Date of Last Revision: September 2024
Responsible Department: Information Technology

Policy Statement

GVSU PCI Equipment Malware Policy

Purpose

Malware, also known as malicious software, refers to a software or firmware that is covertly inserted into another computer system with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations.

Grand Valley State University is committed to providing a PCI network that is free of malware and has established requirements that must be met by all devices that are connected to our PCI network to provide adequate prevention, detection, and remediation of any malware infection.

See PCI DSS 4.0 Requirements 5: https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0_1.pdf

Scope

This policy applies to all employees, contractors, or other third-party business partners granted access to Grand Valley State University managed in-house systems, remote systems, unmanaged home systems, or mobile devices which are connected, or which may be used to connect via wire, wireless, modem, or VPN to the Grand Valley State University PCI network. Within the realm of this policy, a system may be defined as any computing device, regardless of operating system, with networking capability.

Policy

Staff Awareness

Security awareness training on acceptable use of systems, malware prevention techniques which may be employed by system users, and incident reporting procedures will be provided at hire and at least annually to all employees in the PCI environmentCHAD?. Following the initial and annual training,

employees will be tested on the material covered and be asked to read and accept the Grand Valley State University Acceptable System Use Policy. DOCUSIGN?

On an ongoing basis, awareness materials in the form of email broadcasts, printed media, signage, or ad-hoc training sessions will also be provided to all employees.

A similar policy for employee security awareness and training must also be maintained by all applicable contractors or third-party business partners which use or may use Grand Valley State University systems. Review of such a policy will be included in due diligence procedures by authorized Grand Valley State University personnel responsible for establishment of new contractor or business partner relationships. Absence, inadequacy, or negligence by contractors/business partners of such a policy shall be a basis for the dissolution of applicable existing contracts and exclusion from future business considerations.

Incident Prevention

Awareness and training are only one facet of Grand Valley State University's malware prevention efforts.

System or Application Owners will develop, maintain, and disseminate procedural documentation related to use of specific systems and applications to all users of the applicable system or application. ~~Procedural documentation will include examples of malware infection vectors which may be presented by the misuse of the system or application~~. Grand Valley State University Human Resources staff shall maintain a policy reserving the right to disciplinary action up to and including termination for negligence or intentional system or application misuse which results or may have resulted in malware infection.

Grand Valley State University Information Technology staff shall build, maintain, and monitor reporting and status of securely built systems as well as systems which support the prevention of malware infection including but not limited to continuous behavioral analysis, centrally managed anti-malware software, Network Security Control (NSC), content filtering systems, or intrusion prevention systems.

Prior to start of work, Grand Valley State University shall develop, maintain, disseminate, and ensure acceptance of an agreement covering acceptable use including, but not limited to introduction of foreign files, code, or devices to the Grand Valley State University network for all contractor or third-party business partner employees which will use or may use Grand Valley State University systems.

Vulnerability Mitigation

To mitigate the risk of malware exploiting known vulnerabilities within systems, Grand Valley State University Information Technology will develop and maintain baseline security configurations and checklists for the provisioning of new systems. Information Technology will also maintain a patch management program that includes ongoing research of known vulnerabilities to all systems, mitigation strategies/patches for the vulnerabilities, testing of the strategies/patches prior to production deployment, and a commitment to deploy tested patches within thirty days of their public release.

Threat Mitigation

Because malware often exploits unknown or unpatched vulnerabilities, it is important to have layered prevention mechanisms to prevent infection.

Grand Valley State University Information Technology will deploy and maintain a centralized anti-malware software suite on all systems where such a product may be installed. Agents will be configured to send prevention and infection event data to the central monitoring system, will be configured to

prevent protection mechanisms of the agent to be disabled by system users, and will be configured to automatically update malware signature definitions on at least a daily basis. Reporting provided by the central monitoring system will be reviewed daily.

Grand Valley State University Information Technology will deploy and maintain an application whitelisting solution that disallows the installation and use of unauthorized software on Grand Valley State University PCI managed systems. Approval of all whitelisted applications will be documented with application name, version(s), business use, and sponsoring manager. The whitelist will be reviewed and revised at least annually.ENT ARCH/ENT APP

Grand Valley State University Information Technology will deploy and maintain a network intrusion detection and prevention system to monitor real-time network traffic and block traffic known to be malicious or sourced from addresses with previous history of hosting malware.

Grand Valley State University Information Technology will deploy and maintain a NSC such as a firewall with explicit allowance policies followed by an implicit denial of all other traffic at each network perimeter. NSC access logs will be reviewed daily. Review of the allowance policies in each NSC will occur at least once every six months.

{Are host-based NSC/firewalls used? They should be. See PCI DSS 4.0 Requirement 1.4} ENT ARCH

Defensive Architecture

To further prevent the likelihood of malware infection, Information Technology will consider and implement other protection mechanisms when developing systems such as application sandboxing to isolate applications from privileged areas of a system's operating system or whole system virtualization.

Application Owners shall consider the impact of malware on the use of their applications and recommend or mandate the practice of browser separation, if possible, to minimize the risk associated with using a single browser for access of both sensitive and non-sensitive applications.

Incident Response

(See GVSU Comprehensive Emergency Management Plan) https://www.gvsu.edu/cms4/asset/45587EC7-FE4C-BB4F-80A05E76DBCD3970/2020_final_update.pdf