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

Wireless Security Access Policy and Agreement

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for connecting to Fort Valley State University's internal network(s) or related technology resources via any means involving wireless technology. This can include, but is not limited to, access from the following:

- External hosts via remote access technology (for example, using a wireless router at home to connect to the university via a Virtual Private Network connection).
- Wireless gateways on campus premises .
- Third-party wireless Internet service providers (also known as "hotspots").

The policy applies to any equipment used to access university resources, even if said equipment is not university-sanctioned, owned, or supplied. For example, use of a public library's wireless network to access the university network would fall under the scope of this policy.

The overriding goal of this policy is to protect Fort Valley State University's technology-based resources (such as student and business-related data, computer systems, networks, databases, etc.) from unauthorized use and/or malicious attack that could result in theft or loss of information, damage to critical applications, loss of revenue, and damage to our public image. Therefore, all users employing wireless methods of accessing university technology resources must adhere to university-defined processes for doing so.

Scope

This policy applies to all Fort Valley State University employees, including full-time faculty and staff, part-time faculty and staff, contractors, freelancers, students, and other agents who utilize university-owned, personally-owned, or publicly-accessible computers to access the organization's data and networks via wireless means. Wireless access to university network resources is a privilege, not a right. Consequently, employment at Fort Valley State University does not automatically guarantee the granting of wireless access privileges.

Wireless networks should not be considered a replacement for a wired network. They should be seen solely as extensions to the existing wired network, and are to be used for general purpose access in areas of transient use, such as common areas or meeting rooms. Wireless segments should not be used for work sessions involving any form of access to sensitive organizational data.

Addition of new wireless access points within university facilities will be managed at the sole discretion of the Office of Information Technology. Non-sanctioned installations of wireless equipment or use of unauthorized equipment within the university network system is strictly forbidden.

This policy is complementary to any previously-implemented policies dealing specifically with network access and remote access to the university network.

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

Supported Technology

All wireless access points within the university's firewall will be centrally managed by Fort Valley State University's Office of Information Technology department and will utilize encryption, strong authentication, and other security methods at the Office of Information Technology's discretion. Although the Office of Information Technology is not able to manage public wireless resources, end-users are expected to adhere to the same security protocols while utilizing this equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the university's infrastructure. All campus wireless access points will adhere to the *FVSU Wireless Access Standard*.

The following table outlines Fort Valley State University's minimum system requirements for a computer, workstation or related device to wirelessly connect to Fort Valley State University's systems. Equipment that does not currently meet these minimum requirements will need to be upgraded before wireless connection can be sanctioned by the Office of Information Technology.

	PC and PC-Compliant Computers	**Macintosh Computers**	**Handhelds, PDAs and Portables**
Operating System(s)	Windows XP or any flavor of *nix	OS X or higher	Any WiFi capable device with an SSL and JAVA capable browser
CPU (Type, Speed)	Pentium IV or higher	Any x86 based Mac	
RAM	512 Megabytes		
Disk Space			
Wireless NIC Type(s) (Manufacturer/Model #)			
Wireless Standard(s) (802.11a, b, g, or other)	802.11b/g, 802.11a/n	802.11b/g, 802.11a/n	802.11b/g, 802.11a/n

Eligible Users

When staffing becomes available in the Office of Information Technology to allow for access management, all employees or students requiring the use of wireless access for university purposes must go through an application process that clearly outlines why the access is required and what level of service the employee or student needs should his/her application be accepted. Included in the application will be the request for the individual's mac-address that will be connecting to FVSU network. The Office of Information Technology will define a list of traffic types that are acceptable for use over a wireless connection. More sensitive business activities will be similarly defined, and will be limited to non-wireless environments. Application forms must be approved and signed by the employee's unit manager, supervisor, or department head before submission to the Office of Information Technology.

Employees or students may not use privately owned wireless access points. The university's Office of Information Technology cannot and will not technically support third-party wireless hardware or software, a hotspot wireless ISP connection, or any other wireless resource located outside the university's firewall.

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

Policy and Appropriate Use

It is the responsibility of any employee or student of Fort Valley State University who is connecting to the university's network via wireless means to ensure that all components of his/her wireless connection remain secure. It is imperative that any wireless connection used to conduct Fort Valley State University business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

1. Employees and students using wireless access methods will, without exception, use secure remote access procedures. This will be enforced through public/private key encrypted strong passwords in accordance with Fort Valley State University's password policy. Employees and students agree to never disclose their passwords to anyone. Georgia law 16-9-93 (e) states "*Any person who discloses a number, code, password, or other means of access to a computer or computer network knowing that such disclosure is without authority and which results in damages (including the fair market value of any services used and victim expenditure) to the owner of the computer or computer network in excess of $500.00 shall be guilty of the crime of computer password disclosure.*". Georgia law 16-9-93 (h-1) states that "*Any person convicted of computer password disclosure shall be fined not more than $5,000.00 or incarcerated for a period not to exceed one year, or both.*"

2. All remote computer equipment and devices used for business interests, whether personal- or university-owned, must display reasonable physical security measures. Users are expected to secure their university-connected machines when they are physically at their machines, as well as when they step away. Computers will have installed whatever antivirus software deemed necessary by Fort Valley State University's Office of Information Technology. Antivirus signature files must be updated in accordance with existing university policy.

3. Due to the potential for bandwidth conflicts within the university campus, use of unsanctioned equipment operating within the 2.4 GHz range is strictly forbidden. If you have a need to use such equipment – for example, a cordless phone – please consult the Office of Information Technology before proceeding further.

4. Public wireless hotspots will not be allowed to connect to the university network system.

5. Remote users using public hotspots for wireless Internet access must employ for their devices a university-approved personal firewall, VPN, and any other security measure deemed necessary by the Office of Information Technology. VPNs supplied by the wireless service provider should also be used, but only in conjunction with Fort Valley State University's additional security measures. The Office of Information Technology will support its sanctioned hardware and software, but is not accountable for conflicts or problems whose root cause is attributable to a third-party product.

    - Hotspot and remote users must disconnect wireless cards when not in use in order to mitigate attacks by hackers, wardrivers, and eavesdroppers.
    - Users must apply new passwords every business/personal trip where university data is being utilized over a hotspot wireless service, or when a university device is used for personal Web browsing.

6. Any remote connection (i.e. hotspot, ISDN, frame relay, etc.) that is configured to access Fort Valley State University resources must adhere to the authentication requirements of Fort Valley State University's Office of Information Technology. In addition, all hardware security

   configurations (personal or university-owned) must be approved by Fort Valley State University's Office of Information Technology department.

7. Employees, contractors, and temporary staff will make no modifications of any kind to university-owned and installed wireless hardware or software without the express approval of Fort Valley State University's Office of Information Technology. This includes, but is not limited to, split tunneling, dual homing, non-standard hardware, or security configurations, etc.

8. Employees, contractors, and temporary staff with wireless access privileges must ensure that their computers are not connected to any other network while connected to Fort Valley State University's network via remote access.

9. All connections that make use of wireless access must include a "time-out" system. In accordance with Fort Valley State University's security policies, sessions will time out after twenty minutes of inactivity, and will terminate after one hour of continuous connection on the student wireless, after four hours on the staff wireless, and after four hours on the administrative guest wireless. Both time-outs will require the user to reconnect and re-authenticate in order to re-enter university networks through a wireless connection.

10. The wireless access user agrees to immediately report to his/her manager and Fort Valley State University's Office of Information Technology any incident or suspected incidents of unauthorized access and/or disclosure of university resources, databases, networks, and any other related components of the university's technology infrastructure.

11. The wireless access user also agrees to and accepts that his or her access and/or connection to Fort Valley State University's networks may be monitored to record dates, times, duration of access, data types and volumes in order to identify unusual usage patterns or other suspicious activity. As with in-house computers, this is done in order to identify accounts/computers that may have been compromised by external parties.

12. Any questions relating to this policy should be directed to Del Kimbrough Chief Information Officer in the Office of Information Technology, at (478) 825-6228.

13. The Office of Information Technology reserves the right to turn off without notice any access port to the network that puts the university's systems, data, users, and clients at risk.

Policy Non-Compliance

Failure to comply with the Wireless Security Access Policy and Agreement may result in the suspension of remote access privileges, disciplinary action, and possibly termination of employment.

Employee Declaration

I, _____have read and understand the above Wireless Security Access Policy and Agreement, and consent to adhere to the rules outlined therein.

_____ _____

Employee Signature Date

_____ _____

Manager Signature Date

_____ _____

I.T. Director Signature Date

_____