Solano Community College

Wireless Networking Department Policy

Purpose

The purpose of this policy is to define the use and management of Solano Community College wireless networking

Scope

This IT policy applies to Solano Community College employees, contractors, subcontractors, vendors, consultants, advisors, students, guests, and other personnel accessing wireless networks at district locations

Definitions

Wireless LAN Controller – A centralized network device used to define wireless networks and manage wireless access points

SSID – Service Set Identifier. It is the unique network name for a given wireless network

Guest/unsecured network – A wireless SSID/network that is not password protected. Traffic is not encrypted

Secured network – A wireless SSID/network that is password protected, and utilizes encryption

WPA2 – Wi-fi Protected Access, version 2. A method to secure a secured SSID and encrypt traffic

PSK – Pre-shared key. One authentication method utilized by WPA2. Users and devices must enter a password to join a wireless network

802.1X – An authentication method utilized by WPA2. It requires passing user credentials to join a wireless network. The credentials are centrally located on the district network

Process

Wireless management

The district wireless networks will be managed by redundant wireless LAN controllers. It will have the ability to group access points, define SSIDs and the access points/locations they are available. It will also provide access point management and monitoring.

Guest/unsecured networks

These networks are available to all users, including personal devices. Typical users would be students, staff, guests, contractors, vendors and consultants. Use is at the user’s discretion, and they are responsible for security of their device and the data they transmit. Access to district resources are limited.

Secured networks

All secured networks will be protected with WPA2 encryption, using one or more authentication method. Only approved contractor/vendor/consultant and district-owned devices will be permitted to join secured networks.

Networks using PSK will have passwords set and managed by college IT. They are not to be shared with users. In the event of compromise, IT will change the password to re-secure the network.

Networks using 802.1X will have centrally managed and maintained credentials tied to network systems.

Revision History

Version:	Date:	Description:
1.0	10/7/2022	Initial document