CAPILANO UNIVERSITY	POLICY		
Policy No.	Officer Responsible		
OP.421	**Vice President, Finance and Administration**		
Policy Name			
Security Technology - Surveillance Systems			
Approved by	Replaces	Category	Next Review
SCL	**E.210 Video Surveillance**		**May 2026**
Date Issued	Date Revised	Related Policies	
May 2023	**New**	**B.700 Privacy and Access to Information**	

1 PURPOSE

This policy regulates video surveillance installations, monitoring and recording on Capilano University (the University) properties and in its facilities, and ensures appropriate use of surveillance systems and content, consistent with the *Freedom of Information and Protection of Privacy Act* (FIPPA), *The University Act* and other applicable legislation, and University policies and procedures.

2 DEFINITIONS

"Employee" means any person employed by the University, including volunteers.

"Lessee" means a person, or business, who holds a lease of a property; a tenant.

"Student" means an individual enrolled in any course (credit or non-credit) at the University.

"University community" means employees, students, agents, board members and volunteers.

"University premises or property" means any University owned or rented/leased lands, facilities, or vehicle or other transportation conveyance, including on-line forum.

"Video surveillance" means a system of monitoring activity in an area or building using a camera and recording system

"Visitor" means an individual or organization who is not a member of the University community. This can include alumni.

3 SCOPE

3.1 This policy is applicable on all University properties grounds and buildings that currently have, or in the future may have, video surveillance cameras that are part of the security technology, including the Main campus and the Lonsdale facility, Student Housing, and kálax-ay campus.

3.2 This policy does not address live video streaming for internet, or "web cams", for either operational or academic purposes; or, the recording of lectures or meetings in on-line forums.

3.3 Under this policy, the University does not have purview over the Ts'zil Learning Centre or any of the areas outside of University controlled properties grounds and buildings where our staff and faculty work or our students may learn.

4 POLICY

4.1 Video surveillance is an integral part of the security operations at the University.

4.2 Video surveillance cameras will be in operation on a 24-hour basis as a means of monitoring activities throughout the University to:

a) enhance the safety of students, employees, service providers and visitors,

b) protect University property against theft or vandalism,

c) aid in the identification of individuals engaged in potentially criminal activities or in activities disruptive to University operations,

d) discourage or prevent criminal or disruptive activity,

e) conduct investigations, and

f) monitor wildlife on campus that may pose safety concerns.

4.3 Information will not be retained or used for purposes other than those described above.

4.4 Video surveillance cameras will not:

a) be used to actively monitor employee performance,

b) be equipped to capture or record audio data,

c) be equipped with facial recognition and/or physiological biometrics recognition technology,

d) be installed in areas where there is a reasonable expectation of privacy, such as bathrooms and changing rooms.

Personal information is collected and disclosed in accordance with FIPPA.

4.5 Computer monitors used to review video surveillance recordings will be located in a secure area and restricted to authorized persons. Surveillance images must not be accessible or viewable by

non-authorized persons without out either a “need to know” for the performance of their duties and / or in accordance with the provisions of this Policy and FIPPA.

4.6 Video recording and review will be conducted in a professional, ethical and legal manner, consistent with the University’s *Privacy Impact Assessment*. Personnel involved in video recording and review will be appropriately trained and continuously supervised in the responsible use of this technology. Logs must be kept of all instances where recorded information has been accessed. Logs will detail who has accessed the recorded personal information, and how it was used.

4.7 Violation of the procedures for video recording and review will result in disciplinary action appropriate to the violation.

4.8 Signage will be posted at all camera locations on University property and buildings to inform the University community of the presence of video surveillance, why it is being done, the legal authority and a contact number for the office responsible.

4.9 To maintain an informed University community, the Office of Safety and Emergency Services will, on an annual basis, disseminate and publish written materials that describe the purpose and location of video surveillance cameras.

4.10 Any student, employee, service provider or visitor who has been recorded by a video surveillance camera has a right of access to their personal information under FIPPA by contacting the Office of Safety & Emergency Services. The Director of Safety & Emergency Services will work with the Manager, Campus Security on all requests, and inform the Privacy Officer. The University will withhold the personal information of individuals who are not the subject of the access request.

4.11 Disclosure to law enforcement will be in accordance with FIPPA and be properly documented on an information release form. All disclosures must be forwarded to the Director of Safety & Emergency Services who will work with the Manager, Campus Security, in conjunction with the Privacy Officer.

4.12 A *Privacy Impact Assessment* (PIA) will be completed when new surveillance cameras are installed and updated on a bi-annual basis, by the Office of Safety & Emergency Services and submitted to the Privacy Officer for approval by the Vice President, Finance and Administration (VP).

4.13 The PIA will consider:

a) Is video surveillance recording necessary to deliver a program or activity by the University?

b) Is video surveillance recording effective in meeting the objectives defined above?

c) Have other alternatives been explored?

d) In considering other alternatives, cost should be the last factor taken into consideration.

e) Is the loss of privacy proportional to the benefit gained by the University's use of surveillance cameras and video recordings?

f) What steps has the University taken in order to ensure the minimum amount of personal information is being recorded?

5 RETENTION

5.1 All recorded information will be destroyed after 30 days except information:

a) used in an internal investigation, consistent with the *Limitations Act*

b) specifically awaiting review by law enforcement agencies, and

c) information seized as evidence, or information that has been duplicated for use by law enforcement agencies.

6 COMPLAINTS

Any complaints relating to the collection, use, retention or storage of personal recorded information will be handled first by the Director of Safety & Emergency Services and any Privacy related complaints that cannot be resolved informally should be referred to the Privacy Officer to manage.

7 PRIVACY BREACHES

Privacy breaches are managed under the University's *Personal Information Incident Management Procedure*.

8 RESPONSIBILITIES

The Director of Safety & Emergency Services is responsible to:

a) ensure the safe operation of University facilities,

b) ensure the University has adequate resources to operate and maintain a video surveillance system, and

c) ensure that the video surveillance system is audited on a regular basis, in conjunction with the Privacy Officer, and

d) ensure that the video surveillance system complies with the *FIPPA*.

The Director of Safety & Emergency Services may delegate specific duties regarding the operation and maintenance of the system.

8.2 The Manager, Campus Security is responsible for:

a) overseeing and coordinating the video surveillance system at the University to ensure consistent and standard application across the campuses and facilities;

b) ensuring written procedures are in place;

c) ensuring that the use and security of video surveillance equipment is subject to annual audits and regular maintenance and address deficiencies or concerns identified by the audit; and
d) reviewing and evaluating the video surveillance system, at least once every calendar year, to ascertain whether it is still required in accordance with the procedures.

8.3 The Privacy Officer is responsible for:

a) in conjunction with the Director of Safety & Emergency Services, ensuring that the video surveillance system is audited on a regular basis; and
b) ensuring an updated PIA is conducted on an [annual / bi-annual] basis and/or when new cameras are installed.
c) Consulting on the release of requests for disclosure.

9 DESIGNATED OFFICER

The Vice President, Finance and Administration is the Policy Owner, responsible for the oversight of this Policy. The Administration of this Policy and the development, subsequent revisions to and operationalization of any associated procedures is the responsibility of the Director of Safety and Emergency Services.

10. RELATED REFERENCES

Freedom of Information and Protection of Privacy Act (FIPPA)

University Act [RSBC 1979]

Limitation Act [RSBC 1996]

Administrative Records Classification System [2014]

Using Overt Video Surveillance, Office of the Information & Privacy Commissioner for British Columbia