Office of Information Technology

IT Standard

VULNERABILITY STANDARD

Standard:	IT06001
Original Effective Date:	03/28/2012
Last Revised:	02/28/2019
Last Reviewed:	04/06/2022
Next Scheduled Review Date:	04/30/2023
Version No.:	1.1
Administrative Owner:	Director of Information Security Services

PURPOSE

Montgomery College ("College") information technology resources and digital business information are critical to the administrative business and academic success of its students. The task of protecting these resources in compliance with the Board of Trustees approved policy and applicable Federal and State laws and regulations is the responsibility of the Office of Information Technology (OIT).

This standard defines the manner in which the OIT Security Group (ITSG) identifies vulnerabilities in college technology resources and coordinates work within OIT to correct the vulnerabilities and reduce the risk of malicious attacks against the College network and/or applications.

SCOPE

This standard applies to all college technology resources (servers, workstations, printers, applications, switches, routers, etc.) regardless of the location of the technology resource. The standard applies to Montgomery College employees who identify vulnerabilities through scans or other means, and the employees, contractors, and vendors who oversee implementation, maintenance, and support of College technology resources.

DEFINITIONS

Term	Definition
Approved Scanning Vendor (ASV)	Organizations that have been approved by the Payment Card Industry (PCI) Standards Council to validate adherence to the Data Security Standards (DSS) requirements through performing vulnerability scans of Internet facing environments of merchants and service providers.
Contractor or OIT Contractor	An individual representative of a business external to Montgomery College who has been hired by the OIT and assigned to an OIT work group for a set period of time to supplement its work staff. The individual may reside either at an OIT facility or at an offsite facility not within the College boundaries. The individual reports directly to a College OIT supervisor or manager in addition to their own business management.
PCI DSS	Payment Card Industry Data Security Standard (PCI DSS) is an industry based regulation developed by major credit card companies and serves as a set of technological and procedural requirements for better securing credit card processing and cardholder information.
System Administrators (SA)	Term used broadly in this document to include the technical people who are responsible for configuring and administering the enterprise's computers, networks, and application systems.

System Owners (SO)	Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an application system.
Vendor or OIT Vendor	An external business entity contracted by Montgomery College for a set period for providing a service or delivering a product.
Vulnerability Scanning	An automated process of proactively identifying vulnerabilities of computers, computer systems, networks, or applications in order to determine if and where the technology resource is vulnerable to exploitation or threat of potential security breach. The scanning software generates a report of findings that indicates what areas require mitigation actions to maintain security.

STANDARD

A. Vulnerability Identification

1. **Vulnerability Scanning**
   i. The vulnerability scanning program focuses on three types of scanning: network, web application, and PCI DSS compliance. The focus may change as technology changes.
   ii. Network scanning identifies operating system and/or configuration vulnerabilities in network resources including servers, work stations, routers, etc.
   iii. Web application scanning identifies vulnerabilities in end-user web-based applications.
   iv. PCI DSS compliance scanning ensures that credit card processing systems used by college offices comply with the payment card industry requirements.
2. **Vulnerability Alerts and Notifications**
   i. ITSG learns of vulnerabilities and available security patches through several sources, including but not limited to REN-ISAC, SANS, US-CERT, etc.
   ii. ITSG documents any vulnerabilities that apply to technology resources in our environment.

B. Roles and Responsibilities

1. The ITSG is responsible for:
   a. Running vulnerability scans on a routine, ongoing basis; prior to implementation of a new resource in the production environment; upon a suspected compromise or a significant change to a technology resource; and upon request.
   b. Establishing the vulnerability scanning schedule. The schedule may change based on vulnerability findings, threat assessments, and introduction of new technology resources.
   c. Acquiring, implementing and managing the scanning tools necessary to meet the requirements of this standard.
   d. Providing scan results to appropriate SOs/SAs for remediation.
   e. Providing notification of vulnerabilities identified outside of scanning to appropriate Sos/SAs for remediation.
   f. Establishing timeframes for completion of the remediation activities based on the severity levels of the vulnerability. The SO/SA can request an extension if necessary.
   g. Eliminating false positives upon identification and agreement with the SO/SA and eliminating the false positive from future scans.
   h. Overseeing and working with the PCI DSS Approved Scanning Vendor to maintain College compliance with the payment card industry requirements.
2. SOs/SAs are responsible for:

a. Notifying ITSG when new technology resources are to be added to the production environment.

i. Completing review and mitigation activities when vulnerabilities are identified according to the ITSG schedule. The SO/SA can request an extension if necessary.

b. Requesting exceptions through the IT Standard Exception Request process, when required.

3. CIO/VP of Instructional and Information Technology is responsible for:

a. Consulting with ITSG on any Exception Requests related to the vulnerably scans, and approving or denying the request.

C. Vulnerability Processes

The ITSG establishes the processes that SOs and SAs must follow regarding the identification and of technology resources, scanning process, and remediation actions with time lines.

Two processes are defined as follows:

- IT Process: Vulnerability Scanning, IT60001A.
- IT Process: Vulnerability Alerts and Notifications, IT60001 B.

EXCEPTIONS

This standard is applicable as of its Effective Date. Exceptions to this standard will be considered on a case-by-case basis in accordance with the IT Standard Exception Request Form.

COMPLIANCE AND RECOURSE FOR NON-COMPLIANCE

Montgomery College has established College Policies/Procedures and the OIT has established IT Standards and Processes and associated guiding documents to provide appropriate protection of technology resources, to assure protection of personally identifiable and sensitive information and to promote privacy. Any faculty, staff, contractor, or vendor found to have violated any part of College Policies, Procedures or IT Standards or Processes may be subject to disciplinary action and/or legal action.

RELATED DOCUMENTS

♦ Montgomery College Policy 66002: Acceptable Use of Technology
♦ IT Standard Exception Request Form
♦ IT60001A: Vulnerability Scanning Process
♦ IT60001B: Vulnerability Alerts and Notifications

WEB SITE ADDRESS FOR THIS STANDARD

https://info.montgomerycollege.edu/offices/information-technology/it-security/it_standards.html

Approvals / Revision History

DATE	VERSION / REVISION / NOTES	APPROVER
March 28, 2012	Original roll-out of this Vulnerability Standard document.	Patrick Feehan, Information Security and Privacy Director/ITPA
February 28, 2019	Revised.	Patrick Feehan, Information Security and Privacy Director/ITPA
September 30, 2020	Decided upon and added review cycle dates.	Nell Feldman / Keith Wilson
April 2022	Reviewed.	Nell Feldman, Interim Director of Information Security Services/CISO/IT Policy Administrator

Nell Feldman

Digitally signed by Nell Feldman
Date: 2022.04.07 15:32:32 -04'00'