MONTREAT COLLEGE

Vulnerable Electronic Systems Policy

Effective:
September 2, 2016

Purpose

Vulnerability management is an essential component of any information security program and the process of vulnerability assessment is vital to effective management. Vulnerability assessments are used as a means of identifying assets connected to the college's network and the weaknesses associated with them, as well as assessing the risk of those weaknesses. After identification, the next step is to take measured and documentable steps to remediate these vulnerabilities. Montreat College strives to continually improve its security posture to protect the integrity of data assets and the security of the college community.

Policy

All college owned or operated computer systems and devices must be protected through the deployment and installation of software patches, service packs, and hot fixes. Campus Technology is responsible for monitoring the latest update releases, applying them on a regular schedule, and checking to ensure the completeness and effectiveness of their patching processes. Critical security patches, as deemed by the vendor, must be installed on applicable systems within 14 days of release. Non-critical patches should be deployed as soon as possible, but no later than 30 days after release. All security patches must be installed unless testing against critical systems results in system instability or reduction in needed functionality. Exceptions must be documented including a plan of action to eliminate the exception.

Prior to the implementation of a new system or major change of an existing system on Montreat College's network, a vulnerability scan must be performed using a centrally managed vulnerability scanner, any discovered vulnerabilities remediated, and proof of remediation retained. When using a standard image that has been tested and deemed appropriate, no further scan is necessary in those instances.

Campus Technology will conduct periodic or continuous vulnerability assessments of college systems. Targeted vulnerability assessments may also be implemented on an as-needed basis, determined and administered exclusively by Campus Technology or an authorized entity discussed below. A centrally managed vulnerability assessment system will be utilized and administered by Campus Technology. Vulnerability assessments will be conducted in such a way as to cause minimal noticeable impact to college operations. Use of any other network-based tools to scan or verify vulnerabilities must be approved in advance by Campus Technology. Once vulnerability assessments have been conducted, Campus Technology will be responsible for the remediation of any discovered vulnerabilities.

Campus Technology may engage with third parties to conduct internal or external vulnerability assessments or penetration testing as necessary. Campus Technology reserves the right to remove or isolate vulnerable assets from the college's network at any given time without prior communication. Once the cyber threat is contained, Campus Technology will work to seek a resolution.

Contact Information

Campus Technology
Phone: 828-669-8012 Ext. 3663
Email: support@montreat.edu

Revision History

Initial Draft: 08/18/2016
Revised: 09/02/2016