Purpose

This policy specifies the requirements, expectations and limitations of security monitoring of the Virginia State University (VSU) network and all attached devices. The purpose of this policy is to outline the network security scanning conducted by the Office of Information Technology (OIT) at Virginia State University. OIT shall utilize as many monitoring applications and appliances to perform electronic scans of VSU campus or on any system connected to it.

Scans may be conducted to:

- Ensure integrity, confidentiality, and availability of information and resources;
- Evaluate security measures in place protecting the network (wired and wireless);
- Test know system vulnerabilities;
- Penetrate network resources;
- Investigate possible security incidents;
- Ensure conformance to VSU security policies; and
- Monitor user or system activity where appropriate.

Authority, Roles, and Responsibilities

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.

Policy Statements

VSU hereby provides its consent to allow the VSU Information Security Officer (ISO) to access its networks and/or firewalls to the extent necessary to perform the scans authorized in this policy. The VSU Network and System Administrators shall provide protocols, addressing information, and network connections sufficient for the ISO to utilize the software to perform network scanning.

This access may include:

a. User level and/or system level access to any computing or communications device,
b. Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on VSU equipment or premises;

c. Access to work areas (labs, offices, storage areas, etc.);

d. Access to individual user's personal computer if attached to the VSU network by any electronic means; and

e. Access to interactively monitor and log traffic on VSU networks.

Definitions

A. Information Security Officer (ISO) is an individual responsible for the development, implementation, oversight, and maintenance of the VSU information security program.

B. Scan is the act of systematically scanning a computer's ports. Since a port is a place where information goes into and out of a computer, port scanning identifies open doors to a computer. Port scanning has legitimate uses in managing networks, but port scanning also can be malicious in nature if someone is looking for a weakened access point to break into your computer.

C. Sniffer is a program to capture data across a computer network. It is used by hackers to capture user id names and passwords. Software tools that audits and identifies network traffic packets. It is also used legitimately by network operations and maintenance personnel to troubleshoot network problems.

Enforcement

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.

References

Virginia Information Technology Agency (VITA):
Information Technology Security Standard (ITRM Standard SEC501-01)
Virginia State University (VSU):
Policy 6520: Acceptable Use Policy
Policy 6420: Electronic Records and Retention Policy
Policy 6110: IT Resource Security Policy
Policy 6640: Network Monitoring Policy
Policy 6530: Security Awareness Training Policy
Policy 6540: Access Determination and Control Policy
Policy 6310: Banner Security Policy
Policy 6630: Data Breach Notification Policy
Policy 6620: IT Security Handling Policy

APPROVED BY: [Signature]
President

Date: 1/28/08