coast mountain college

RESOURCE INF-007G

Server Security Guideline

Purpose

The purpose of this guideline is to define standards and restrictions for the base configuration of internal server equipment owned and/or operated by or on Coast Mountain College's (CMTN's) internal network(s) or related technology resources via any means.

Overview

The servers at CMTN provide a wide variety of services to internal and external users, and many servers also store or process-sensitive information for CMTN. These hardware devices are vulnerable to attacks from outside sources, which requires due diligence by the IT Department to secure the hardware against such attacks.

Definitions

File Transfer Protocol (FTP): A standard Internet protocol for transmitting files between computers on the Internet.

Scope

This guideline applies to all internal server equipment that is owned and/or operated by or on CMTN's internal network(s) or related technology resources via any means. This includes but is not limited to:

- Internet servers (e.g., FTP servers, web servers, mail servers, proxy servers)
- application servers
- database servers
- file servers
- print servers
- third-party appliances that manage network resources.

This guideline also covers any server device outsourced, co-located, or hosted at external/third-party service providers, if that equipment resides in the coastmountaincollege.org domain or appears to be owned by CMTN.

The overriding goal of this guideline is to reduce operating risk. Adherence to this guideline will:

- eliminate configuration errors and reduce server outages

- reduce undocumented server 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 server 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.

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

Details

Responsibilities

CMTN's VP of IT has the overall responsibility for the confidentiality, integrity, and availability of CMTN data.

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

Supported Technology

All servers will be centrally managed by CMTN's IT Department and will use approved server configuration standards. Approved server configuration standards 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 server equipment supporting CMTN's systems 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 IT or the VP of IT.
- Access to services must be logged or protected through appropriate access control methods.
- Security patches must be installed on the system as soon as possible through CMTN's configuration management processes.
- Trust relationships allow users and computers to be authenticated (to have their identity verified) by an authentication authority. Trust relationships should be evaluated for their inherent security risk before implementation.
- Authorized users must always use the standard security principle of "least required access" to perform a function.
- System administration and other privileged access must be performed through a secure connection. Root is a user account with administrative privileges that allow access to any file or folder on the system. Do not use the root account when a non-privileged account will do.
- All CMTN servers are to be in access-controlled environments.
- All employees are specifically prohibited from operating servers in environments with uncontrolled access (e.g., offices).

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

Any CMTN employee who is installing or operating server equipment is responsible for protecting CMTN's technology-based resources (e.g., CMTN data, computer systems, networks, databases) 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

- None