


Procedure Name:	CLOSED CIRCUIT VIDEO CAMERA	
Approved By:	Policy Review Committee	
Approval Date:	March 14, 2025	
Next Scheduled Renewal Date:	2026 or As Required	
Procedure Holder:	VP, Corporate Services & CFO	
Operational Lead:	Director, Facilities and Security Services	
Procedure Number:	FAC-010P	

## CLOSED CIRCUIT VIDEO CAMERA PROCEDURE

### 1.00 PURPOSE

- 1.1 This procedure is designed to ensure the consistent and standard application of Coast Mountain College’s (CMTN’s) closed circuit video camera (CCVC) system in all locations, consistent with FAC 010 *Closed Circuit Video Camera Policy*.

### 2.00 DEFINITIONS

In this policy, these terms have the following meanings:

- 2.1 **Bookmark:** A method of marking a section of recorded video to help the operator find and review the event later. Bookmarked video can be protected against scheduled data cleanup so that the video is never deleted. In the CMTN system, video footage is only bookmarked upon request.
- 2.2 **CIO:** Chief Information Officer.
- 2.3 **CCVC Audit:** An audit of the CCVC system conducted by CMTN.
- 2.4 **CCVC Maintenance:** The College administrator or other designated person responsible for a coordinating role in the installation, maintenance, and awareness of CCVCs at their location.
- 2.5 **CCVC Data:** Information captured using the CCVC system.
- 2.6 **Closed Circuit Video Camera (CCVC):** Any camera installation used in the CCVC system.
- 2.7 **CCVC System:** A closed system consisting of video cameras, display devices/ monitors, and wired or wireless data networks that allow images to be transferred from video cameras to monitors.
- 2.8 **College Community:** All CMTN employees, students, and board members, and any other person who is contractually obligated to comply with CMTN policy; for the purposes of this policy, includes employees of the CMTN Students’ Union.
- 2.9 **Director:** Director, Facilities and Security Services.
- 2.10 **Privacy Officer.** The senior official designated to investigate disclosures of security breaches.

### 3.00 ADMINISTRATIVE RESPONSIBILITIES

- 3.1 CCVC Maintenance, in consultation with the Director will perform a coordinating role on respective campuses by complying with all of the following:
  - a. coordinate the approval of the terms of use for new or expanded CCVC systems in accordance with FAC-010, *Closed Circuit Video Camera Policy*
  - b. oversee the installation of the CCVC system
  - c. maintain the CCVC system to ensure that it is working properly
  - d. provide guidance on compliance with FAC-010, *Closed Circuit Video Camera Policy*
  - e. promote awareness by the College Community on the appropriate use of CCVCs
  - f. cooperate in audits of the CCVC system conducted under FAC-010, *Closed Circuit Video Camera Policy*
  - g. assist, where appropriate, in the investigation of breaches and potential breaches of FAC-010, *Closed Circuit Video Camera Policy*.
- 3.2 Violation of the procedures for video recording and review will result in disciplinary action appropriate to the violation.
- 3.3 The Director is responsible for the planning and budgeting of the CCVC system for CMTN campuses.
- 3.4 Where renovation or new construction is involved, the Director will account for the CCVC system within the renovation or new construction budget and planning.
- 3.5 The Director is responsible for notifying the public about the CCVC system through signage and posting FAC-010, *CCVC Policy* and this procedure on its website.

### 4.00 RECORDS OF CLOSED CIRCUIT VIDEO CAMERAS

- 4.1 The records of the CCVC system will specify all of the following:
  - a. precise location of each camera
  - b. nature of each camera, including technical specifications such as resolution, frame rate, colour or grey scale, low light capability, and pan/tilt/zoom (PTZ) function
  - c. area under observation by each camera
  - d. specific purpose for each camera (e.g., deter and detect unauthorized entry).

### 5.00 RECORD KEEPING

- 5.1 The Director shall maintain a log of all access to the CCVC system.
- 5.2 If an incident involving public safety or damage to CMTN property occurs and a request for CCVC camera data has been made, where the CCVC system may have captured footage and the footage has not yet been deleted through the regular operation of the 30-day automatic deletion feature of the CCVC system, the Director will maintain a log of bookmarked requested CCVC camera data, including all of the following:
  - a. the date the data was saved
  - b. related incident report number
  - c. related investigation file name.

- 5.3 Footage captured by the CCVC system will only be kept past 30 days upon request.
- 5.4 A detailed activity log of the CCVC system will record all of the following:
  - a. CCVC-detecting activity resulting in a response by Campus Security
  - b. CCVC video that is being kept for one or more of the following reasons:
    - i. retained for investigative purposes
    - ii. used to make a legal or administrative decision with respect to an individual
    - iii. provided to a law enforcement officer under a subpoena, warrant, or approved request
    - iv. provided to individuals
    - v. provided to third parties under a subpoena or warrant
  - c. the denial of CCVC data for any reason to one or more of the following:
    - i. law enforcement officers
    - ii. individuals under surveillance
    - iii. third parties
  - d. written direction or authorization relating to any of the above
  - e. all other relevant information about each incident in question, including in the case of video or still pictures being retained for one year or more, a copy of the video or still pictures.
- 5.5 The CCVC digital activity log will be held in a safe and secure location with the CCVC equipment.
  - a. All authorized persons with access to the CCVC images are responsible for entering their own log data at the time of the activity.
    - i. This log is saved automatically and every user has a specific password.
  - b. This log will be audited by CMTN, as required.

## 6.00 RETENTION, STORAGE, ACCESS, AND MAINTENANCE

- 6.1 Except as provided in 6.2, all video or digital recordings maintained by authorized personnel will be automatically overwritten after 30 days from the date of recording.
- 6.2 Recorded CCVC data will be retained for more than 30 days if it meets one or more of the following criteria:
  - a. CCVC data that is needed to facilitate or document an investigation or legal proceeding may be retained for as long as required for that purpose.
  - b. CCVC data that has been used to make a decision that directly affects an individual must be retained for at least one year after the date of that decision.
- 6.3 The Director will retain recordings that contain personal information about an individual, and are used to make a decision that directly affects the individual, for one year after the decision is made pursuant to the [BC Freedom of Information and Protection of Privacy Act](#) (FOIPPA).
  - a. Recordings used for evidence in any criminal or civil proceedings will be retained by the Director until any subsequent appeal periods have expired.

- 6.4 CCVC system equipment, controllers, storage devices, and data will be stored in a secure on-site location with limited access by authorized personnel only in accordance with FAC-010, *Closed Circuit Video Camera Policy* and these procedures.
- 6.5 All storage devices that are not in use will be stored securely in a locked area located in a controlled access area.
- 6.6 Access to CCVC data on storage devices is limited to personnel authorized in writing by the Director, and who will be trained in the technical, legal, and ethical standards of appropriate camera and recorder use.
  - a. CCVC Maintenance will receive a copy of this procedure and provide written acknowledgement that they have read and understood its contents by signing a confidentiality agreement.
  - b. CCVC Maintenance will have a distinctive login and password assigned to them to identify their access to the CCVC system.
- 6.7 All equipment of the CCVC system will be reviewed and evaluated yearly.
- 6.8 A log of equipment maintenance will be retained in a secure location.

#### 7.00 AUDITING AND OVERSIGHT OF CAMERA SYSTEMS

- 7.1 The Director will ensure that periodic audits of the CCVC system (including monitors and storage systems) are conducted to ensure that:
  - a. the CCVC system is being used in accordance with the approved terms of use
  - b. the CCVC system has proven effective in addressing the problems it was intended to address
  - c. the problems that required the use of the CCVC system remain a concern
  - d. any changes needed in its use or configuration are made
  - e. the terms of use have received the required approval
  - f. the Director has considered whether there is a valid and substantive reason that justifies its termination in whole or part.
- 7.2 The Director will promptly and effectively address any concerns that are raised by audits conducted under these procedures.

#### 8.00 LEGALLY RELATED REQUESTS FOR CCVC DATA

- 8.1 Requests for access to or disclosure of recorded CCVC data from CMTN employees acting in the course of their duties will be referred to the Director.
- 8.2 Requests for recorded CCVC data from law enforcement agencies in Canada or further to any legal proceeding will be referred to the Director, who will not disclose the requested information except where the requester has provided written legal authorization to receive the information in the form of a subpoena or warrant, or where otherwise permitted by the BC [Freedom of Information and Protection of Privacy Act](#) (BC FOIPPA).

#### 9.00 REQUESTS RELATED TO PERSONAL INFORMATION

- 9.1 For any request of disclosure of images possibly captured by the CCVC system of the person requesting or in respect of another person lawfully made (e.g., by a parent or

legal guardian), the procedure for responding with such requests will be in accordance with [ADM-003, Freedom of Information and Protection of Privacy Policy](#), FAC-010, *Closed Circuit Video Camera Policy*, as applicable, and as follows:

- a. The person will forward a request in writing to the Privacy Officer for CMTN and, in addition to any of the requirements under [ADM-003, Freedom of Information and Protection of Privacy Policy](#), will include
  - i. the date and approximate time the image was captured
  - ii. a photograph of Government-issued identification for the person whose image may have been captured.
- b. Within three business days of receiving the request, the Director will inspect the digital files to determine if the camera in question recorded video at the specified time.
- c. If CCVC data was recorded by the camera at the specified time, the Director will review the recording to determine whether the person making the request appears in the recording.
- d. If an image of the person in respect of such a request appears in the recording, the relevant footage may be provided.
  - i. All video frames showing persons other than the person making the request and all frames that do not show the person making the request will be removed.
  - ii. The opportunity to view the footage with the VP Corporate Services & CFO will be scheduled. The requester of the footage is not authorized to record at the time of viewing.

9.2 CMTN will not provide CCVC data to a requesting party if one or more of the following conditions applies:

- a. the required information is not provided in the original request
- b. the camera in question did not record video at the time specified
- c. the recorded information has been automatically overwritten
- d. the person making the request does not appear in the recording
- e. other persons appear in each video frame in which the requester also appears, and CMTN is unable to protect the privacy of the other persons by masking, pixilation, or other means.

## 10.00 PRIVACY BREACH

10.1 In the event of a privacy breach to the CCVC system, the Vice-President of Corporate Services & CFO, the Director, and the Privacy Officer will undertake the following steps:

- a. Contain the breach:
  - i. Stop the leak of records, recover the information where possible, change the management practice if applicable, but generally do what needs to be done to stop the leakage of information.
  - ii. The Privacy Officer will lead an investigation.

- b. Evaluate the risks with respect to the breach:
  - i. Determine the nature of the information leaked and the possible illegitimate uses for the leaked information.
  - ii. Determine which individuals were affected by the breach and the harm that could potentially accrue to them.
  - iii. Determine the cause of the breach. For example, was the breach a result of a theft, or was it simply a loss? Is the breach a systemic problem or an isolated incident?
- c. Notify those affected:
  - i. Notification includes not only individuals whose personal information may have been compromised, but potentially the greater College Community, law enforcement organizations, insurers, and regulatory bodies (including the [Office of the Information and Privacy Commissioner](#)).
- d. Take steps to prevent any further breach of privacy:
  - i. Investigate the cause of the breach and take whatever steps are necessary to prevent another breach.
- e. Notify the Office of the Information and Privacy Commissioner about the potential breach.

11.00 RELATED POLICIES AND PROCEDURES

- 11.1 [ADM-003, Freedom of Information and Protection of Privacy Policy](#)
- 11.2 [FAC-010, Closed Circuit Video Camera Policy](#)

12.00 OTHER SUPPORTING DOCUMENTS

- 12.1 [Accountable Privacy Management in BC’s Public Sector](#), Office of the Information and Privacy Commissioner for BC, Feb. 2023
- 12.2 [BC Freedom of Information and Protection of Privacy Act](#)
- 12.3 [BC Privacy Impact Assessment Directions](#)

13.00 HISTORY

Created/Revised/ Reviewed	Date	Author’s Name and Role	Approved By
Created	Mar. 14, 2025	Director Facilities and Security Services	Policy Review Committee