Standard: Network Security

Executive Summary

Network security is important in the protection of our network and services from unauthorized modification, destruction, or disclosure. It is essential that protection of information and the supporting infrastructure used for delivery be built into the SJSU's network and culture to adhere to a "defense in depth" model. Network Security Standard defines the requirements for network security for all SJSU's computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU. This standard describes the controls and process for access to the campus network, placement of assets on the campus network, transport of data across the network, network authorization and authentication, and management of the network against security threats.

Information Security Standards

Network Security

Standard #	IS-NS	Effective Date	10/3/2022	Email	security@sjsu.edu
Version	4.0	Contact	Information Security Team	Phone	408-924-1530

Revision History

Date	Action
5/31/2014	Draft sent to Mike
7/10/2014	QA Review
8/21	ISO Review – Added additional network device controls
12/1/2014	Reviewed. Content suggestions. Added comments. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.
11/18/2020	Reviewed. Nikhil Mistry
10/20/2021	Reviewed & Grammar Corrections. Cole Gunter
10/3/2022	Reviewed and Updated. Cole Gunter

Table of Contents

Executive Summary 2
Introduction and Purpose 6
Scope 6
Standard 6
- Network Security Filtering 6
  - Inbound Access from Internet to Campus computers 6
  - Open ports and services based on business need 6
- Secure Network Configuration 6
  - Change Control for Network Infrastructure 6
  - Firewall Policy Management 6
- Authorization for Usage of network services 6
  - Discontinuing Service 6
  - Internet Connection Approval 7
  - Standards of Common Carriers 7
  - Minimizing Wireless Network Unauthorized Signal Interception 7
- User authentication for external connections 7
  - Remote Access Passwords 7
  - Computer-Connected Network Access 7
  - Dial-Up Users 7
  - In-Bound Internet Access 7
  - Common Directory Service and User Authentication 7
  - Unsecured Remote Computer Connections to SJSU Network Denied 7
  - Remote diagnostic and configuration port protection 8
  - Diagnostic Port Access 8
  - Segregation in networks 8
  - Public Access to Wired Network 8
  - High-Security and High-Reliability Computers and Networks 8
  - Web Server Firewalls 8
  - Logical Isolation of Wireless Access Points 8
  - Internal Network Device Access Control System 8
  - Internal Network Device Passwords 8
  - Access to Production Internal Network Devices 8
  - Implementing Multi-User Systems 8
  - System Interconnection 9

Network routing control 9
Network-Connected Computers Access Control 9
Connecting Third-Party Networks 9
Workstation Modems 9
Modem Line Registry 9

Introduction and Purpose

This standard defines the requirements for network security for all San Jose State University (SJSU) computer and communication system information, with the goal of safeguarding the confidentiality, integrity, and availability of information stored, processed, and transmitted by SJSU.

Scope

This standard applies to all SJSU State, Self-Fund, and Auxiliary ("campus") computer systems and facilities (including SJSU remote network locations), with a target audience of SJSU Information Technology employees and partners. For the purposes of this document, network control devices include but are not limited to: firewalls, routers, switches, routers, and wireless networking equipment.

Standard

Network Security Filtering

Inbound Access from Internet to Campus computers

Inbound access to SJSU desktop, laptop & tablet computers from the public Internet, including lab, workstation, and test systems, is prohibited including RDP and SSH.

Open ports and services based on business need

Each Information Owner for the campus department is responsible for ensuring that network ports and services for assets are firewalled to only allow necessary ports and services, and all other ports and services are blocked. A risk review of adherence will take place on an annual basis, by the Information Security Office.

Secure Network Configuration

Change Control for Network Infrastructure

IT Services will actively manage the security configuration of network infrastructure devices using a configuration management and change control process.

Firewall Policy Management

IT Services will actively manage the security configuration of firewall devices using a firewall change control procedure with approvals flowing through the Information Security Office.

Authorization for Usage of network services

Users should only be provided with access to the services that they have been specifically authorized to use.

Discontinuing Service

In alignment with ICSUAM8105, IT Services reserves the right to block, conceal, deny, or discontinue its network service at any time without advance notice in the event of an Information Security Risk. Departmental IT teams shall notify IT Services any time an internet facing server is removed from service. IT Services may choose to block known protocols or application types

(i.e. SMTP, RDP BitTorrent, Ares) as necessary to maintain a secure environment. Exceptions shall be granted on an as-needed basis.

Internet Connection Approval

Workers must not establish any external network connections that could permit non-SJSU users to gain access to SJSU systems and information, unless prior approval by the Information Security Officer has first been obtained.

Standards of Common Carriers

The networking services provided by SJSU are provided on a contractual carrier basis, and not a common carrier basis. This means that SJSU's relationship with users is dictated by the terms and conditions found in its contract, not by legal requirements which generally apply to telephone companies and related service providers.

Minimizing Wireless Network Unauthorized Signal Interception

Wireless network access points must be placed and the coverage area designed so that the possibility of unauthorized signal interception is minimized.

User authentication for external connections

Appropriate authentication methods should be used to control access by remote users.

Remote Access Passwords

User IDs with factory default, blank or null passwords (passwords with no characters), or passwords which do not meet or exceed the requirements in the SJSU Password Standard must not be permitted to gain remote access to any SJSU computer or network.

Computer-Connected Network Access

All users must have their identity verified with a user ID and a secret password or by other means that provide equal or greater security prior to being permitted to use SJSU computers connected to a network.

Dial-Up Users

Dial up connections to campus networks are prohibited. Any diagnostic lines necessary to bridge campus and external networks shall be approved by the Information Security Team.

In-Bound Internet Access

All users establishing a connection with SJSU computers on its internal network through the Internet must first authenticate themselves at a firewall that employs an extended user authentication process approved by the Information Security Team.

Common Directory Service and User Authentication

A common directory service endorsed by the Information Security Team must be used for all user authentication processes involving servers connected to the internet. An exception will be made in those cases where the Information Security Team has evaluated and deemed a particular server as technically unable to interface with the common directory service.

Unsecured Remote Computer Connections to SJSU Network Denied

At the time that they make a connection with the SJSU internal network, all external computers may be automatically scanned to determine whether they have adequate security measures

installed and operating. Computers that cannot be scanned, as well as those that are not adequately secured, may be denied network access.

Remote diagnostic and configuration port protection
Physical and logical access to diagnostic and configuration ports should be controlled.

Diagnostic Port Access
Access to all diagnostic and maintenance ports must be securely controlled with the use of a key lock, or related measures, used in conjunction with effective procedures.

Segregation in networks
Groups of information services, users, and information systems should be segregated on networks.

Public Access to Wired Network
All walk-up network access for visitors to connect back to their home networks must employ a separate subnet that has no connection to the SJSU internal network.

High-Security and High-Reliability Computers and Networks
Every high-security and high-reliability system managed by or owned by SJSU must have its own dedicated computers and networks, unless approved in advance by the Information Security Team.

Web Server Firewalls
All web servers accessible through the Internet must be protected by a router and/or firewall approved by the Information Security Team.

Logical Isolation of Wireless Access Points
All wireless access points must be logically distinguished from, and firewalled off from, the main internal SJSU internal network using configurations approved by the Information Security Team.

Internal Network Device Access Control System
IT Services will maintain a Network Access Control System capable of managing user accounts for administrative access on to all critical Network Devices including, but not limited to, routers, firewalls and access control servers. This system must integrate with the campus Active Directory for password and user management. The system will be the primary mechanism for authentication of Networking Services staff on to Internal Network Devices.

Internal Network Device Passwords
All SJSU internal network devices including, but not limited to, routers, firewalls, and access control servers, must have unique local-device passwords. These passwords are to be secured in an encrypted password vault and only accessed in the event of a malfunction of the Network Device Access Control System.

Access to Production Internal Network Devices
Administrative user accounts to Production Internal Network Devices shall be disabled or read-only at all times unless configuration changes are actively taking place. Unlocking of Production accounts, including those used by vendors, shall only take place following an approved Change Control entry, approval for change from the Information Security Office and approved technical review by a network engineer. To maintain separation of duties, activation of

administrative accounts in Production shall be executed by a party external to Networking Services.

Implementing Multi-User Systems

Workers must not establish intranet servers, electronic bulletin boards, local area networks, VPN's, modem connections to existing internal networks, wireless network access points, or other multi-user systems for communicating SJSU information without the specific approval of the Information Security Team.

System Interconnection

Real-time connections between two or more in-house computer systems from different security tiers must not be established unless the Information Security Team has first determined that such connections will not unduly jeopardize information security.

Network routing control

Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

Network-Connected Computers Access Control

All SJSU computers that can be reached by third-party networks must be protected by a privilege access control system approved by the Information Security Team.

Connecting Third-Party Networks

SJSU computers or networks must be connected only to third-party computers or networks after the Information Security Team has determined that the combined system is in compliance with SJSU security requirements.

Workstation Modems

Workers must not connect dial-up modems to workstations, personal computers, or local area network clients that are simultaneously connected to a local area network or another internal communication network unless the telephone line does not permit direct inward dialing (NON-DID).

Modem Line Registry

Workers must not install or contract for the installation of modem lines that connect to SJSU computers or networks, unless these lines have been approved by the Networking Services Director and entered into the organization-wide modem line registry.