

Policy History
Policy No. SR13
Approving Jurisdiction: President
Administrative Responsibility: Vice President Human Resources
Effective Date: September 2, 2025

Closed Circuit Video Equipment (CCVE) Procedure

A. DEFINITIONS

1. **CCVE:** Closed Circuit Video Equipment.
2. **DRS:** Director Risk and Security.
3. **Recording:** Video image recorded and stored by the CCVE system.
4. **RS:** Risk and Security.
5. **Safety/Security Event:** An event on a University campus involving the safety or security of persons or University property.
6. **The FIPPA:** The *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, c. 165
7. **The Policy:** Policy SR13 Closed Circuit Video Equipment (CCVE) Policy.
8. **University:** Kwantlen Polytechnic University.

B. PROCEDURES

1. Responsibilities

- a. The DRS oversees the management of the CCVE system operations and will ensure the day to day compliance with the requirements of the Policy and the *FIPPA*.
- b. The DRS or authorized designate will approve access to, use of and disclosure of recordings collected by the CCVE system.
- c. The DRS may not delegate his/her responsibilities under section 1(a), but

may by written delegation appoint an authorized designate to exercise his/her responsibilities under section 1(b).

2. Operation

- a. The CCVE system monitors identified locations, including exterior pathways, walkways and building entrance, egress points, parking lots, student enrolment services front counters, and others as deemed necessary to enhance safety and security across the University. The CCVE system cameras operate 24 hours a day, 7 days a week.
- b. Operation and access by identified individuals to the CCVE system must be approved by the DRS or authorized designate.
- c. In an emergency, and where it is not reasonably practical to secure prior authorization from the DRS or authorized designate, the Manager, Security Systems may grant access to persons whose job or responsibilities require access to the CCVE system.
- d. The DRS will conduct compliance audits to ensure that all access to and use of the CCVE system complies with the terms of this Procedure, the Policy and the FIPPA.
- e. A log recording all persons entering the CCVE monitoring area shall be kept. In addition, the security systems automatically record and retain User activity within the system.

3. Notification

- a. The DRS will ensure that signs providing notice of the CCVE equipment will be posted at all locations where cameras are active.
- b. Notices will be clearly visible and will advise the public of the use of surveillance, its purposes, the legal authority for its use, and contact information for a University official who can answer queries about the CCVE system.

4. Collection, Use, Disclosure, Retention, and Destruction of Recordings

- a. Recordings collected by the CCVE system will not be routinely monitored or reviewed on a continuous basis.
- b. Real-time monitoring will occur when authorized by the DRS or authorized designate. Real time monitoring of the CCVE system may occur: during an active Safety/Security Event (e.g. intrusion system activates, emergency on campus) that has been reported to the DRS; or, as otherwise permitted or required by law.
- c. Access to Recordings must be approved by the DRS or authorized designate. Such access may be granted in response to a Safety/Security Event or as permitted or required by law.
- d. The CCVE system will be used in compliance with the University's Policy EI1 Diversity & Inclusiveness.
- e. The CCVE System is protected by reasonable technological, organizational, and

physical security measures, including storage of all Recordings in a secure location and measures to prevent unauthorized access, use, disclosure, tampering, loss, theft and unauthorized duplication of Recordings.

- f. Recorded data will usually be retained until such time when the data is automatically recorded over, unless otherwise permitted or required by law. The retention period on each camera recording system is variable and is dependent on the total available storage space, resolution and numbers of cameras being recorded and the amount of motion or action observed by each camera. All recordings will be securely destroyed when no longer needed. Recorded data that has been saved to another medium, for investigation or evidentiary purposes, will be retained for at least one year after being used, or as otherwise permitted or required for legal, administrative or other purposes.
- g. Requests for access to Recordings will be processed as permitted or required under FIPPA or by applicable law.
- h. Subject to the foregoing, the University may, at its discretion, redact or provide opportunities to view footage rather than releasing copies of Recordings.

5. Locations

- a. Specific locations of the CCVE cameras will be chosen to meet the purposes and objectives of the CCVE system as set out in the Policy.
- b. CCVE cameras will be clearly visible to the public, and will not be directed to areas in which there is a usual expectation of privacy (e.g. residences or washrooms).
- c. Once cameras are installed, the field of view may only be adjusted with the permission of the DRS or designate.
- d. The CCVE system shall not be used for monitoring employees for the purposes of tracking productivity, attendance, or performance evaluation.

C. RELATED POLICIES

SR13 Closed Circuit Video Equipment (CCVE) Policy