RESOURCE INF-023G

Personal Device Acceptable Use and Security Guideline

Purpose

This guideline defines the standards, procedures, and restrictions for end users who have legitimate business requirements to access Coast Mountain College (CMTN) corporate data using their personal device.

Overview

Acceptable use of BYOD at CMTN must be managed to ensure that access to CMTN's resources for business are performed in a safe and secure manner for participants of the CMTN BYOD program. A participant of the BYOD program includes, but is not limited to:

- employees
- contractors
- board of directors
- volunteers
- related constituents who participate in the BYOD program.

This guideline is designed to maximize the degree to which private and confidential data is protected from both deliberate and inadvertent exposure and/or breach.

Refer to INF-003, *CMTN-Owned Mobile Devices Policy* and INF-023G, *Personal Device Acceptable Use and Security Guideline*.

Definitions

Bring Your Own Device (BYOD): Privately owned wireless and/or portable electronic handheld equipment.

Scope

This guideline applies to all CMTN employees, including full- and part-time staff, Board of Directors, volunteers, contractors, freelancers, and other agents who use personally-owned mobile devices to access, store, back up, relocate, or access any organization or member-specific data.

- Such access to this confidential data is a privilege, not a right, and forms the basis of the trust CMTN has built with its members, suppliers, and other constituents.

- Employment at CMTN does not automatically guarantee the initial and ongoing ability to use these devices to gain access to corporate networks and information.

This guideline applies to, but is not limited to, any mobile devices owned by any Users listed above participating in the CMTN BYOD program which contains stored data owned by CMTN, and all devices and accompanying media that fit the following classifications:

- laptops, notebooks, and hybrid devices
- tablets
- mobile/cellular phones, including Smartphones
- any non-CMTN-owned mobile device capable of storing corporate data and connecting to an unmanaged network.

Details

Threats

Threat	Description
Loss	Devices used to transfer, or transport, work files are lost or stolen.
Theft	Sensitive corporate data is deliberately stolen and sold by an employee.
Copyright Infringement	Software copied onto a mobile device violates licensing.
Malware	Virus, Trojans, worms, spyware, and other threats are introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data exposes CMTN to the risk of non-compliance with various identity theft and privacy laws.

The addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of IT.

Non-sanctioned use of mobile devices to back up, store, and otherwise access any enterprise-related data is strictly forbidden.

This guideline is complementary to any other implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the CMTN network.

Guideline Detail

This guideline applies to:

- any privately owned wireless and/or portable electronic handheld equipment, hereby referred to as BYOD
    - CMTN grants potential participants of the BYOD program the privilege of purchasing and using a device of their choosing at work for their convenience.
- related software that could be used to access corporate resources.

This guideline is intended to protect the security and integrity of CMTN's data and technology infrastructure. Limited exceptions to the guideline may occur due to variations in devices and platforms.

Users must agree to the terms and conditions set forth in this guideline to be able to connect their devices to the company network.

If Users do not abide by this guideline, CMTN reserves the right to revoke this privilege.

The following criteria will be considered initially, and on a continuing basis, to determine if the User is eligible to connect a personal smart device to the CMTN network:

- management's written permission and certification of the need and efficacy of BYOD for that User
- sensitivity of data the User can access
- legislation or regulations prohibiting or limiting the use of a personal smart device for CMTN business
- must be listed on the Information Technology Department's list of approved mobile devices
- User's adherence to the terms of the Bring Your Own Device Agreement (Appendix A) and this guideline and other applicable policies
- technical limitations
- other eligibility criteria deemed relevant by CMTN or IT.

Responsibilities of CMTN

The IT Department:

- will centrally manage the BYOD program and devices including, but not limited to, onboarding approved users, monitoring BYOD connections, and terminating BYOD connections to company resources upon the User's leave of employment or service to CMTN
- will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable
- reserves the right to refuse, by non-physical means, the ability to connect mobile devices to CMTN and CMTN-connected infrastructure.
    - IT will engage in such action if it feels the equipment is being used in a way that puts CMTN's systems, data, users, and members at risk
- will maintain a list of approved mobile devices and related software applications and utilities:
    - Devices that are not on this list may not be connected to the CMTN infrastructure.
    - To find out if a preferred device is on this list, an individual should contact the IT Department Service Desk.
    - Although IT currently allows only listed devices to be connected to the CMTN infrastructure, IT reserves the right to update this list in the future.
- will maintain enterprise IT security standards
- will inspect all mobile devices attempting to connect to the CMTN network through an unmanaged network (e.g., the Internet) using technology centrally managed by the IT Department
- will install the mobile VPN software required on Smart mobile devices (e.g., Smartphones) to access the CTN network and data.

The IT Department reserves the right to:

- install anti-virus software on any BYOD-participating device
- restrict applications
- limit use of network resources

- wipe data on lost or damaged devices or upon termination from the BYOD program or CMTN employment
- properly perform job provisioning and configuration of BYOD-participating equipment before connecting to the network
- through enforcement and any other means it deems necessary, to limit the ability of Users to transfer data to and from specific resources on the CMTN network.

Responsibilities of BYOD Participants

All potential participants will be granted access to the CMTN network on the condition that they read, sign, respect, and adhere to the CMTN policies concerning the use of these devices and services (see Appendix A).

Prior to initial use on the CMTN network or related infrastructure, all personally owned mobile devices must be registered with IT.

Participants of the BYOD program and related software for network and data access will, without exception:

- use secure data management procedures
    - All BYOD equipment containing stored data owned by CMTN must use an approved method of encryption during transmission to protect data.
- be expected to adhere to the same security protocols when connected with approved BYOD equipment to protect CMTN's infrastructure.

CMTN data is not to be accessed on any hardware that fails to meet CMTN's established enterprise IT security standards. Users must:

- ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied to BYOD use
- use a device lock with authentication, such as a fingerprint or strong password, on each participating device. Refer to INF-008G, Password Choice and Protection Guideline for additional information
- agree never to disclose their passwords to anyone, particularly to family members, if business work is conducted from home
    - Passwords and confidential data should not be stored on unapproved or unauthorized non-CMTN devices.
- exercise reasonable physical security measures.
    - The User is responsible for keeping their approved BYOD equipment safe and secure.

A device's firmware/operating system must be up to date to prevent vulnerabilities and make the device more stable.

- The patching and updating processes are the responsibility of the owner.

Any non-corporate computers used to synchronize with BYOD equipment will have installed anti-virus and anti-malware software deemed necessary by CMTN's IT Department.

- Anti-virus signature files must be up to date on any additional client machines (e.g., a home PC) on which this media will be accessed.

IT can and will establish audit trails and these will be accessed, published, and used without notice.

- Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse.

If any BYOD device is:

- lost or stolen, the User must immediately contact CMTN IT
- scheduled to be upgraded or exchanged, the User must contact IT in advance; IT will disable the BYOD and delete associated company data.

BYOD equipment that is used to conduct CMTN business will be used appropriately, responsibly, and ethically.

- Failure to do so will result in immediate suspension of that User's access.

Any attempt to contravene or bypass security implementation will be deemed an intrusion attempt and will be dealt with in accordance with CMTN's overarching security policy.

Use of location-based services and mobile check-in services which leverage device GPS capabilities to share real-time User location with external parties is prohibited within the workplace.

The User agrees to and accepts that his/her/their access and/or connection to CMTN's networks may be monitored to record dates, times, duration of access, etc.

- This is done to identify unusual usage patterns or other suspicious activity, and to identify accounts/computers that may have been compromised by external parties.
- In all cases, data protection remains CMTN's highest priority.

Employees, Board of Directors, volunteers, contractors, and temporary staff will not reconfigure mobile devices with any type of CMTN-owned and -installed hardware or software without the express approval of the IT Department.

The User agrees to immediately report, to his/her/their manager and the IT Department, any incident or suspected incidents of unauthorized data access, data loss, and/or disclosure of CMTN resources, databases, networks, etc.

Third-Party Vendors

Third-party vendors are expected to secure all devices with up-to-date anti-virus signature files and anti-malware software relevant or applicable to a device or platform.

All new connection requests between third parties and CMTN require that the third party and CMTN representatives agree to and sign the Third Party Agreement.

- This agreement must be signed by the Vice President of the sponsoring department, as well as a representative from the third party who is legally empowered to sign on behalf of the third party.
- By signing this agreement, the third party agrees to abide by all referenced policies.
- The document is to be kept on file.
- All non-publicly accessible information is the sole property of CMTN.

The IT Department can supply a non-CMTN Internet connection using a cellular hot spot, if needed.

Help and Support

CMTN's IT Department is not accountable for conflicts or problems caused by using unsanctioned media, hardware, or software.

This applies even to devices already known to the IT Department.

Organizational Protocol

CMTN may offer a reimbursement of expenses to employees if they choose to use their own mobile devices in lieu of accepting a CMTN-issued device.

This may depend on the User's function within the company and will be in accordance with a schedule in the associated procedure. Refer to INF-003, *CMTN-Owned Mobile Devices Policy* and INF-023G, *Personal Device Acceptable Use and Security Guideline*.

Related Policies, Procedures, and Supporting Documents

INF-001, *Acceptable Use of Information Systems Policy*

INF-003, *CMTN-Owned Mobile Devices Policy*

INF-008G, *Password Choice and Protection Guideline*

Appendix A: Bring Your Own Device (BYOD) Agreement

This Bring Your Own Device Agreement is entered into between the User and Coast Mountain College (CMTN), effective the date this agreement is executed by CMTN's Information Technology (IT) Department. The parties agree as follows:

Eligibility

The use of a supported smart device owned by the User in connection with CMTN business is a privilege granted to the User, by Management approval, per INF-023G, *Personal Device Acceptable Use and Security Guideline*. A supported smart device is defined as an Android or IOS-based cell phone or tablet running a manufacturer's supported version of its operating system. If the User does not abide by the terms, IT Management reserves the right to revoke the privilege granted herein. The policies referenced herein are aimed to protect the integrity of data belonging to CMTN and to ensure the data remains secure.

In the event of a security breach or threat, CMTN reserves the right, without prior notice to the User, to disable or disconnect some or all BYOD services related to connection of a personal smart device to the CMTN network.

Reimbursement Considerations

CMTN offers a fixed reimbursement to eligible Users starting the month following BYOD enrolment. The User is personally liable for the device and carrier service.

Accordingly, CMTN will NOT reimburse the User, over and above the monthly reimbursement, for any loss, cost, or expense associated with the use or connection of a personal smart device to the CMTN network. This includes, but is not limited to, expenses for voice minutes used to perform CMTN business, data charges related to the use of CMTN services, expenses related to text or other messaging, cost of handheld devices, components, parts, or data plans, cost of replacement handheld devices in case of malfunction whether or not the malfunction was caused by using applications or services sponsored or provided by CMTN, loss related to unavailability of, disconnection from, or disabling the connection of a smart device to the CMTN network, and loss resulting from compliance with this Agreement or applicable CMTN policies.

Security Considerations and Acceptable Use

Compliance by the User with the following CMTN policies and guidelines is mandatory:

- INF-001, *Acceptable Use of Information Systems Policy*
- INF-004, *Safeguarding Member Information Policy*
- INF-005, *Network Security and VPN Acceptable Use Policy*
- INF-001G, *Anti-Virus Guideline*
- INF-008G, *Password Choice and Protection Guideline*
- INF-016G, *Telecommuting Guideline*
- INF-020G, *Email Guideline*
- INF-023G, *Personal Device Acceptable Use and Security Guideline*.

The User of the personal smart device shall not remove sensitive information from the CMTN network, attack CMTN assets, or violate any of the security policies related to the subject matter of this Agreement.

Support

CMTN will offer the following support for the personal smart device: connectivity to CMTN servers, including email and calendar, and security services, including password management and decommissioning and/or remote wiping in case of loss, theft, device failure, device degradation, upgrade (trade-in), or change of ownership.

CMTN is not able to provide any additional assistance on any personally owned device and is not responsible for carrier network or system outages that result in a failure of connectivity to the CMTN network.

The User assumes full liability including, but not limited to, an outage or crash of any or all of the CMTN network, programming and other errors, bugs, viruses, and other software or hardware failures resulting in the partial or complete loss of data or which render the smart device inoperable.

Disclaimer

CMTN expressly disclaims, and the User releases CMTN from, all liability for any loss, cost, or expense of any nature whatsoever sustained by the User in connection with the privilege afforded the User under the terms of this Agreement.

User Signature _____

User Name (printed) _____

Date _____