

Periodic Testing of Security, Systems and Processes

Date: 06/12/06

Policy ID: UVAW - 10

Status: Approved

Contact Office: Department of Information Technology

Oversight Executive: Director of Information Technology

Applies to: University of Virginia's College at Wise Networks and Systems

Reason for Policy: To test the security and vulnerabilities of the UVa-Wise networks, systems and resources thereby assisting administrators in providing optimal protection against threats.

Definitions:

Policy Statement: New vulnerabilities come to light every day in one way or another, whether as a software flaw or a faulty network device/medium. Testing and auditing the networks and systems will provide a method of identifying these vulnerabilities before they are exploited.

Procedures:

- 1.0 Periodically test the security, systems and processes of the networks
 - 1.1 Devices and networks containing sensitive data shall receive periodic security audits and testing
 - 1.2 Internal and external vulnerability scans shall be done at least quarterly.
 - 1.3 Penetration testing of network infrastructure shall be done at least annually.
 - 1.4 IDS and IPS shall be updated regularly and audited to ensure optimal protection.
 - 1.5 Systems will be continually monitored to ensure CIA (confidentiality, integrity, and accessibility)

Related Information: See also PCI Network Testing Policy PCI – 11

Background: Approved by Brian Ward, CIO - UVa-Wise, June 13, 2006