

Title: Vulnerability Assessment Policy

1.0 Overview

Almost daily new vulnerabilities are discovered in computer operating systems, network devices and application software. These vulnerabilities may be exploited by hackers and malicious logic. This exploitation may lead to loss of availability, confidentiality and integrity of data residing on the exploited systems as well as providing a launching point for exploitation of additional Middle Georgia State University network computing resources.

The Office of Network Administration is responsible for ensuring the integrity, confidentiality, and availability of Middle Georgia State University network computing resources, while minimizing the impact of security procedures and policies upon institute productivity.

2.0 Purpose

To empower the Office of Network Administration to perform information security vulnerability assessments for the purpose of determining areas of vulnerability, and to initiate appropriate fix action.

3.0 Scope

Vulnerability assessments can be conducted on any entity within Middle Georgia State University or any outside entity that has been issued Middle Georgia State University IP addresses.

4.0 Policy

The Office of Network Administration will perform vulnerability assessments on all Middle Georgia State University network computing resources to identify and eliminate or mitigate known vulnerabilities.

Vulnerability assessments may be performed periodically on all Middle Georgia State University network computing resources and when a systems security posture changes. Changes which affect a systems security posture include initial operating system installation and subsequent reloads, firewall access requests and significant configuration changes.

Identified vulnerabilities will be reported to the system administrator for fix action. The execution, development and implementation of fix actions is the joint responsibility of The Office of Network Administration and the department responsible for the systems being assessed. Employees are expected to cooperate fully with any vulnerability assessment being conducted on systems for which they are held accountable. Should accountability be in question it is the responsibility of the department chair to designate someone.

The system administrator for the system will be given a deadline for completion of the fix action. In the event that the fix action will not be complete by the deadline, the Office of Network Administration must be notified and given the following information:

Contact Name:

Contact Phone Number:

Contact Email address:

Contact's Department:

System IP address(s):

Reason for not completing a fix action by the deadline:

Date when fix action will be complete:

Measures taken to mitigate exposure of the identified vulnerabilities:

5.0 Enforcement

The Office of Network Administration may take actions necessary to mitigate the exposure of any vulnerabilities not corrected by the deadline, including but not limited to restricting access to the system through the firewall, removing DNS registration, deactivating network ports and other action.

Any systems not fixed by the deadline will be reported to the CIO for review.

6.0 Definitions

Terms	Definitions
Entity	Any institute unit, department, group, or third party, internal or external to Middle Georgia State University, responsible for maintaining Middle Georgia State University assets.
Vulnerability	Those factors that could affect confidentiality, availability, and integrity of Middle Georgia State University's key information assets and systems.
Malicious Logic	ComputerUser.com High-Tech Dictionary at http://www.computeruser.com defines malicious logic as "Logic (hardware or software) that is purposely introduced into a system with harmful intent."
CIO	Chief Information Officer
Network Computing Resources	The network, computers and any network connected device.
IP	Internet Protocol
System Administrator	The person held accountable for the system.

7.0 Revision History

11/13/2002 - Original

01/28/2013 - Changed institution name to reflect consolidation

08/04/2015 - Changed institution name to reflect University status