Title: Security Updates 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 other Middle Georgia State University network computing resources.

2.0 Purpose
To develop a standard that will maintain system security patches with minimal effort.

3.0 Scope
This document covers all computer systems owned, operated or maintained by Middle Georgia State University and any third party computers connecting to Middle Georgia State University networks.

4.0 Policy

All computer systems connecting to Middle Georgia State University networks must be maintained with current security patches. This requirement specifically includes all LAN, WAN, Dial-up, VPN and Wireless access methods.

Standard

The Office of Technology Resources (OTR) is responsible for maintaining security patches on the workstations it supports. OTR may enable automatic software updates either locally or via a centrally managed software updates server to accomplish this task. When security patches are centrally managed, they will be tested on a small group of computers prior to being fully deployed.

Administrators of servers on the Middle Georgia State University network are responsible for maintaining security patches on their servers.

Personal computer owners who connect their computers to the Middle Georgia State University network are responsible for maintaining security patches on their computers. They must configure their computers to do one of the following in order of preference:

- Automatically download the updates, and install them
- Automatically notify the user of available updates

5.0 Enforcement
Active directory group policy will enforce automated update settings on Middle Georgia State University owned, operated or maintained computers running Windows 2003/XP/2008/7 or later.

Per the “Vulnerability Scan Policy”, systems will be audited periodically to ensure system administrators are maintaining security patches adequately.

Without notice, the Office on Network Administration may temporarily suspend or limit network connections or accounts of any user or system considered to be in violation of this policy until the violation is resolved.

The Office of Network Administration or the CIO must approve any waiver of these requirements.

6.0 Revision History

04/20/2006 - Original
04/18/2013 - Changed institution name to reflect consolidation
04/18/2013 - Removed configuration instructions for each operating system
08/04/2015 - Changed institution name to reflect University status