POLICY: SERVER MALWARE PROTECTION & SERVER SECURITY POLICY

Type of Policy: Security
Last Revised: June 2, 2019

Policy Owner: Information Services & Institutional Assessment
Policy Contact: Sharlene Harris
VP of Information Services & Institutional Assessment
sharris@uvi.edu

1.0 Overview

The purpose of this policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the University of the Virgin Islands (UVI). Effective implementation of this policy will minimize unauthorized access to UVI proprietary information and technology. UVI is entrusted with the responsibility to provide professional management of clients' servers as outlined in each of the contracts with its customers. Inherent in this responsibility is an obligation to provide appropriate protection against malware threats, such as viruses and spyware applications. Effective implementation of this policy will limit the exposure and effect of common malware threats to the systems they cover.

2.0 Scope

This policy applies to server equipment owned and/or operated by UVI, and to servers registered under any UVI-owned internal network domain. This policy is specifically for equipment on the internal UVI network. This policy applies to all servers that UVI is responsible to manage. This explicitly includes any system for which UVI has a contractual obligation to administer. This also includes all server systems setup for internal use by UVI, regardless of whether UVI retains administrative obligation or not.

3.0 Anti-Virus and Anti-Spyware Policy

UVI Information Services & Institutional Assessment (IS& IA) staff will adhere to this policy to determine which servers will have anti-virus and/or anti-spyware applications installed on them and to deploy such applications as appropriate.

3.1 Anti-Virus

All servers must have an anti-virus application installed, which offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Non-administrative users have remote access capability
- The system is a file server
- NBT/Microsoft Share access is open to this server from systems used by non-administrative users
- HTTP/FTP access is open from the Internet
- Other "risky" protocols/applications are available to this system from the Internet at the discretion of the UVI Systems or Network Administrator

All servers should have an anti-virus application installed that offers real-time scanning protection to files and applications running on the target system if they meet one or more of the following conditions:

- Outbound web access is available from the system

3.2 Mail Server Anti-Virus

If the target system is a mail server it MUST have either an external or internal anti-virus scanning application that scans all mail destined to and from the mail server.

3.3 Anti-Spyware

All servers MUST have an anti-spyware application installed that offers real-time protection to the target system if they meet one or more of the following conditions:

- Any system where non-technical or non-administrative users have remote access to the system and ANY outbound access is permitted to the Internet
- Any system where non-technical or non-administrative users have the ability to install software on their own

4.0 Server Security Policy

4.1 Ownership and Responsibility

ITS system or network administrators must have access to all internal servers deployed at UVI for system administration. System or network administrators must have administrative rights to all servers deployed in the enterprise not owned or managed by ITS.

- Servers must be registered within Information Services & Institutional Assessment. At a minimum, the following information is required to positively identify the point of contact:
  - Server contact(s) and location, and a backup contact
  - Hardware and Operating System/Version
  - Main functions and applications, if applicable
  - Username and password for any local administrative account
- Server information must be kept up-to-date and maintained by the system or network administrator.
- Configuration changes for production servers must follow the appropriate change management procedures.

4.2 General Configuration Guidelines

- Operating system configuration should be in accordance with approved Information Services & Institutional Assessment guidelines.
- Services and applications that will not be used must be disabled or decommissioned where practical.
- Access to services should be logged and/or protected through access-control methods such as TCP Wrappers, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication will do.
- Always use standard security principles of least required access to perform a function.
- Do not use root when a non-privileged account will do.

- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPSec).
- Servers should be physically located in an access-controlled environment.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

4.3 Monitoring

- All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
    - All security related logs will be kept online for a minimum of 1 week.
    - Daily incremental backups will be retained for at least 1 month.
    - Weekly full backups of logs will be retained for at least 1 month.
    - Monthly full backups will be retained for a minimum of 2 years.
- Security-related events will be reported to system or network administrators, who will review logs and report incidents to the appropriate ITS Manager or the Vice President of IS & IA. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

5.0 Enforcement

The responsibility for implementing this policy belongs to all Information Services & Institutional Assessment staff at UVI. Responsibility for ensuring that new and existing systems remain in compliance with this policy resides with the system and network administrators. Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.