

Virginia State University
Wireless Network Security Policy
Version 1.1

I. EXECUTIVE SUMMARY

This policy specifies the requirements, expectations and limitations of security for Virginia State University (VSU) wireless network services.

II. AUTHORITY

The Office of Information Technology (OIT) at VSU is accountable for the operation and security of the VSU data network. Specification, configuration, and management of all devices connecting to the VSU network shall remain under the authority and responsibility of OIT.

III. PURPOSE

The effective management of information technology resources is crucially important to the success of the academic, research, and public service missions of Virginia State University. Because of the inherent nature of wireless communication, wireless networks require increased cooperation and coordination between campus entities to maximize the technology's benefits to the students, faculty, and staff of the University, to allow connection to wireless networks in different campus buildings, and eventually, to facilitate the ability to roam from building to building without losing network connectivity.

This document sets forth the policies for using wireless technologies and assigns responsibilities for the deployment of wireless services and the administration of the wireless radio frequency spectrum in a distributed campus network environment. This policy expands the Information Technology Resources Security Policy by including specific direction regarding wireless communications and the resolution of issues that may arise.

This policy is subject to change as new technologies and processes emerge.

IV. REFERENCES

Commonwealth of Virginia:

Virginia State University:

VSU Acceptable Use Policy for Electronic Resources
Information Technology Resources Security Policy
ISSO Minimal Security Requirements and Practices Policy
Network Monitoring Policy
Data Management Policy

The SANS Institute:

An Overview of Wireless Security Issues,
<http://www.sans.org/rr/papers/68/943.pdf>

Cisco Systems Inc:

Cisco Aironet Wireless LAN Security Overview. August 09, 2002,
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
Wireless LAN Security in Depth,
http://www.cisco.com/warp/public/cc/so/cuso/eps0/sqfr/safwl_wp.htm

V. DEFINITIONS

802.11: The Institute of Electrical and Electronics Engineers, (IEEE) 802.11 is a standard introduced by IEEE June 1997 used for wireless Ethernet networks. Below is a listing of each of the wireless IEEE standards currently available.

IEEE 802.11	The initial release of the standard capable of transmissions of 1 to 2 Mbps and operates in the 2.4 GHz band.
IEEE 802.11a	Capable of transmissions of up to 54 Mbps and operates in the 5 GHz band.
IEEE 802.11b	Capable of transmissions of up to 11 Mbps and operates in the 2.4GHz band.
IEEE 802.11c	Defines wireless bridge operations
IEEE 802.11d	Defines standards for companies developing wireless products in different countries.
IEEE 802.11e	Defines enhancements to the 802.11 MAC for QoS.
IEEE 802.11g	Capable of transmissions of up to 20 Mbps and operates in the 2.4 GHz band.

Client hardware/software: Client hardware/software means the electronic equipment and software that is installed in a desktop, laptop, handheld, portable, or other computing device to provide a local area network (LAN) interface to a wireless network.

Coverage: Coverage is the geographical area where a baseline level of wireless connection service quality is attainable.

Interference: Interference refers to the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Interference can slow down or eliminate a wireless transmission depending on the strength of the interfering signal.

IPsec: IPsec is short for IP Security; IPsec is a set of protocols being developed by the Internet Engineering Task Force to support secure exchange of packets at the IP layer.

Information System Security Officer (ISSO): Individual responsible for the development, implementation, oversight, and maintenance of the VSU information security program.

Privacy: Privacy means the condition that provides for the confidentiality of personal, student, faculty and staff communications, and institutional and patient data transmitted over a wireless network.

SSH: Secure Shell is a program for logging into a remote machine and for executing commands on a remote machine. It is intended to replace telnet, ftp (fetch), rlogin and rsh, and provide secure encrypted communications between two untrusted hosts over an insecure network. SSH encrypts all traffic (including passwords) to effectively eliminate eavesdropping, connection hijacking, and other network-level attacks. Additionally, SSH provides a myriad of secure tunneling capabilities, as well as a variety of authentication methods.

Wireless Access Point: Wireless Access Points are electronic hardware devices that serve as a common connection point for users in a wireless network. An access point acts as a network hub that is used to connect segments of a LAN, using transmit and receive antennas instead of physical ports for access by multiple users of the wireless network. Access points are shared bandwidth devices and can be connected to the wired network, allowing access to the campus network backbone.

WEP: WEP is a protocol that adds security to wireless networks based on the 802.11b standard. WEP can either be enabled or disabled. It is designed to afford wireless networks the same level of protection as a comparable wired network. WEP security is based on a scheme called RC4 that involves a combination of secret user keys and system-generated values. The original implementations of WEP used 40-bit encryption that implements a key length of 40 bits and 24 additional bits of system-generated data (64 bits total). Research has shown that 40-bit WEP contains security flaws, and consequently most product vendors today employ 128-bit or above encryption.

Wireless Infrastructure: Wireless Infrastructure consists of wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network.

Wireless Network: A wireless network is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. A standard, IEEE 802.11, specifies the technologies for wireless LANs. The standard includes an encryption method, the Wired Equivalent Privacy algorithm. VSU implements this technology to extend the range of the wired network.

VI. SCOPE

This policy applies to all wireless network devices utilizing VSU Internet Protocol (IP) space (including private IP space within University networks) and all users of such devices, and governs all wireless connections to the campus network backbone, frequency allocation, network assignment, registration in the Domain Name System (DNS), and services provided over wireless connections to the campus network backbone to departments, or divisions of VSU.

VII. POLICIES

- 1.** Virginia State University is the owner of the unlicensed radio frequencies on campus. These include the FCC 2.4 GHz Industrial/Scientific/Medical (ISM) and the 5 GHz Unlicensed National Information Infrastructure (UNII) bands used in wireless networking. OIT is responsible for managing these radio frequencies for the benefit of the University community and may restrict use of any devices that can cause interference in the unlicensed radio frequencies ranges. These include cordless phones, microwave ovens, high voltage audio speakers, etc.
- 2.** OIT is solely responsible for providing wireless networking services on campus. No other department may deploy wireless network access points or other wireless service on campus. Private wireless access points in the dormitories or offices are strictly prohibited.
- 3.** Wireless equipment and users must follow all network connection policies as set forth in this document and all other relevant VSU policies. All provisions of the VSU Acceptable Use Policy for Electronic Resources and the ISSO Minimal Security Requirements and Practices apply to this policy.
- 4.** The University will deploy a campus wireless network, based on the 802.11b/g standards. OIT will work with departments to accommodate special needs, where technically feasible. OIT will collaborate with academic departments where devices used for specific educational or research applications may require specific solutions. If consensus cannot be reached between departments normal escalation processes remain in place via the CIO and ultimately the governing IT committee for resolution.

5. Access to the wireless network will be granted at the same times as the wired network. Access is gained by authenticating the login credentials of the individual attempting access to the Radius server that verifies the given credentials with the E-Directory accounts. E-Directory accounts are established during the creation of GroupWise email accounts, the userid and password combination works for all, E-Directory, GroupWise and Wireless networking.
6. OIT is responsible for maintaining a secure network and will deploy adequate security procedures to support wireless networking on campus.
7. All acceptable use provisions of the Acceptable Use Policy for Electronic Resources and the Information Technology Resource Security Policy apply to wireless network services. Interference or disruption of other authorized communications that result from the intentional or incidental misuse or misapplication of wireless network radio frequency spectrum is prohibited.
8. Wireless access points must abide by all federal, state, and local laws, rules or regulations pertaining to wireless networks.
9. Wireless access points shall require user authentication at the access point before granting access to campus or Internet services. Wireless network interfaces and end-user devices shall support authentication to access wireless networks that allow connectivity to the Campus Network Backbone.
10. Physical security will be considered when planning the location of wireless access point and other wireless network components.
11. Wireless passwords and data must be encrypted. No application should rely on IP address based security or reusable clear text passwords. Other methods may be allowed but require the approval of the Network Security Officer (ISSO).
12. Assume that the link layer offers no security. Use higher-level security mechanisms such as IPsec and SSH for security, instead of relying on WEP. Treat all systems that are connected via 802.11 as external. Place all access points outside the firewall on a separate VLAN. Assume that anyone within physical range can communicate on the network as a valid user. Keep in mind that an adversary may utilize a sophisticated antenna with much longer range than found on a typical 802.11 PC card.
 - a. Wireless networks must be designed and deployed to avoid physical and logical interference between components of different network segments and other equipment. In the event that a wireless device interferes with other equipment, the Network Manager or

Administrator, under the direction of OIT shall resolve the interference as determined by use priority. The arbiter, in case of conflict, is the governing IT committee.

13. It is a violation of this policy for users to attempt to gain unauthorized access to the wireless network or in any way damage, alter, or disrupt the operations of this IT Resource. It is also a violation of this policy for users to tamper with any access control mechanism that could permit unauthorized access, except where expressly required in the performance of their duties and with prior approval of the ISSO.

VIII. ROLES AND RESPONSIBILITIES

Information Systems Security Officer (ISSO) Reports directly to the Chief Information Officer. The governing IT committee is responsible for approving University security policies and plans. The ISSO is responsible for the coordination, review and approval of procedures used to provide the requisite security for Restricted, University Internal or Essential Information Technology Resources. The ISSO has overall coordination responsibility for compliance with this policy. Responsibilities and roles include but are not limited to:

1. The ISSO will attempt to resolve any interference or security incidents by coordinating with the registered Point of Contact (POC) for the wireless network. If a POC is not available, the incident is resolved through administration of the network connection to the backbone.
2. The ISSO is authorized to take whatever reasonable steps are necessary to ensure compliance with this, and other network related policies that are designed to protect the integrity and security of the campus network backbone.

IX. REPORTING

All suspected or actual wireless security breaches must immediately be reported to the OIT helpdesk. Network and System Administrators should report security incidents to the ISSO. If any attempt or actual compromised of a restricted system containing personal or financial information (e.g. credit card information, social security, etc.), the division must also report the event to the University's Security Office.

Disconnect Authorization. Any wireless network on campus, which poses a security threat, may be disconnected from the campus backbone network. If a serious security breach is in process, OIT and the ISSO may disconnect the LAN immediately. Every reasonable attempt will be made to reach the registered "Point of Contact" to resolve

security problems. OIT has the authority to disconnect any wireless network from the campus network backbone whose traffic violates practices set forth in this policy, the Acceptable Use Policy for Electronic Resources Policy, the Information Technology Resources Security Policy, or any other network related policy. It is the responsibility of the departments or division to be knowledgeable regarding the provision of such policies.

The University reserves the right to revoke access to any Information Technology Resource for any user who violates this policy, or for any other business reasons in conformance with applicable University or campus policies.

Grievance matters with this policy or conflicts between OIT and/or the ISSO and any University department, or division are directed to the Chief Information Officer for resolution. If the conflict is not resolved to the satisfaction of OIT or the department, or division, the matter may be escalated to the governing Information Technology Committee for further review and action.