

Virginia Commonwealth University Technology Services

Security Standard for VCU's Wireless Network

Effective Date: April 19, 2007
Compliance Date: November 2007
Scheduled Review: November 2008

Revisions:

Version	Date	Revision Issuance
1	April 2007	Initial draft
2	January 2008	Revisions

Scope:

This standard covers the use and operation of enterprise-wide wireless connectivity on the VCU campuses and includes all wireless equipment with the exception of specialized in-facility wireless connectivity such as robotics or research data collection applications.

Definition:

This standard applies to all users who access the VCU wireless network.

Applied Industry Best Practices of:

- National Institute of Standards Technology (NIST)
- Center for Internet Security Consensus Security Benchmarks
- SANS Institute Password Best Practices and Policy Template

Requirements of the Standard

- Only VCU authorized Access Points may be used for wireless connectivity on the VCU campuses. Other Access Points are considered to be rogues and their use is prohibited due to the security threats they present and the interference they propagate with legitimate VCU wireless equipment.
- Access to the VCU wireless network must be done via authentication using the eID credentials (user ID and password). This authentication is done on a secure web page that is presented upon accessing the VCU wireless network. Short term guest IDs are available through the Technology Services Help Desk or departmental IT support staff.
- With the exception of the logon web page, general traffic on the VCU wireless network is not encrypted and must not be used for the transmission of confidential data. If there is a requirement to transmit confidential or sensitive data on the wireless network, other technologies such as VPN must be used. See the VPN Security Standard for further information.

Enforcement

Violation of this standard could result in loss of access to the wireless network or personnel disciplinary actions.

Exceptions

Requests for exceptions to the requirements of this standard should be made to the VCU Chief Information Officer. Please use the Security Standard Request for Exception form that is located on the VCU security website and send the completed form to the VCU Chief Information Officer.

Review Frequency: Annually or as needed.
Authority: VCU Chief Information Officer
VCU Information Security Officer

In Compliance with: COV ITRM Information Technology Security
Management Standard SEC 501-01
VCU Computer and Network Resources Use Policy