Definitions

Domain: In computing and telecommunication in general, a domain is a sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses.

Overview

The workstations at {COMPANY-NAME} provide a wide variety of services to process sensitive information for {COMPANY-NAME}. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the IT Department to secure the hardware against such attacks.

Purpose

The purpose of this policy is to enhance security and quality operating status for workstations utilized at {COMPANY-NAME}. IT resources are to utilize these guidelines when deploying all new workstation equipment. Workstation users are expected to maintain these guidelines and to work collaboratively with IT resources to maintain the guidelines that have been deployed.

The overriding goal of this policy is to reduce operating risk. Adherence to the {COMPANY-NAME} Workstation Configuration Security Policy will:

- Eliminate configuration errors and reduce workstation outages
- Reduce undocumented workstation configuration changes that tend to open up security vulnerabilities
- Facilitate compliance and demonstrate that the controls are working
- Protect {COMPANY-NAME} data, networks, and databases from unauthorized use and/or malicious attack

Therefore, all new workstation equipment that is owned and/or operated by {COMPANY-NAME} must be provisioned and operated in a manner that adheres to company defined processes for doing so.

This policy applies to all {COMPANY-NAME} company-owned, company operated, or company controlled workstation equipment. Addition of new workstations, within {COMPANY-NAME} facilities, will be managed at the sole discretion of IT. Non-sanctioned workstation installations, or use of unauthorized equipment that manage networked resources on {COMPANY-NAME} property, is strictly forbidden.

Policy Detail

Responsibilities

{COMPANY-NAME}'s VP of IT has the overall responsibility for the confidentiality, integrity, and availability of {COMPANY-NAME} data.

Other IT staff members, under the direction of the VP of IT, are responsible for following the procedures and policies within IT.

Supported Technology /R

All workstations will be centrally managed by {COMPANY-NAME}'s IT Department and will utilize approved workstation configuration standards, which will be established and maintained by {COMPANY-NAME}'s IT Department.

All established standards and guidelines for the {COMPANY-NAME} IT environment are documented in an IT storage location.

The following outlines {COMPANY-NAME}'s minimum system requirements for workstation equipment.

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the VP of IT.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. {COMPANY-NAME} has deployed a patch management process; reference the Patch Management Policy.
- All workstations joined to the {COMPANY-NAME} domain will automatically receive a policy update configuring the workstation to obtain future updates from our desktop management system.

- All systems within {COMPANY-NAME} are required to utilize anti-virus, malware, and data leakage protection. IT will obtain alerts of infected workstations and perform certain remediation tasks.
- All workstations will utilize the {COMPANY-NAME} domain so that all general policies, controls, and monitoring features are enabled for each workstation. No system should be managed manually but should be managed through some central tool or model in order to efficiently manage and maintain system security policies and controls.
- Third-party applications need to be updated and maintained. So that software with security updates is not exposed to vulnerabilities for longer than necessary, a quarterly review will be performed.
- Third-party applications, including browsers, shall be updated and maintained in accordance with the {COMPANY-NAME} patch management program.
- Any critical security updates for all applications and operating systems need to be reviewed and appropriate actions taken by the IT Department to guarantee the security of the workstations in accordance with the {COMPANY-NAME} patch management program.
- Internet browsers on workstations will remain up to date. To ensure all browsers are up to date, the IT Department will perform quarterly reviews. If there is a reason the browser cannot be updated, due to conflicts with applications, these exceptions will be recorded.
- By default, all workstations joined to the {COMPANY-NAME} domain will obtain local security settings through policies.

This policy is complementary to any previously implemented policies dealing specifically with security and network access to {COMPANY-NAME}'s network.

It is the responsibility of each employee of {COMPANY-NAME} to protect {COMPANY-NAME}'s technology based resources from unauthorized use and/or malicious attack that could result in the loss of member information, damage to critical applications, loss of revenue, and damage to {COMPANY-NAME}'s public image. Procedures will be followed to ensure resources are protected.