SAFETY AND SECURITY CAMERAS

THOMPSON RIVERS UNIVERSITY
805 TRU Way
Kamloops, BC V2C 0C8
tru.ca

POLICY NUMBER	ADM 31-0
APPROVAL DATE	October 28, 2019
AUTHORITY	President
CATEGORY	Administrative
PRIMARY CONTACT	Privacy and Access Office
ADMINISTRATIVE CONTACT	(TBD)

POLICY

The University employs safety and security camera technology to enhance the safety and security of the University community and to protect the University's assets and property. The University recognizes and is committed to using this technology in a manner that respects and safeguards the privacy of those who work, study, visit and live on the University's campuses.

REGULATIONS

1. PURPOSE

The purpose of this Policy is to ensure that Camera Systems[1] are set-up and configured to surveille and/or record identifiable images of individuals in compliance with:

1.1. relevant University policies;

1.2. information security best practices; and

1.3. applicable legislation including the BC Freedom of Information and Protection of Privacy Act (FIPPA).

2. SCOPE

2.1. This Policy applies to all Camera Systems that are operated by the University or by Service Providers (as that term is defined in FIPPA) to the University, with the exception of Camera Systems used for the following purposes:

a. communications, such as videoconferencing systems;

b. technical support of information technology/audiovisual systems;

[1] Capitalized terms in this Policy have the meaning ascribed to them in the definition section below.

c. academic instruction, and exam invigilation;

d. research projects approved by the University Research Office; and

e. to cover specific events temporarily (e.g. convocation, town hall meetings, etc.).

2.2. This Policy does not apply to buildings and areas that are not in the possession of the University. TRU residences are in the possession of the University.

3. GENERAL

3.1. The University will collect Personal Information using Camera Systems only when the information relates directly to and is necessary:

a. to assist in the protection of the safety of individuals, or property;

b. to assist in the prevention and investigation of criminal activity, injury, property loss, or violation of University policies; or

c. for other purposes expressly authorized by law.

3.2. No Camera System may be installed, modified, replaced, or expanded (collectively "Camera System Installation/Enhancement") unless such Camera System Installation/Enhancement is first approved under this Policy.

3.3. Applications for a Camera System Installation/Enhancement (an "Application") must address the Application Criteria (attached as Appendix A) and be submitted in writing to the Director. Applications reviewed and deemed complete by the Director will be forwarded to the Information Security Committee (ISC) for its review and recommendation. A recommendation for or against approval by the ISC will be forwarded to the Vice-President Administration and Finance for his/her consideration. Approvals by the Vice-President Administration and Finance must be documented in writing and implemented and managed in accordance with this Policy.

3.4. A Privacy Impact Assessment must completed by the University's Privacy and Access Office and must accompany each Application.

3.5. Within 12 months of the approval of this Policy, all existing uses of Camera Systems and their supporting systems and software must comply with Parts 5, 6 and 7 of this Policy.

4. DEFINITIONS

4.1. Camera System(s) means any camera installation (including streaming cameras) for both closed circuit and internet protocol (IP) cameras operated by or for the University, their monitors, storage and supporting systems and software, except for a system that does not capture images of identifiable individuals. This does not include portable personal devices such as smart phones.

4.2. Camera Data means information captured and/or created by a Camera System.

4.3. Covert Camera means any camera for which there is no prominently posted Privacy Notification signage.

4.4. Director means the Director, Risk Management Services.

4.5. Privacy Intrusive Cameras means cameras located in areas where there is an expectation of privacy (e.g. classrooms or offices).

4.6. Personal Information means recorded information about an identifiable individual, but excludes business contact information.

4.7. Security Team means the University's contract security company's staff members who are responsible for University security services, and in emergencies also includes the Director, the Emergency Operations Centre (EOC) Incident Commander and EOC team.

4.8. Surveille/Surveillance means real-time live viewing of individuals (with or without recording).

5. ACCEPTABLE USES OF CAMERA SYSTEMS AND DISCLOSURE OF CAMERA DATA

5.1. All Camera Data will be treated as though it contains Personal Information.

5.2. All Personal Information collected through a Camera System is confidential and may only be used or disclosed in accordance with the FIPPA. Camera Data will not be disclosed to parties other than the University or the University's Service Providers (as defined by FIPPA) without the prior written approval of the Privacy and Access Officer, the Director or the Vice-President Administration and Finance. All requests for such data must be in writing.

5.3. TRU's Access Control Standard outlines Camera System access requirements. No one will have access to Camera Systems or Camera Data until they have completed the TRU Information Security Training Programme.

5.4. Notwithstanding other provisions of this Policy, the University's Privacy and Access Office will manage requests for Camera Data submitted under the FIPPA as an access to information application.

5.5. Camera Data will be retained for no more than 30 days with the following exceptions:

a. if it is needed to facilitate or document an investigation or legal proceeding, it may be retained as required for that purpose; or

b. retention beyond the 30-day period is approved by the Vice-President Administration and Finance.

5.6. Camera Systems will not be used for the purposes of employee performance

management.

6. PRIVACY INTRUSIVE CAMERA SYSTEMS AND COVERT CAMERAS

6.1. Privacy Intrusive Cameras may only be installed in exceptional cases where clear and specific grounds exist that make it necessary to use them and where there is:

a. a strong possibility that their use will be effective; and

b. there is no reasonable alternative for their use in all of the circumstances.

6.2. Privacy Intrusive Cameras:

a. will be discontinued at the earliest available opportunity;

b. will be used for a maximum period of six months unless an extension to this period is granted in writing by the Vice-President Administration and Finance; and

c. are not permitted inside washrooms or change rooms.

6.3. Covert Cameras are not be permitted on TRU campuses and property without the prior written approval of the Vice-President, Administration and Finance.

7. PUBLIC AWARENESS OF CAMERA SYSTEMS

7.1. Cameras must not be hidden or disguised without the prior written approval of the Vice-President, Administration and Finance. Camera signage will notify the University community and the public about camera location(s) so individuals have notice when entering a monitored area. Where practical, signage will provide an internet address for a publicly posted Safety and Security Camera Privacy Notification.

7.2. The publicly posted Safety and Security Camera Privacy Notification will follow University Privacy Notification standards, which are consistent with privacy law requirements.

8. OVERSIGHT AND AUDITING OF CAMERA SYSTEMS

8.1. The Director has primary responsibility for Camera Systems at the University and shall maintain and update as required a central log inventory of all Camera Systems that includes:

a. camera type;

b. camera location;

c. field of view for each camera;

d. special camera capabilities as outlined in Appendix A - 3(b);

e. if the camera does real time monitoring, recording or both (ongoing or periodic); and

f. placement of notification signage near camera locations.

8.2. The Director shall prepare annual reports on the use of all Camera Systems and present these reports annually to the ISC.

8.3. The University's Privacy and Access Office will conduct periodic audits of each University Camera System to assess compliance with this Policy and to make recommendations to the Information Security Committee:

a. whether any changes need to be made in the use or configuration of the cameras/Camera System; and

b. whether the camera use should be terminated because:

i. it was installed after November 1, 2019 without complying with this Policy;

ii. it is not being used in accordance with this Policy;

iii. it has proven ineffective in addressing the problem it was intended to address;

iv. the problems that justified the Camera System's use in the first place are no longer significant; or

v. there is another reason to justify its termination.

Appendix A

Camera System Application Criteria

Requests to install or expand Camera Systems owned or operated by/on behalf of TRU must consider and clearly address the following criteria:

1. Rationale
   a. The purpose/objective for these cameras.

   b. The necessity for the use of cameras in the proposed location.

   c. What less privacy intrusive alternatives were considered and why they were rejected.

2. Scope

   a. Description of area(s) to be monitored and placement of cameras (including diagrams showing fields of view).

   b. Number of cameras to be installed/added.

   c. Individuals who will be affected by the camera installation (public, employees, students, etc.).

   d. Type of cameras to be used (video, audio, steaming, surveilling or recording).

3. Privacy

   a. How cameras will be positioned/configured to collect the minimum amount of personal information necessary to achieve the purpose of the collection.

   b. Special camera capabilities (zoom, facial recognition, night vision, license plate recognition, appearance recognition, etc.).

   c. Will there be real-time (surveillance) monitoring?

   d. Rationale and expected benefits of real-time monitoring. (Consider conducting stakeholder consultations to assist in determining the merits of the proposed surveillance.)

   e. When will recording occur?

   f. How will notification about the Camera System's use be provided.

4. Security of Camera System and Camera Data

   a. Technical/Physical security arrangements of the Camera System and Camera Data.

   b. Where Camera Data will be received and/or monitored. (Location of a suitable monitoring station in a controlled area).

c. How/where Camera Data will be stored.

d. Security arrangements to protect against unauthorized access to and viewing of Camera Data (including backup data).

e. Will remote access of the Camera System be permitted, under what circumstances and how will that access be secured.

Safety and Security Camera System Application Form

Name: **Department:**

Proposed Camera Location:

Date of Application:

1. **Rationale**

a	Purpose/objective for these cameras.	
b	The necessity for the use of cameras in the proposed location.	
c	What less privacy intrusive alternatives were considered and why they were rejected.	

2. **Scope**

a	Description of area(s) to be monitored and placement of cameras (including diagrams showing fields of view).	
b	Number of cameras to be installed/added.	
c	Individuals who will be affected by the camera installation (public, employees, students, etc.).	
d	Type of cameras to be used (video recording, audio recording, live-steaming).	

3. **Privacy**

a	How cameras will be positioned/configured to collect the minimum amount of personal information necessary to achieve the purpose of the collection.	
b	Special camera capabilities (zoom, facial recognition, night vision, license	

	plate recognition, appearance recognition, etc.).	
c	Will there be real-time (surveillance) monitoring?	
d	Rationale and expected benefits of real-time monitoring[2].	
e	When will recording occur.	
f	How will notification about the Camera System's use be provided.	

4. Security of Camera System and Camera Data

a	Technical/Physical security arrangements of the Camera System and Camera Data.	
b	Where Camera Data will be received and/or monitored. (Location of a suitable monitoring station in a controlled area.)	
c	How Camera Data will be stored.	
d	Security arrangements to protect against unauthorized access to and viewing of Camera Data (including backup data).	
e	Will remote access of the Camera System be permitted, under what circumstances and how will that access be secured.	

[2] Consider conducting stakeholder consultations to assist in determining the merits of the proposed surveillance.

Safety and Security Camera System Application Form

Name: Joe Worker **Department:** Facilities

Proposed Camera Location: Parking Lot ZZ3 (fictitious)

Date of Application: April 15, 2019

1. **Rationale**

a	Purpose/objective for these cameras.	To reduce vandalism and theft from vehicles in parking lot ZZ3.
b	The necessity for the use of cameras in the proposed location.	Over the past three months there has been a rash of broken car windows and items stolen from cars parked in parking lot ZZ3.
c	What less privacy intrusive alternatives were considered and why they were rejected.	TRU has increased foot patrol by security personnel but this has not been effective in reducing the problems in parking lot ZZ3

2. **Scope**

a	Description of area(s) to be monitored and placement of cameras (including diagrams showing fields of view).	The new small parking lot (20 stalls) behind the Animal Health Technology building and near the TRU warehouse. Locations of camera and fields of view are mark on attached map.
b	Number of cameras to be installed/added.	Initially there will be two cameras. With the expected improvements, this may be reduced to one camera after a trial of four months.
c	Individuals who will be affected by the camera installation (public, employees, students, etc.).	Public, students, staff
d	Type of cameras to be used (video recording, audio recording, live-steaming).	Video recording

3. **Privacy**

a	How cameras will be positioned/configured to collect the minimum amount of personal information necessary to achieve the	Cameras will located at each end of parking lot ZZE. The cameras will capture images anyone entering this parking lot. (see attached map)

	purpose of the collection.	
b	Special camera capabilities (zoom, facial recognition, night vision, license plate recognition, appearance recognition, etc.).	Cameras have zoom, night vision and facial recognition capabilities.
c	Will there be real-time (surveillance) monitoring?	Yes.
d	Rationale and expected benefits of real-time monitoring[3].	Real-time monitoring will occur after dusk. Real-time monitoring will allow Security staff to quickly respond to any issues in parking lot ZZ3 as they arise and are witnessed on the Camera System monitors.
e	When will recording occur.	Cameras will continuously record.
f	How will notification about the Camera System's use be provided.	Privacy Notification signage will be posted both ends of Lot ZZ3, advising about the use of Safety and Security Cameras in parking lot ZZ3.

4. Security of Camera System and Camera Data

a	Technical/Physical security arrangements of the Camera System and Camera Data.	Cameras will link into the general TRU camera system. There is a physical barrier to access the area were the camera monitors are located. A password is required to access Camera Data.
b	Where Camera Data will be received and/or monitored. (Location of a suitable monitoring station in a controlled area.)	HOL security station – main floor (where the existing camera monitoring station is located).
c	How Camera Data will be stored.	Encrypted on a TRU server.
d	Security arrangements to protect against unauthorized access to and viewing of Camera Data (including backup data).	Any access to the Camera System where the data is stored creates logs that records who accesses the Camera System and Data. Logs can be reviewed should unauthorized access to Camera Data be suspected, and can be used for audit purposes.
e	Will remote access of the Camera System be permitted, under what circumstances and how will that access be secured.	There will be no remote access to parking lot ZZ3 cameras.

[3] Consider conducting stakeholder consultations to assist in determining the merits of the proposed surveillance.

Safety and Security Camera System Application Form
Proposed Location Map

Location of parking lot ZZ3 (fictitious).

Black arrows indicate fields of view (covers entire parking lot).