

 <p>Category: Information Technology</p> <p>Policy applicable for: Faculty/Staff/Student</p>	<p><i>Policy Title:</i> Vulnerable Electronic Systems</p> <p>Effective Date: 01/04/2008</p> <p>Prior Effective Date: N/A</p> <p>Enabling Acts: ISO 17799:2005, COBIT, NIST SP 800-68</p>	<p><i>Policy Number:</i> 9.1.2</p> <p>Policy Owner: Director, Information Security</p> <p>Responsible Office(s): Information Security</p>
---	--	--

Background

Students, faculty and staff at the University of Cincinnati generate massive amounts of sensitive information. From personal data covered by Federal regulations (such as FERPA, HIPAA or GLBA) to financial information to research results, the networks and systems at UC are filled with information and data that should remain confidential. As such, UC must work to continuously improve the security posture of its systems and the sensitive information on those systems. The purpose of this policy is to ensure that UC infrastructure is protected against the top threats as defined monthly by SANs, ISS, Microsoft and other best in breed security companies. This policy creates a program of continuous vulnerability assessment and provides a process to drive remediation of any serious issues discovered.

Policy

UC Information Security is responsible for conducting various vulnerability tests on a regular and ongoing basis. These tests are to be conducted using tools & methods and on a schedule determined by the Director of Information Security. The tests will assess vulnerabilities across the UC infrastructure that are determined by the industry as the vulnerabilities of highest concern. The vulnerability tests will be conducted in such a way as to cause no or little user noticeable impact to system performance. Vulnerabilities discovered during testing will be classified as to severity and reported to the owners of the systems tested.

Severity classifications to be used are:

- **Catastrophic** – A system that places the other components and/or data that reside on the UC infrastructure at significant risk; An attack that exploits this vulnerability is already spreading across the internet.
- **Critical** – A system that is easily accessible, requires little or no authentication, and will provide the ability to access confidential information, corrupt/delete data, or create a system outage; a system containing a vulnerability for which an exploit exists and that provides significant risk to the affected system or the infrastructure on which it resides.

No system connected to UCNNet should be used to perform network scans on any subnets or computer systems except under the following conditions:

- The scans are conducted by UC Information Security
- The scans are conducted by the owners of the system and the machines on the subnet being scanned
- The scans are conducted by UC Internal Audit during the course of an audit of the department owning the system or machines on the subnet

When the owner of a system or subnet is going to perform a scan of their devices they should contact UC Information Security before hand to inform them of the activity.

Remediation of vulnerabilities:

- Results of system test will be provided to the system owner. If the owner can not be identified, the report will be sent to the IT coordinator for the site. If a vulnerability is found and reported, the steps required to remedy the problem will also be provided. It is expected that all vulnerabilities categorized as Critical or Catastrophic be resolved within ninety (90) days of the system owner receiving initial notification.
- After the 90-day mark, systems that contained Critical or Catastrophic vulnerabilities will be retested. If the vulnerabilities have not been resolved, they will be re-reported to the system owner and also reported to the administrative head of the functional area. System owners will be given an additional ninety (90) days to take the necessary remediation steps.
- 180 days after the original test, systems that had Critical or Catastrophic vulnerabilities will be retested once again. Any system that continues to show the originally discovered Critical or Catastrophic vulnerability after this retest will be disconnected from the UC network until remediation is complete.
- In cases where the system owner or his/her manager feels that remediation of a critical vulnerability is not needed, Information Security will notify the VRB with an e-mail summary of the situation, requesting the VRB make a final decision on whether or not remediation is necessary.
- In the rare case where a vulnerable system is being used to commit a crime (phishing, money laundering, etc.) UC Information Security has the right to remove it from the network immediately and seize the machine as evidence for local or federal law enforcement agencies.

Audience:

This policy applies to all organizations and individuals associated with UC.

Definitions:

Vulnerability: A weakness in a system allowing an attacker to violate the confidentiality, integrity, availability, access control, consistency or audit mechanisms of the system.

Vulnerability Assessment: The process of identifying and quantifying vulnerabilities in a system. Assessments are typically performed according to the following steps:

1. Cataloging assets and capabilities (resources) in a system
2. Assigning quantifiable value and importance to the resources
3. Identifying the vulnerabilities or potential threats to each resource
4. Mitigating or eliminating the most serious vulnerabilities for the most valuable resources

Exploit: Software, data, or a sequence of commands that takes advantage of a vulnerability in order to get unintended or unanticipated behavior out of computer software, hardware, or something electronic (usually computerized). This frequently includes such things as gaining control of a computer system or allowing privilege escalation or a denial of service attack.

Threat: An action that can cause harm to systems, data or other resources.

Attack: An action taken to actively exploit a vulnerability. Attacks are designed to prevent systems from being used, to steal or manipulate organizational data or to discover system passwords and business logon functions.

Remediation: To remove or otherwise address vulnerabilities so that the system is no longer exploitable by an attacker. Remediation can also refer to putting controls in place to minimize the chance of an attacker exploiting a vulnerability on the system.

Vulnerability Review Board (VRB): A group comprised of 12 UC Network System Administrators and UC Technology Coordinators who mediate when debate occurs over remediation of a particular critical vulnerability

Procedure:

ISO 17799:2005	International Standards Organization for Information Security
COBIT	ISACA Audit Controls Objective for IT
NIST SP 800-68	National Institute of Standards and Technology Guide for Windows IT administrators
PCI	Payment Card Industry Standards

Related links:

- [International Standards Organization 17799:2005](#)
- [Control Objectives for IT](#)
- [NIST Special Publication 800-68](#)
- [Payment Card Industry Standards](#)

Phone Contacts:

UC Information Security	8-ISEC
Director, Information Security	6-9177
UC Office of the CIO	6-2228

Disciplinary Actions:

Violation of this policy may result in revocation of network access for the effected system(s). Violation of this policy may also result in disciplinary action which may include termination for employees and temporaries; a termination of employment relations in the case of contractors or consultants and dismissal for interns and volunteers. Additionally, individuals are subject to loss of University of Cincinnati Information Resources, access privileges, civil, and in some cases criminal prosecution.