Policy Title:	Computing Device Security		
Category:	☐ Institutional - Board ☒ Institutional - Administrative	☐ Academic - Administrative ☐ Employment - Administrative	
Approved by:	☐ Board	☒ President	
Date approved:	August 27, 2020	**Effective date:**	August 27, 2020
Policy Sponsor:	Chief Information Officer	**Date last reviewed:**	NEW
Date of Mandatory Review (expiry date)	August 2023	**Date of last revision of Procedures**	NEW

1 POLICY

1) Encryption

All Computing Devices being used to access *High Risk* or *Moderate Risk* CMCC Data are to use encrypted data storage using an encryption technology approved by the Division of IT.

2) Authentication

All Computing Devices being used to access *High Risk* or *Moderate Risk* CMCC Data are to enforce user authentication, using authentication standards approved by the Division of IT. Users are not to subvert authentication mechanisms by any means including (but not limited to) the sharing of passwords.

3) Software Update

All Computing Devices being used to access *High Risk* or *Moderate Risk* CMCC Data are to be kept up to date with manufacturer or reseller provided software and firmware updates, which are to be checked for and applied at least once a month.

4) Malware Protection

All Computing Devices being used to access *High Risk* or *Moderate Risk* CMCC Data are to have appropriate malware protection in place as mandated by the Division of IT.

5) Physical Security

All Computing Devices being used to access *High Risk* or *Moderate Risk* CMCC Data are to be locked or shutdown and hidden from view when unattended, with any available anti-theft mechanism activated.

6) Notice of Loss

All lost or stolen Computing Devices that contain *High Risk* or *Moderate Risk* CMCC Data are to be reported immediately to CMCC.

7) Duty of Care

Users are to protect *High Risk* or *Moderate Risk* CMCC Data accessed from or residing on Computing Devices.

a. Users are only to load CMCC Data that is essential to their role onto their Computing Device(s).
b. Computing Devices are not to be "jailbroken" or "rooted" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the user.
c. Users are not to load pirated software or illegal content onto their Computing Devices.
d. Applications are to be installed only from official platform-owner approved sources and never from untrusted sources. If unsure of an application's source contact the Division of IT.

8) Restricted Access to Services and Data

CMCC reserves the right to limit the ability of users to access IT Services and/or transfer CMCC Data when using Computing Devices by requiring the use of Computing/Mobile Device Management (CDM/MDM), Multi-Factor Authentication (MFA), Virtual Private Networks (VPN), or other security measures as authorized by the Division of IT.

9) Removable Media

a. CMCC reserves the right to restrict the use of any Removable Media at any time if the usage of that device poses any risk to the security of CMCC Data, including (but not limited to) transport of viruses or malware.
b. Only encrypted removable media devices are to be used to store *High Risk* or *Moderate Risk* CMCC Data.
c. Removable Media is not to be left unsecured or loaned to others.

10) Unsecured Public Networks

All Computing Device being used to access *High Risk* or *Moderate Risk* CMCC Data are to be connected to an unsecured public WiFi network (hot spot) only with the use of a Virtual Private Network (VPN) or other security measure approved by the Division of IT.

11) Erasure of Data

Users are to permanently erase *High Risk* or *Moderate Risk* CMCC Data from Computing Devices once it is no longer required.

12) Backup of Data

The user is responsible for the backup of their own personal data and CMCC does not accept responsibility for the loss of data due to a non-compliant device being wiped by Computing/Mobile Device Management (CDM/MDM) for security reasons.

13) Regulatory Compliance

All users of Computing Devices that access IT Services and/or CMCC Data are to be in compliance with all appropriate regulatory restrictions including (but not limited to) PIPEDA and PHIPA.

2 PURPOSE

To protect the integrity of all CMCC Data through the definition of security standards, procedures and processes for end users who have legitimate requirements to access CMCC Data and/or IT Services from a Computing Device.

3 SCOPE

All Computing Devices that are being used to access *High Risk* or *Moderate Risk* CMCC Data.

Exemptions: Where there is a business need to be exempted from this policy (too costly, too complex, adversely impacting other business requirements) a risk analysis must be conducted, and a written exemption must be provided by the Chief Information Officer.

4 INFORMATION AND COMPLIANCE PLANS (not a comprehensive list)

- PIPEDA: *Personal Information Protection and Electronic Documents Act,* Federal legislation
- PHIPA: *Personal Health Information Protection Act,* Ontario legislation

Computing Devices, such as desktops, laptops, phones and tablets, are important tools for the organization and CMCC supports their use to achieve educational and business goals. However, Computing Devices also represent a significant risk to data security as, if the appropriate security standards, procedures, and processes are not applied, they can be a conduit for unauthorized access to the organization's data and IT infrastructure. This can subsequently lead to data loss and damage to information systems. CMCC has a requirement to protect its information assets in order to safeguard its students, employees, intellectual property and reputation.

This document outlines a set of practices and requirements for the safe use of Computing Devices and applications.

5 RELATED POLICIES (not a comprehensive list)

- Computing and Information Technology Use
- Confidentiality and Release of Information
- Discipline – Employees
- Discipline - Students
- Privacy

6 DEFINITIONS

Authentication mechanisms include (but are not limited to) passwords, PIN numbers, and biometric sensors such as fingerprint readers and facial recognition scanners.

CMCC Data is any data residing in the CMCC Information Technology infrastructure. This includes data stored on-premises at our campus locations and also data stored in a public or private cloud.

Computing Device is any general-purpose electronic equipment controlled by a CPU, including (but not limited to) desktop and laptop computers, smartphones and tablets.

- CMCC Issued Device – Computing Devices owned by CMCC.

Generally referred to as a “Corporate Owned Device” (COD)
- Personal Computing Device – Computing Devices not owned/provided by CMCC. Generally referred to as “Bring Your Own Device” (BYOD)

CMCC Data Risk Classification - There are three categories of data risk:

High Risk*: Data is classified as High Risk if:*
1. *Protection of the data is required by law/regulation,*
2. *CMCC is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or*
3. *The loss of confidentiality, integrity, or availability of the data could have a significant adverse impact on our mission, safety, finances, or reputation.*

Moderate Risk*: Data is classified as Moderate Risk if it is not considered to be High Risk, and:*
1. *The data is not generally available to the public, or*
2. *The loss of confidentiality, integrity, or availability of the data could have a mildly adverse impact on our mission, safety, finances, or reputation.*

Low Risk: Data is classified as Low Risk if:
1. The data are not considered to be Moderate or High Risk, and:
2. The data is intended for public disclosure, or
3. The loss of confidentiality, integrity, or availability of the data would have no adverse impact on our mission, safety, finances, or reputation.

IT Service is a set of Information Technology (software and/or hardware) that is provided, by the Division of IT to users for a particular purpose. An IT Services typically provides access to CMCC Data. Some examples of IT Service categories include (but are not limited to):
- Administrative and Business Services
- Communication and Collaboration Services
- Desktop and Mobile Computing Services
- Teaching and Learning Services
- Clinical Care Services

Malware Protection is security mechanisms that may include (but are not limited to) anti-virus protection and firewall protection.

Mobile Device is any device that is not physically fixed to a specific physical location at CMCC. This includes (but is not limited to) the following:
- Phones and Tablets (e.g., iPhones, iPads, Android Devices)
- Laptops (e.g., Windows Laptops, Mac Laptops)

Removable Media is any form of computer storage that is designed to be inserted and removed from a Computing Device. This includes (but is not limited to) the following:
- USB flash drives
- External hard drives
- Memory cards
- Writable optical disks

New Policy Approved (date): August 27, 2020 **Policy Revision History (dates):**

----------**END OF POLICY**----------

7 PROCEDURES

1. Implementing Computing Device Security

   For assistance in the technical implementation of any policy provision in this document, users are to contact the CMCC Helpdesk via email to helpdesk@cmcc.ca or by visiting https://helpdesk.cmcc.ca. Assistance is available (but is not limited to) the following:
   - Setting up data Encryption
   - Enabling user Authentication
   - Updating Operating Systems and Applications
   - Installing Anti-Virus and/or Firewall Protections
   - Using Virtual Private Networks (VPN)
   - Backing up your Computing Devices

2. Requesting Access to IT Services and/or CMCC Data

   To request access to IT Services and/or CMCC Data, users are to contact the IT Helpdesk via email to helpdesk@cmcc.ca or by visiting https://helpdesk.cmcc.ca.

3. Reporting the Loss of a Computing Device

   In the event of loss of any Computing Device containing CMCC Data:
   - Employees are to immediately report to their manager, and notify Helpdesk by email at helpdesk@cmcc.ca.
   - Students are to report to Student Services or the Clinic Management Team.

4. Reporting Unauthorized Use and/or Disclosure of CMCC Data

   In the event of any unauthorized use and/or disclosure of CMCC Data:
   - Users are to immediately contact the Vice President, Administration and Finance (Chief Privacy Officer) using the Privacy Incident Report Form, which is available at CMCC-Public/Form Templates, and notify Helpdesk by email at helpdesk@cmcc.ca.
     - If the unauthorized data disclosure is patient information, the completed Privacy Incident Report Form is also to go immediately to the Dean, Clinics (Chief Health Records Custodian).
   - Students may contact Student Services or the Clinic Management Team for help in accessing the Privacy Incident Report Form.

New Procedures Approved (date):
August 27, 2020
Procedure Revision History (dates):