MISSISSIPPI VALLEY STATE UNIVERSITY

Workstation Hardening Policy

General Information

Workstations, including both desktop and laptops, are used by staff to accomplish their day-to day duties. These assets must be protected from both security and performance related risks. One of the required steps to attain this goal is to ensure that hardware is installed and maintained in a manner that prevents unauthorized access, unauthorized use, consistent configuration, and minimal service disruptions.

Purpose

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of information. This policy provides procedures and requirements for installing a new workstation in a secure manner and maintaining the security integrity of the hardware and application software.

Scope

This policy applies to all MVSU staff that use, deploy, or support desktop computing hardware covers all IT systems and devices that comprise the University's network or that are otherwise controlled by the University.

Policy

A. GENERAL

A workstation hardening procedure will be created and maintained that provides detailed information required to configure and harden MVSU workstations whether remote or local. The procedure shall include:

- Installing the operating system from an MVSU IT Department approved source;
- Applying all appropriate vendor supplied security patches and firmware updates;
- Removing unnecessary software, system services, and drivers;
- Setting security and operational parameters including configuring system services, workstation firewall, Viper anti-virus, Malwarebytes anti-malware, and ACS account local passwords; and,
- Applying MVSU Domain-based Active Directory workstation group policy.

B. OPERATIONS AND MAINTENANCE

MVSU IT Department support staff shall perform the following procedures and processes to ensure hardening compliance after the initial system is delivered:

- Post-Install operating system, utility, and application security patches shall be pre-tested and deployed on a regular basis against similar systems before rolling out to the user community.
- In the case of custom applications or enterprise software, MVSU desktop support shall take appropriate precautions to ensure patch compatibility prior to installation.
- Ensure that all sensitive information is stored on secured MVSU network servers.
- All server based information shall be encrypted and comply with applicable policy and procedure.
- Laptops (and other remote computing devices) containing sensitive information shall have their hard drives encrypted and shall have additional physical security components installed to protect the assets and the data they store.

Audit Controls and Management

On-demand documented procedures and evidence of practice should be in place for this operational policy as part of the MVSU internal processes and procedures. Examples of appropriate controls and documentation are:

- Documented desktop build processes and images
- Internal configuration and asset management protocols and procedures
- Patch logs containing workstation name, patch installed, and date
- GPO documentation showing hardening and security measures employed across the enterprise

Enforcement

MVSU Staff members found in policy violation without consulting the MVSU IT Department may be subject to disciplinary action.

Distribution

This policy is to be distributed to all MVSU staff.

Review

This policy will be reviewed annually by the Director of IT