Closed Circuit Television Surveillance Procedures – SF 3.1

Procedures Title:	**Closed Circuit Television Surveillance Procedures**
Associated Policy:	Closed Circuit Television Surveillance, SF 3.0
Procedure Holder:	Safety and Security Services Department
Executive Lead:	Manager, Safety and Security
Original Date:	March 2025
Last Revised:	n/a
Next Review:	March 2027

1. Purpose and Background

1.1. Yukon University ("University") recognizes the need to strike a balance between the individual's right to privacy and the University's duty to promote and maintain a safe and secure environment for students, staff, faculty, residents and visitors.

1.2. The use of closed circuit television ("CCTV") surveillance systems results in the collection of personal information in the form of images and records the conduct of individuals. CCTV surveillance systems are employed by the University to record unlawful conduct as well as to prevent and to deter such conduct. Information obtained from CCTV systems is also used as an aid in the investigation of such conduct.

1.3. These procedures will provide direction for the appropriate use of CCTV surveillance on University campuses for the purposes of safety and security.

2. Guiding Principles

2.1. To provide protective security, reassurance, and community safety to all campus users.

2.2. To ensure compliance with the Access to Information and Protection of Privacy Act ("ATIPP").

2.3. To ensure every entrance/exit to the University has signage making persons aware that CCTV surveillance is in place.

2.4. To ensure responsibilities and procedures outlining the installation, monitoring, and recording of CCTV surveillance systems are clearly identified.

2.5. To clearly outline who has authorized access to CCTV monitoring and recordings and how long CCTV recordings are stored.

3. Procedures

3.1. Responsibility

Responsibility for implementation and operation of CCTV surveillance resides with the Safety and Security Services Department, which will establish best practices and will include the following:

3.1.1. The CCTV system will be placed in public areas where there would be no reasonable expectation of privacy.

3.1.2. Appropriate signage will be in place at all entrances/exits to the University advising of the use of CCTV cameras.

3.1.3. No one should assume the presence of CCTV surveillance on campus will always guarantee the safety of persons or property. Instead, CCTV surveillance is a tool in the University's continuing efforts to increase campus safety and security.

3.1.4. Individuals shall not tamper with any CCTV equipment.

3.1.5. Security Personnel will be trained and aware of their responsibilities with respect to safeguarding personal privacy.

3.1.6. The Manager of Safety and Security Services or designate will conduct a documented operational audit of the CCTV surveillance program annually and ensure that the implementation and operation of all CCTV systems comply with these procedures.

3.2. Installation

3.2.1. Requests for CCTV installation must be made to the Manager of Safety and Security Services.

3.2.2. Requests for CCTV installations will be approved by the Manager of Safety and Security Services in consultation with the Director of University Infrastructure and the manager of any affected department.

3.2.3. Requests for CCTV installations will normally be considered during the annual audit unless the installation is identified to be time sensitive.

3.2.4. CCTV cameras will be installed in public areas, such as hallways, common areas, parking lots, and walkways.

3.2.5. The University will make every effort to position cameras so that they only cover University premises or occupied spaces.

3.2.6. CCTV surveillance for the purpose of monitoring work areas or sensitive areas may only occur in special circumstances where approved by the Director of University Infrastructure and the Provost & Vice-President Academic.

3.2.7. Where CCTV surveillance is to be installed in Campus Housing areas the Director of Hospitality Services (Campus Housing) will be consulted.

3.3. Monitoring

3.3.1. Only individuals authorized by the Manager of Safety and Security Services following a reasonable vetting process will be permitted to monitor the CCTV surveillance system.

3.3.2. Some cameras may be actively monitored though the majority will not be actively monitored. The Manager of Safety and Security Services will maintain a confidentially held plan which outlines which CCTV cameras will be actively monitored and by whom. Authorized employees who do not adhere to this plan will be subject to disciplinary measures.

3.3.3. CCTV monitoring shall be conducted in a professional, ethical and legal manner only by authorized employees who have signed a confidentiality agreement.

3.3.4. Personnel involved in CCTV monitoring will be appropriately trained and supervised in the lawful and responsible use of this technology.

3.3.5. Personnel who monitor CCTV cameras will be subject to a criminal background check by the University, which will include a police services vulnerability screening.

3.3.6. CCTV monitoring shall be limited to uses that do not violate a person's reasonable expectation of privacy.

3.4. Securing and Retaining Images

3.4.1. No attempt shall be made to alter any part of a CCTV recording.

3.4.2. CCTV recordings, which have not been viewed for law enforcement or public safety purposes, will be retained for a minimum of 14 days and a maximum of 90 days unless an extension is authorized by the Manager of Safety and Security Services or designate.

3.4.3. No CCTV recording is to be retained after 90 days unless requested by the Manager of Safety and Security Services, solely for the purpose of an investigation.

3.4.4. Copies of CCTV recordings shall be managed by security personnel. All copies of recorded data from the CCTV surveillance system shall be recorded in a logbook and shall only be made for investigative and/or evidence purposes except as outlined in 3.5.1.

3.4.5. CCTV recordings used for law enforcement or public safety purposes will be destroyed in a secure manner after one (1) year from the time they were created or following court proceedings and the expiry of any relevant appeal period, whichever occurs later.

3.5. Access to Images

3.5.1. Disclosure of CCTV recordings to third parties will only be made in accordance with the purpose(s) for which the system was installed, and will be limited to:

- 3.5.1.1. Law enforcement agencies for the purpose of an investigation.
- 3.5.1.2. Prosecution agencies.
- 3.5.1.3. Relevant legal representatives.
- 3.5.1.4. Members of staff involved in University disciplinary processes.
- 3.5.1.5. For use at a formal University proceeding such as a Student Code of Conduct hearing.
- 3.5.1.6. To assist in the identification of individuals relating to a criminal incident.
- 3.5.1.7. To comply with a Freedom of Information request by the person whose identity has been recorded and who shall have the right to access such information, unless an exemption under ATIPP applies.
- 3.5.1.8. Other circumstances as approved by the University Secretariat.

3.5.2. CCTV recordings will be stored in a secure location.

3.5.3. CCTV recordings will be released to news or media sources only with the approval of the President.

3.5.4. All other requests will be facilitated according to the ATIPP.

3.6. Non-Compliance with this Policy

3.6.1. Any non-compliance of this policy by University departments, individuals or third-party suppliers shall be reported to the Manager of Security and Safety Services.

3.6.2. The Director of University Infrastructure will review all reports of non-compliance and advise the Provost & Vice-President Academic to determine the appropriate resolution or sanction.

3.6.3. Personnel charged with monitoring CCTV surveillance and recording CCTV data will be subject to discipline if they breach the policy or relevant procedures of the University.

4. Exceptions to the Procedures

There are no foreseen exceptions to these procedures.

5. Problem Solving

Any questions arising out of the content or communication of this policy or disputes arising from a decision made as a result of applying this policy should be first reported to the Executive Lead who will endeavor to find a resolution with all stakeholders. Failing such a resolution, the matter should be reported to the University Secretariat.

6. Document History

Include all updates here, including non-substantive changes, beginning with formal approval.

Date (Month DD, YYYY)	*Update (*Approver: change)
March 2025	The Procedures established as approved by the President