Audit Vulnerability Scan Policy

1.0 Purpose

The purpose of this policy is to set forth the requirements regarding network security scanning at Duke University's Fuqua School of Business. Duke University's Office of Information Technology (OIT) and/or the Fuqua IT Infrastructure Team shall utilize software to perform electronic scans of Fuqua's networks and/or firewalls or any computer system or IP addressable device at Fuqua.

Audits may be conducted to:

- Ensure integrity, confidentiality and availability of information and resources
- Investigate possible security incidents
- Ensure conformance to Fuqua security policies
- Monitor user or system activity where appropriate.

2.0 Scope

This policy covers all computer and communication devices owned or operated by Fuqua. This policy also covers any computer and communications device that are present on Fuqua premises, but which may not be owned or operated by Fuqua.

3.0 Policy

When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of OIT or the Fuqua IT Infrastructure Team. Fuqua hereby provides its consent to allow OIT to access its networks and/or firewalls to the extent necessary to allow OIT to perform the scans authorized in this policy. Fuqua shall provide protocols, addressing information, and network connections sufficient for OIT to utilize the software to perform network scanning.

This access may include:

- User level and/or system level access to any computing or communications device
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted or stored on Fuqua equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on Fuqua networks.

3.1 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. Fuqua releases OIT of any and all liability for damages that may arise from network availability restrictions caused by the network scanning, unless such damages are the result OIT's gross negligence or intentional misconduct.

3.2 Client Point of Contact During the Scanning Period. Fuqua shall identify in writing a person to be available if the OIT Scanning Team has questions regarding data discovered or requires assistance.

3.3 Scanning period. Fuqua and the OIT Scanning Team shall identify in writing the allowable dates for the scan to take place.

4.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

5.0 Revision History

Date	Who made the revision	Change made
2012-02-06	Fuqua Infrastructure	Initial issue

This document was adapted from a draft created by the SANS Institute and is used by permission of the SANS Institute.