INF-020G

Email Guideline

Purpose

The purpose of this guideline is to establish rules for the use of Coast Mountain College (CMTN) email for sending, receiving, or storing of electronic mail.

Overview

Email at CMTN must be managed as a valuable and mission-critical resource. Therefore, this guideline is established to:

- create prudent and acceptable practices regarding the use of information resources
- educate individuals who may use information resources with respect to their responsibilities associated with such use
- establish a schedule for retaining and archiving email.

Definitions

Anti-Spoofing: A technique for identifying and dropping data units, called packets, that have a false source address.

Antivirus: Software used to prevent, detect, and remove malicious software.

Electronic Mail (Email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic Mail System: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Email Spoofing: The forgery of an email header so the message appears to have originated from someone other than the actual source. Email spoofing aims to get recipients to open and possibly even respond to, a solicitation to provide sensitive data or perform an action such as processing a wire transfer.

Inbound Filters: A software-based traffic filter allowing only designated traffic to flow toward a network.

Quarantine: Suspicious email messages may be identified by an antivirus filter and isolated from the normal mail inbox.

SPAM: Unsolicited email, usually from Internet sources. It is often referred to as junk email.

Scope

This guideline applies equally to all individuals granted access privileges to any CMTN information resource with the capacity to send, receive, or store electronic mail.

Details

Legal

Individuals involved may be held liable for:

- sending or forwarding:
  - emails with any libelous, defamatory, offensive, racist, or obscene remarks
  - confidential information without permission
  - copyrighted material without permission
- knowingly sending or forwarding an attachment that contains a virus.

CMTN Emails Are Not Private

Users expressly waive any right of privacy in anything they create, store, send, or receive on CMTN's computer systems.

CMTN can but is not obliged to monitor emails without prior notification.

All emails, files, and documents, Including personal emails, files, and documents, are owned by CMTN, may be subject to open records requests, and may be accessed in accordance with this guideline.

Information Security

Incoming emails must be treated with the utmost care due to the inherent information security risks.

An antivirus application is used to identify malicious code(s) or files.

All email is subjected to inbound filtering of email attachments to scan for viruses, malicious code, or spam.

- Spam will be quarantined for the user to review for relevancy.
- Introducing a virus or malicious code to CMTN systems could wreak havoc on the ability to conduct business. If the automatic scanning detects a security risk, IT must be immediately notified.

Anti-spoofing practices have been initiated for detecting spoofed emails.

- Employees should be diligent in identifying a spoofed email.
- If email spoofing has occurred, IT must be immediately notified.

Incoming emails are scanned for malicious file attachments.

- If an attachment is identified as having an extension known to be associated with malware, or prone to abuse by malware or bad actors or otherwise poses heightened risk, the attachment will be removed from the email prior to delivery.
- Email rejection is achieved through listing domains and IP addresses associated with malicious actors. Any incoming email originating from a known malicious actor will not be delivered.
- Any email account misbehaving by sending out spam will be shut down. A review of the account will be performed to determine the cause of the actions.

Appropriate Use of Email

Email is to be used for business purposes and in a manner that is consistent with other forms of professional business communication.

All outgoing attachments are automatically scanned for virus and malicious code. The transmission of a harmful attachment can not only cause damage to the recipient's system, but also harm CMTN's reputation.

The following activities are prohibited:

- sending email that may be deemed intimidating, harassing, or offensive; this includes, but is not limited to:
    - abusive language
    - sexually explicit remarks or pictures
    - profanities
    - defamatory or discriminatory remarks regarding race, creed, colour, sex, age, religion, sexual orientation, national origin, or disability
- using email for conducting personal business
- using email for the purposes of sending SPAM or other unauthorized solicitations
- violating copyright laws by illegally distributing protected works
- ending email using another person's email account, except when authorized to send messages for another while serving in an administrative support role
- creating a false identity to bypass policies and guidelines
- forging or attempting to forge email messages
- using unauthorized email software
- knowingly disabling the automatic scanning of attachments on any CMTN personal computer
- knowingly circumventing email security measures
- sending or forwarding joke emails, chain letters, or hoax letters
- sending unsolicited messages to large groups, except as required to conduct CMTN business
- sending excessively large messages or attachments
- knowingly sending or forwarding email with computer viruses
- setting up or responding on behalf of CMTN without management approval.

All confidential or sensitive CMTN material transmitted via email, outside CMTN's network, must be encrypted.

- Passwords to decrypt the data should not be sent via email.

Email is not secure. Users must not email passwords, social security numbers, account numbers, PIN numbers, dates of birth, mother's maiden name, etc. to parties outside the CMTN network without encrypting the data.

- All user activity on CMTN information system assets is subject to logging and review.
- CMTN has software and systems in place to monitor email usage.

Email users must not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of CMTN, unless appropriately authorized (explicitly or implicitly) to do so.

Users must not send, forward, or receive confidential or sensitive CMTN information through non-CMTN email accounts.

- Examples of non-CMTN email accounts include, but are not limited to, Hotmail, Yahoo mail, AOL mail, and email provided by other Internet Service Providers (ISP).
- Users with non-CMTN-issued mobile devices must adhere to INF-023G, *Personal Device Acceptable Use and Security Guideline* for sending, forwarding, receiving, or storing confidential or sensitive CMTN information.

Incidental Use

Incidental personal use of sending email is restricted to CMTN-approved users; it does not extend to family members or other acquaintances.

Without prior management approval, incidental use must not result in direct costs to CMTN.

Incidental use must not interfere with the normal performance of an employee's work duties.

No files or documents may be sent or received that may cause legal liability for or embarrassment to CMTN.

Storage of personal files and documents within CMTN's IT systems should be nominal.

Email Retention

Messages are retained for three months. Emails older than three months are subject to automatic purging.

Deleted and archived emails are subject to automatic purging.

Appointments, tasks, and notes older than the retention period are subject to automatic purging.

Email Archive

Only the owner of a mailbox and the system administrator have access to the archive.

Messages will be deleted from the online archive three months from the original send/receive date.

Related Policies, Guidelines and Other Resources

- INF-023G, *Personal Device Acceptable Use and Security Guideline*