coast mountain college

RESOURCE INF-011G

Vulnerability Assessment Guideline

Purpose

The purpose of this guideline is to establish standards for periodic vulnerability assessments.

Overview

At Coast Mountain College (CMRN), vulnerability assessments are necessary to manage the increasing number of threats and risks to information systems and the equipment associated with them, and also the responsibilities of the Information Technology (IT) Department.

Vulnerabilities are not only internal and external, but there are also additional responsibilities and costs associated with ensuring compliance with laws and rules, while retaining business continuity and safety of CMTN and member data.

Definitions

None

Scope

This guideline covers all computer and communication devices owned or operated by CMTN. This guideline also covers any computer and communications device that is present on CMTN premises, but which may not be owned or operated by CMTN.

Denial of service testing or activities will not be performed.

Details

This guideline reflects CMTN's commitment to identify and implement security controls, which will keep risks to information system resources at reasonable and appropriate levels.

The operating system or environment for all information system resources must undergo a regular vulnerability assessment. This standard will empower the IT Department to perform periodic security risk assessments for determining the area of vulnerabilities and to initiate appropriate remediation. All employees are expected to cooperate fully with any risk assessment.

Vulnerabilities to the operating system or environment for information system resources must be identified and corrected to minimize the risks associated with them.

Audits may be conducted to:

- ensure integrity, confidentiality, and availability of information and resources
- investigate possible security incidents
- ensure conformance to CMTN's security policies
- monitor user or system activity where appropriate.

To ensure these vulnerabilities are adequately addressed, the operating system or environment for all information system resources must undergo an authenticated vulnerability assessment.

The frequency of these vulnerability assessments will depend on the operating system or environment, the information system resource classification, and the classification of the data associated with the information system resource.

Retesting will be performed to ensure the vulnerabilities have been corrected. An authenticated scan will be performed by either a third-party vendor or using an in-house product.

All data collected and/or used as part of the vulnerability assessment process and related procedures will be formally documented and securely maintained.

IT leadership will make vulnerability scan reports and ongoing correction or mitigation progress to senior management for consideration and reporting to the Board of Directors.

Related Policies, Guidelines, and Other Resources

- None