Title: Wireless Security Policy Policy: 6250

Purpose

The Purpose of this policy is to define the high-level specifications for the secure deployment and use of the Virginia State University ("VSU") wireless network. This policy is designed to ensure the optimal performance and security for users of the campus wireless network infrastructure.

Guiding Principles

The following principles guide the development and implementation of the VSU Wireless Security Policy.

a. The VSU Wireless Security Policy aims to:
   I. Ensure the confidentiality, integrity and availability of VSU information;
   2. Protect against any anticipated threats or risks to the security or integrity of the information; and
   3. Protect against unauthorized access to or use of the information that could result in harm to the University, data owners or users.

Scope of Policy

The policy applies to all users in all departments and facilities. Additionally, this policy covers all wireless network equipment and infrastructure that is owned, leased or operated by the University.

Wireless Policy Statement

The following principles guide the development and implementation of the VSU Wireless Policy:

A. It is the policy of the University that the high-level specifications listed below are employed for the protection and use of the wireless network.
B. Wireless LAN (WLAN) Connectivity on the VSU Enterprise Network
These requirements will be met in the deployment, configuration and administration of WLAN Infrastructure connected to any internal VSU network:

Authority, Responsibility, and Duties

A. VSU's Technology Services Depa11ment is responsible for the secure configuration and deployment of wireless networks, hotspots, and wireless bridging as outlined in this policy.
B. The users' are responsible for adhering to the policy requirements as set forth in this document and for requesting exceptions as business needs dictate.
C. The VSU Technology Services Depai1ment (i.e. system administrators) are responsible for monitoring the wireless networking infrastructure to ensure the policy provisions are being adhered to and to assist

in ensuring the computing safety of the users. The system administrators are also responsible for monitoring the wireless networking infrastructure to ensure the protection of the University assets.

Definitions

The IT security definitions and terms can be found in the COV ITRM IT Glossary. It is referenced on the ITRM Policies, Standards, and Guidelines web page on www.vita.vin:inia.gov/librarv.

The terms "client and/or user" are used interchangeably throughout the document, but pertain specifically to the end user of the network infrastructure.

Policy

C. Internal Wireless Network and Associated Infrastructure:

It is the policy of the University that these requirements are met in the deployment, configuration and administration of WLAN infrastructure connected to any internal VSU network:

1. Client devices connecting to the internal VSU WLAN utilize two-factor authentication (i.e., digital certificates and Active Directory);
2. Internal WLAN infrastructure authenticates each client device prior to permitting access to the internal WLAN;
3. Internal LAN user authorization infrastructure (i.e., Active Directory) is used to authorized access to internal LAN resources;
4. Only VSU owned or leased equipment are granted access to utilize the internal VSU WLAN (in other words, **no** "Bring Your Own Device" access to the internal network will be allowed);
5. All internal WLAN connected devices must utilize secure encryption that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption keys multiple times during the said session. A connected device must also provide support for secure encryption protocols (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
6. Physical or logical separation between WLAN and wired LAN segments exists;
7. All VSU WLAN access is monitored for malicious activity, and associated event log files are stored on a centralized storage device;
8. Configuration and security data associated with the internal WLAN are not provided to Unauthenticated devices. Such as, determining DHCP addresses being issued by an access point;
9. WLAN clients only permit infrastructure mode communication.
10. Devices and access to the internal network will not be shared by the user with others (regardless of mode of sharing i.e. sharing accounts/passwords or sharing the device).

11. The users do not have any expectation of privacy of his or her communications on the VSU internal wireless network and infrastructure.
12. Knowingly, broadcasting any WLAN channel or SSID that interferes with VSU's WLAN is strictly prohibited.

D. WLAN Hotspot (Wireless Internet)

For wireless networks which only provide unauthenticated access to the Internet, VSU implements the following security:

1. WLAN Hotspots have logical or physical separation from the agency's LAN;
2. WLAN Hotspots have packet filtering capabilities enabled to protect clients from malicious activity;
3. All WLAN Hotspots access and traffic are monitored for malicious activity, and log files are stored on a centralized storage device; and
4. Where VSU clients are concerned, WLAN clients only permit infrastructure mode communication.
5. Users do not have any expectation of privacy or confidentiality on the WLAN Hotspot.
6. Any and all default accounts (administrator and guest) for the Hot Spot Access Point(s) has been disabled and/or the default password for that account has been changed.
7. "Bring Your Own Device" devices are required to connect to the guest WLAN. Users acknowledge compliance to same in the VSU Acceptable Use Policy.

E. Wireless Bridging

The following network configuration are used when bridging two wired LANs.

1. All wireless bridge communications utilizes a secure encryption that provides an automated mechanism to change the encryption keys multiple times during the connected session and provides support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);
2. Wireless bridging devices do not have a default gateway configuration;
3. All default administrator accounts on the wireless bridging devices are disabled;
4. Wireless bridging devices are physically or logically separated from other networks;
5. Wireless bridge devices only permit traffic destined to traverse the bridge and do not directly communicate with any other VSU network;
6. Configuration and security data associated with the WLAN are not provided to unauthenticated devices.
7. Knowingly, broadcasting any WLAN channel or SSID that interferes with VSU's WLAN is strictly prohibited.
8. Wireless bridging devices are not configured for any other service than bridging (i.e., a wireless access point).

9. Users do not have any expectation of confidentiality or privacy for any of the traffic and communications that is communicated on the wireless bridges.

Exceptions to Wireless Policy Requirements

If the user determines that compliance with the provisions of this policy or any related information security policy would adversely impact a business process of the agency, the user may request approval to deviate from a specific requirement by submitting an exception request to the VSU ISO. For each exception, the requesting the data owner shall fully document:

1. The business need,
2. The scope and extent,
3. Mitigating safeguards,
4. Residual risks, and
5. The specific duration

Each request shall be in writing to the VSU ISO and approved by the VSU CIO indicating the acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. The requesting user will be informed of the action taken. An exception will not be accepted for processing unless all residual risks have been documented. Denied exceptions may be appealed to the CIO of VSU. The form to document exceptions requests is included in Attachment A of this document.

Once the exception request is approved by the VSU CIO, the request is then submitted to the President of VSU for signature and submitted to VITA Commonwealth Security and Risk Management for final approval by the COV CISO.

Exemptions from Applicability
Not applicable.

Policy Review
This policy will be reviewed every two years on the anniversary of the policy effective date or more frequently as needs of the University warrants.

Violations of Policy
Violation of this policy may result in:

- Disciplinary action under the Virginia Department of Human Resources Policy 1.60, Standards of Conduct (4/16/08, 6/1/11)
- Prosecution under "Virginia Computer Crimes Act." § 18.2-152.1.
- Any other applicable law that may have been breached by the user

References

Virginia Information Technology Agency (VITA):
Information Security Standards (SEC501-09) (02/20/2015)

NIST Special Publications
Recommend Security Controls for Federal Information Systems and Organizations SP 800-53, Rev. 4.

Approval By: _____ Date: 5/10/16
President