented in order to facilitate auditing of access control practices

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 deregistration 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 deregistration 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.

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. 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. The ID must be assigned solely with the user to whom it was assigned, and must not be reassigned after a worker or customer terminates their relationship with SJSU.

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.

Termination of Access

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. An **annual** review (at least) is required by the Chancellor's Office.

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 MPP that their access is consistent with the business purpose. This list should be reviewed **annually**, at least.

Password Management

Any system utilizing a password must abide by SJSU's [Password Standard](#). Access to systems storing, processing, or transmitting Level 1 data must use authentication methods requiring multi-factor authentication, including both a secure password (as per SJSU's Password Standard). Appropriate controls must be in place to prevent unauthorized access to these Information Assets. All are required to identify and document public or shared resources that are excluded from this requirement.

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 required to change their initial password; enable this option if the system allows.

Password Reset

As specified by SJSU's [Password Standard](#), procedures will be followed to properly verify a user's identity before a replacement password or reset.

Reuse of Authentication Credentials on Public Websites

SJSU workers must never use their internal network credentials (user id 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 Team.

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.

Logon Information

Whenever 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.

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).

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

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. 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

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

Whenever 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/documentated by the Information Security Team.

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.

Auditing

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.

Definitions

Access Control

A security technique that regulates who or what can view or use resources in a computing environment. It is a fundamental concept in security that minimizes risk to the business or organization. There are two types of access control: physical and logical. Physical access control limits access to campuses, buildings, rooms and physical IT assets. Logical access control limits connections to computer networks, system files and data.

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://www.sjsu.edu/it/security/antivirus-software.php/>>

[2] Admin Rights Request
<<https://app.docusign.com/templates/details/6ee04edb-4850-4505-9177-0ec6a4d2caa2>>

References

[CSU's Policy and Standards](#)

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
7/31/2023	Updated by Noel
5/28/24	Updated by Noel

1/24/2025	Reviewed and Updated. Janice Lew
-----------	----------------------------------
