Standard: 802.11 Airwave

Executive Summary

Information Technology Services (ITS) recognizes the increased use and availability of various wireless technologies at SJSU. SJSU is responsible for providing a communication network that is accessible, accountable, reliable, legal, and secure. In order to guarantee this level of service IT Services manages the airspace. Maintaining security of the wireless system is crucial. Therefore, access to the wireless system will be limited to individuals authorized to use campus and Internet resources through username and password authentication. Any College, Department, Unit, or Individual who wishes to utilize wireless technology must follow stated policies, protocols, practices, and procedures. This standard outlines the roles, processes, requirements, and restrictions surrounding 802.11 wireless “Wi-Fi” networks.

Information Security Standards

802.11 Airwave

Standard #	IS-A	Effective Date	11/10/2015	Email	security@sjsu.edu
Version	3.0	Contact	Mike Cook	Phone	408-924-1705

Revision History

Date	Action
5/16/2014	Draft Complete
6/30/2014	Reviewed by IT Management Advisory Committee, Campus Information Security Committee, ITS Security Team
7/9/2014	Approved by CIO
01/26/2015	Reviewed. Content suggestions. Added VPN passage. Hien Huynh
11/10/2015	Incorporated changes from campus constituents – Distributed to Campus.

Table of Contents

Introduction and Purpose

SJSU is responsible for providing a communication network that is accessible, reliable, legal, and secure. In order to guarantee this level of service IT Services manages the airspace. Any College, Department, Unit, or Individual who wishes to utilize wireless technology must follow stated policies, protocols, practices, and procedures.

This standard outlines the roles, processes, requirements, and restrictions surrounding 802.11 wireless "Wi-Fi" networks.

Scope

This policy applies to all 802.11 wireless "Wi-Fi" networks whose transmission origin is located on a property currently owned or occupied by San José State University or its auxiliaries including but not limited to: SJSU Main Campus (including all Academic, Administrative, Auxiliary, MLK Library, Foundry, University Housing buildings and outdoor spaces), SJSU South campus (all buildings and outdoor spaces), 210 N. 4th Street, Moss Landing Marine Labs, and Bunker Hill where WiFi is provided by campus.

Standard

Security and Encryption

Identification of Users

In order to ensure compliance with ICSUAM 8000, all wireless devices capable of accessing campus Wi-Fi systems must authenticate utilizing a username and password. IT Services will provide a mechanism to register devices incapable or infeasible of following this standard by the means of device registration. Devices will be registered to an individual and in accordance with ICSUAM 8105 that individual will be held accountable for any activities taking place on those devices.

Illegal Content

IT Services reserves the right to block all known malicious protocols, ports and all applications whose mainstream usage is for illegal activity (Ares, Bittorrent, IRC, etc.) or non-supported payment methods (Paypal, Square).

Encryption

In order to support all devices, a number of supported wireless networks exist. Users shall connect to the network with the least amount of security risk.

Connection Order for Wireless Networks

1. SJSU_Premier
2. Eduroam
3. SJSU_Guest
4. SJSU_MyDevices

Impersonation of IT Services Supported Wireless Networks

No Colleges, Departments, Units, or Individuals shall configure a wireless SSID that contain "SJSU" (case insensitive) within SJSU's airspace. Any users doing so will be referred to the appropriate Vice President or Judicial Affairs.

Airwave Control

Includes: SJSU Main Campus (including all Academic, Administrative, Auxiliary, MLK Library, Self-Support, University Housing and outdoor spaces), SJSU South campus (all buildings and outdoor spaces), 210 N. 4th Street, Moss Landing Marine Labs, and Bunker Hill.

IT Services shall provide the sole means for wireless connectivity in all supported locations. Hotspots and Printers with WiFi shall be configured to disable wireless features wherever possible. IT Services is committed to providing reliable wireless services to all on-campus buildings and select outdoor areas. Poor service in specific areas is not adequate justification for installing rogue access point. IT Services reserves the right to disable wired ports, wirelessly disable Access Points and block MAC Addresses associated with rogue wireless networks. To report on-campus areas with inadequate service, contact the IT Help Desk at 4-1530 (408-924-1530) or email ithelpdesk@sjsu.edu

For more information on wireless coverage please visit the Wireless Web Site.

Unsupported Networks

Colleges, Departments, Units, or Individuals shall not knowingly or willingly activate wireless networks without prior written authorization from IT Services ISO or CIO. This includes but is not limited to wireless routers and printers, which broadcast their own network. IT Services reserves the right to disconnect, flood, or block unsupported wireless networks within SJSU's airspace.

Under certain circumstances IT Services may approve non-standard network communication devices for usage. Non-standard devices must meet the following criteria:

- The use is for a specific purpose.
- The device will only be used in a specific location and not moved without prior written authorization from the IT Services ISO or CIO.
- The device must be manageable as appropriate by either IT Services or authorized entity.
- If available, devices must require username/password authentication.
- The strongest form of encryption available must be used.
- IP Address assignment must be made in coordination with IT Services.

Final responsibility for the data security and proper use of non-standard devices shall remain with the requestor. Any network problem caused by such a device or by any attached device(s) will result in the immediate disconnection of the device or deactivation of network port. All connections of non-standard network communication devices must be pre-approved by IT Services Change Control.

Bandwidth Considerations

In order to maintain adequate services for all parties, IT Services reserves the right to throttle bandwidth or cap total usage as it deems required to meet the needs of the university.

Roles and Responsibilities

Colleges, Departments, Units, Individuals

Colleges, Departments, Units, and Individuals are responsible for compliance with SJSU security policies, standards, and procedures. Colleges, Departments, Units, and Individuals are responsible for contacting the IT Help Desk (4-1530, 408-924-1530, or email ithelpdesk@sjsu.edu) with any issues and requests.

Colleges, Departments, Units, and Individuals requesting unsupported devices are responsible for contacting IT services to initiate the request process, providing all requested information in relation to the service, and notifying IT Services when service is no longer needed.

IT Services – IT Help Desk

The IT Help Desk responds to trouble tickets initiated by individuals, escalates issues as appropriate, and provides a single point of contact for all requests.