# <Company Name>
# Vulnerability Assessment 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. Overview

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective vulnerability management. Vulnerability assessment provides visibility into the vulnerability of assets deployed in the network. Vulnerability assessment consists of scanning to identify networked assets, determine potential vulnerabilities and assessment of potential vulnerabilities. Remediation of the vulnerabilities is another facet of vulnerability management.

## 2. Purpose

To permit authorized <Company Name> personnel to perform information security vulnerability assessment for the purpose of determining areas of vulnerability.

## 3. Scope

Vulnerability Assessments can be conducted on any asset, product or service within <Company Name>.

## 4. Cancellation or Expiration

The policy in this document does not have an expiry date. However, this document is reviewed and updated as required annually.

## 5. Policy

The development, implementation and execution of the vulnerability assessment process is the responsibility of the Security Operations area under the authority of the Chief Security Officer (CSO).

Periodic or continuous vulnerability assessment scans will be performed on all network assets deployed on <Company Name> IP address space.

A centrally managed vulnerability assessment system will be deployed. Use of any other network based tools to scan or verify vulnerabilities must be approved, in writing, by the Security Operations manager via the Security Assessment Authorization Form.

Assessment of vulnerabilities is the joint responsibility of Security Operations and the area responsible for the asset, product or service being assessed.

<Company Name> personnel are expected to cooperate fully with any vulnerability assessment being conducted on systems for which they are held accountable.

<Company Name> personnel are further expected to cooperate with the Security Operations area in the development of a remediation plan.

Any vulnerability scans or follow-up activities, performed outside of the centrally managed vulnerability assessment tool, required to assess vulnerabilities must be approved, in writing, by the Security Operations manager via the Security Assessment Authorization Form.

The Security Operations manager is permitted, with approval of the CSO, to hire third-party security companies to run external vulnerability scans against externally deployed <Company Name> assets, products or services.

## 6. Vulnerability Assessment Process

For additional information, go to the Vulnerability Assessment Process.

## 7. Exceptions

Any exceptions to this policy, such as exemption from the vulnerability assessment process, must be approved via the Security Exemption Process.

## 8. Enforcement

Any <Company Name> personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment and potentially legal action.

## 9. Related Documents

The following documents are referenced by this policy:

- Vulnerability Assessment Process
- Security Exemption Process
- Security Assessment Authorization Form

## 10. Revision History

| Version | Date of | Author | Description of Changes |
|---|---|---|---|

| | Revision | | |
|---|---|---|---|
| 1.0 | 2006 | Unknown | Initial Version |
| 1.1 | 7 May 2012 | Rick Wanner | Revision |