
SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Wireless Security*

Wireless Security (Jan 2010 Revision)

Purpose

Wireless security requirements define the high-level specifications for the secure deployment and use of wireless networking.

Requirements

Each agency ISO is accountable for ensuring the following steps are followed and documented:

Wireless LAN (WLAN) Connectivity on the COV Network:

The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

1. The following requirements shall be met in the deployment, configuration and administration of LAN infrastructure connected to any internal Commonwealth of Virginia network.
 - a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e. digital certificates).
 - b. WLAN infrastructure must authenticate client devices prior to permitting access to the WLAN.
 - c. LAN user authorization infrastructure (i.e. Active Directory)_ must be used to authorize access to LAN resources.
 - d. Only COV owned or leased equipment shall granted access to an internal WLAN.
 - e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption protocols such as the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher.
 - f. Physical or logical separation between WLAN and wired LAN segments must exist.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Wireless Security*

g. All COV WLAN access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device.

h. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled.

i. WLAN clients will not permit wireless peer to wireless peer communication.

WLAN Hotspot (Wireless Internet)

The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

2. When building a wireless network which will only provide unauthenticated access to the Internet the following must be in place:

a. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption methods such as the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher.

b. Hotspot WLANs must have logical or physical separation from the Agency's LAN.

c. Hotspot WLANs must have proper traffic filtering capabilities enabled to protect clients from malicious activity.

d. All hotspot WLAN access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device.

e. Configuration and security data associated with the hotspot WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled.

f. WLAN clients will not permit wireless peer to wireless peer communication.

SOUTHSIDE VIRGINIA COMMUNITY COLLEGE INFORMATION TECHNOLOGY SECURITY PLAN

IT Systems Security – *Wireless Security*

Wireless Bridging

The SVCC IT Network administrator will be responsible for satisfying the following requirements and maintaining auditable documentation for the same:

3. The following network configuration shall be used when bridging two wired LANs:
 - a. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption methods such as the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher.
 - b. All traffic traversing the wireless bridge must be encrypted using a mechanism other than the wireless bridge.
 - c. Wireless bridging devices will not have a default gateway configured.
 - d. Wireless bridging devices must be physically or logically separated from other networks.
 - e. Wireless bridge devices must only permit traffic destined for the bridge and should not directly communicate with any other network.
 - f. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled.
 - g. Wireless bridging devices must not be configured for any other service than bridging (i.e. a wireless access point).