FORT VALLEY STATE UNIVERSITY
A State and Land-Grant Institution • University System of Georgia

Wireless Access Standard

Purpose

The purpose of this standard is to secure and protect the information assets owned by Fort Valley State University. Fort Valley State University provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. Fort Valley State University grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets. This standard specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a Fort Valley State University network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the Office of Information Technology in writing are approved for connectivity to the Fort Valley State University network system.

Scope

All employees, contractors, consultants, students, temporary and other workers at Fort Valley State University, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of Fort Valley State University must adhere to this standard. This standard applies to all wireless infrastructure devices that connect to a Fort Valley State University network or reside on a Fort Valley State University site that provides wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data. The Fort Valley State University Office of Information Technology must approve exceptions in writing to this policy in advance.

Statement of Requirements

All wireless infrastructure devices that connect to a Fort Valley State University network or provide access to Fort Valley State University Confidential, Fort Valley State University Highly Confidential, or Fort Valley State University Restricted information must:

- Use Extensible Authentication Protocol-Fast Authentication via Secure Tunneling (EAP-FAST), Protected Extensible Authentication Protocol (PEAP), or Extensible Authentication Protocol-Translation Layer Security (EAP-TLS) as the authentication protocol, or utilize WebAuth authentication.
- Use Temporal Key Integrity Protocol (TKIP) or Advanced Encryption System (AES) protocols with a minimum key length of 128 bits unless the SSID is by design on a designated public wireless VLAN.
- Must be approved for use by the Office of Information Technology.
- Broadcast of SSIDs not configured for general public use will be disabled.

FORT VALLEY STATE UNIVERSITY
A State and Land-Grant Institution • University System of Georgia

Lab and Isolated Wireless Device Requirements

- Lab device Service Set Identifier (SSID) must be different from Fort Valley State University's production device SSIDs.
- Broadcast of lab device SSID must be disabled.

Equipment

- All wireless access points deployed within the campus network will be centrally managed by the Office of Information Technology's Cisco Wireless Access Manager.

References

In support of this standard, the following policies, guidelines, and resources are included:

- FVSU Wireless Access Policy

Enforcement

This standard is part of the *FVSU Wireless Access Policy* and failure to conform to the standard is a violation of the policy. Any employee or student found to have violated the policy may be subject to disciplinary action, up to and including termination of employment. Any violation of the policy by a temporary worker, contractor or vendor may result in the termination of their contract or assignment with Fort Valley State University

.

Definitions

AES Advanced Encryption System
Fort Valley State University network A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.
Campus connectivity A connection that provides access to the Fort Valley State University network.
EAP-FAST Extensible Authentication Protocol-Fast Authentication via Secure Tunneling: authentication protocol for wireless networks.
EAP-TLS Extensible Authentication Protocol-Translation Layer Security, used to create a secured connection for 802.1X by pre-installing a digital certificate on the client computer.
Enterprise Class Teleworker (ECT) An end-to-end hardware VPN solution for teleworker access to the Fort Valley State University network.
Information assets Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.
PEAP Protected Extensible Authentication Protocol, a protocol used for transmitting authentication data, including passwords, over 802.11 wireless networks.
Service Set Identifier (SSID) A set of characters that give a unique name to a wireless local area network.
TKIP Temporal Key Integrity Protocol, an encryption key that's part of WPA.
WPA-PSK WiFi Protected Access pre-shared key