Audit Vulnerability Scan Policy

Created by or for the SANS Institute. Feel free to modify or use for your organization. If you have a policy to contribute, please send e-mail to stephen@sans.edu

1.0 Purpose
The purpose of this agreement is to set forth our agreement regarding network security scanning offered by the <Internal or External Audit Name> to the <Company Name>. <Internal or External Audit Name> shall utilize <Approved Name of Software> to perform electronic scans of Client's networks and/or firewalls or on any system at <Company Name>.

Audits may be conducted to:

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

2.0 Scope
This policy covers all computer and communication devices owned or operated by <Company Name>. This policy also covers any computer and communications device that are present on <Company Name> premises, but which may not be owned or operated by <Company Name>. The <Internal or External Audit Name> will not perform Denial of Service activities.

3.0 Policy
When requested, and for the purpose of performing an audit, consent to access needed will be provided to members of <Internal or External Audit Name>. <Company Name> hereby provides its consent to allow of <Internal or External Audit Name> to access its networks and/or firewalls to the extent necessary to allow [Audit organization] to perform the scans authorized in this agreement. <Company Name> shall provide protocols, addressing information, and network connections sufficient for <Internal or External Audit Name> 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 <Company Name> equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.)
- Access to interactively monitor and log traffic on <Company Name> networks.

3.1 Network Control.
If Client does not control their network and/or Internet service is provided via a second or third party, these parties are required to approve scanning in writing if scanning is to occur outside of the <Company Name's> LAN. By signing this agreement, all involved parties acknowledge that they authorize of <Internal or External Audit Name> to use their service networks as a gateway for the conduct of these tests during the dates and times specified.

3.2 Service Degradation and/or Interruption. Network performance and/or availability may be affected by the network scanning. <Company Name> releases <Internal or External Audit Name> 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 <Internal or External Audit Name>'s gross negligence or intentional misconduct.

3.3 Client Point of Contact During the Scanning Period. <Company Name> shall identify in writing a person to be available if the result <Internal or External Audit Name> Scanning Team has questions regarding data discovered or requires assistance.

3.4 Scanning period. <Company Name> and <Internal or External Audit Name> 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

29 September 2003, updated to include National Association of State Auditors, Comptrollers, and Treasurers; the National Association of Local Government Auditors; the U.S. General Accounting Office; and U.S. Inspectors General Legal and Reporting Considerations.