coast
mountain
college

RESOURCE INF-013G

Workstation Configuration Guideline

Purpose

The purpose of this guideline is to enhance the security and quality operating status for workstations used at Coast Mountain College (CMTN).

Overview

The workstations at CMTN provide a wide variety of services to process sensitive information for the College. These hardware devices are vulnerable to attacks from outside sources which require due diligence by the Information Technology (IT) Department to secure the hardware against such attacks.

The overriding goal of this guideline is to reduce operating risk. Adherence to this guideline 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 CMTN data, networks, and databases from unauthorized use and/or malicious attack.

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

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.

Scope

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

IT resources are to use 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.

Details

Responsibilities

CMTN's Director of Information and Technology has the overall responsibility for the confidentiality, integrity, and availability of CMTN data.

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

Supported Technology

All workstations will be centrally managed by CMTN's IT Department and will utilize approved workstation configuration standards, which will be established and maintained by CMTN's IT Department.

All established standards and guidelines for the CMTN IT environment are documented in an IT storage location.

CMTN's minimum system requirements for workstation equipment are:

- Operating System (OS) configuration must be in accordance with approved procedures.
- Unused services and applications must be disabled, except where approved by the Director of Information and Technology.
- All patch management to workstations will be monitored through reporting with effective remediation procedures. CMTN has deployed a patch management process (INF-009G, *Patch Management Guideline*).
- All workstations joined to the CMTN domain will automatically receive an update configuring the workstation to obtain future updates from our desktop management system.
- All systems within CMTN 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 CMTN 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 CMTN 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 CMTN 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 CMTN domain will obtain local security settings through policies and guidelines.

This guideline is complementary to any previously implemented policies and guidelines dealing specifically with security and network access to CMTN's network.

Each employee is responsible for protecting CMTN’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 CMTN’s public image. Procedures will be followed to ensure resources are protected.

Related Policies, Guidelines, and Other Resources

- INF-009G, *Patch Management Guideline*