



## Vulnerability Assessment and Penetration Testing Policy

<b>Issue Date:</b> 6/2/05	<b>Approved By:</b> Laurie Scheich, AVP Auxiliary Services
<b>Effective Date:</b> 6/2/05	<b>Review Date:</b> May, 2007

### Background

To properly secure this organization's information technology assets, the information security team is required to assess our security stance periodically by conducting vulnerability assessments and penetration testing. Only with knowledge of these vulnerabilities can our organization apply security fixes or other compensating controls to improve the security of our environment. Several tools (including but not limited to Nmap, Nessus, and password quality assessment tools) are instrumental in assessing risk and can also act as an early warning system for new attacks. (Supporting documentation may be viewed at <http://www.auxs.umn.edu/asis/security/index.htm>)

### Purpose

The purpose of this policy is to grant authorization to appropriate members of our information security team to conduct vulnerability assessments and penetration tests against this organization's assets. The Security Assessment Authorization Form (see reverse) shall be used to control who may perform these tasks. Authorization to scan the computer assets of a given department may be granted by the departmental manager/director. Authorization to globally scan all Auxiliary Services machines must be granted by the Associate-VP for Auxiliary Services or assignee.

These activities involve scanning Auxiliary Services and Auxiliary Services Departmental desktops, laptops, servers, network elements, and other computer systems owned by Auxiliary Services on a regular, periodic basis to discover vulnerabilities present on these systems. IS Staff will take reasonable care to not disrupt services. Departmental IS staff will be notified in all non-emergency instances in advance of testing.

All extensive security scans that have any potential of causing a system (or a service on a system) to behave erratically will have advance notification and coordination of efforts before performing these types of scans.



# Security Assessment Authorization

Employee Name: _____	Department: _____
----------------------	-------------------

Has authorization to perform the following security assessment tasks:

Assessment	
Nmap Port Scans	Yes / No
Nessus Vulnerability Scans	Yes / No
Password Quality Assessment	Yes / No
Other: (please describe below)	Yes / No

---



---



---

Has authorization to perform the above tasks on the following systems: (select only one)

All Auxiliary Services Computers (requires A-VP signature or equiv)	Yes / No
Computers Owned by the following Department(s) (list below)	Yes / No

---



---



---

I have read the Vulnerability Assessment and Penetration Testing Policy and agree to comply with it and understand that I may perform the tasks listed above in the normal course of my duties:

Employee Signature \_\_\_\_\_ Date: \_\_\_\_\_

Authorized Signature \_\_\_\_\_ Date: \_\_\_\_\_

This permission is granted for the above employee until modified or revoked or until the employee terminates employment with Auxiliary Services.