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.

Grand Valley State University 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.

Scope

This policy applies to all employees, contractors, or other third-party business partners granted access to Grand Valley State University's 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.

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

Incident Prevention

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.

Grand Valley State University Human Resources staff maintains policies reserving the right to disciplinary action up to and including termination for negligence or intentional system or application misuse.

Vulnerability Mitigation

To mitigate the risk of malware exploiting known vulnerabilities within systems, Grand Valley State University Information Technology will develop and maintain security configurations 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

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 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 firewall with explicit allowance policies followed by an implicit denial of all other traffic at each network perimeter.

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.