

**CLOSED CIRCUIT TELEVISION VIDEO SURVEILLANCE**

Section:	Administration (AD)
Subject:	Security
Legislation:	<i>Freedom of Information and Protection of Privacy Act (RSA 2000 cF-25); Personal Information Protection Act (SA 2003, cP-6.5); Privacy Act, R.S.C.1985, c.P-21; Security Services and Investigators Act (SA 2008 cS-4.7).</i>
Effective:	November 17, 2015
Revision:	September 1, 2016 (reformatted)

**APPROVED:** \_\_\_\_\_  
**President and CEO**

## POLICY

The policy of the Board of Governors is to provide a safe and secure work and learning environment for all members of the SAIT community through the effective use of closed circuit television video surveillance.

## PROCEDURE

### DEFINITIONS

**CCTV surveillance**

A television system in which signals are not publicly distributed but are monitored and recorded, primarily for surveillance and security purposes. The signals are transmitted from a television camera to receivers by cables or telephone links forming a closed circuit. References throughout this procedure to CCTV surveillance also includes reference to "other video surveillance", defined below.

**Law enforcement**

Policing, including but not limited to criminal investigations or proceedings having the potential of leading to penalties or sanctions.

*The official controlled version of this document is held in the Board of Governors Office.*

<b>Other video surveillance</b>	A system of monitoring activity using an audiovisual system in which systems are not publicly distributed but are monitored and recorded, primarily for surveillance and security purposes.
<b>SAIT community</b>	SAIT's governors, employees, students, contractors, consultants, agents, volunteers and visitors.

## GOVERNING PRINCIPLES

1. This procedure regulates the installation, use and destruction of CCTV surveillance at SAIT. The purpose of such surveillance is to assist in the protection of the SAIT community and its assets, deter crime and anti-social behavior, safeguard academic integrity, support an immediate response to active incidents and assist with any student misconduct proceedings and/or criminal investigations.
2. All public areas of the SAIT campus, as well as on or in SAIT-owned or operated property, are subject to CCTV surveillance. CCTV surveillance will not be placed in or on areas in which individuals have a reasonable expectation of privacy, including but not limited to locker rooms and washrooms.
3. The collection, use and distribution of CCTV surveillance and any other video surveillance must adhere to all applicable municipal, provincial and federal legislation, and be consistent with SAIT's other policies and procedures.
4. The responsibility for the use, installation and maintenance of CCTV equipment and technology rests with the Facilities Management department. The surveillance of the records that the CCTV surveillance system produces shall be managed by Security and Emergency Services, and carried out by the Security department.
5. Information obtained through CCTV surveillance will be used only for the purposes described in Governing Principle 1 of this procedure.
6. This procedure does not apply to surveillance used for law enforcement as an investigative tool where such activity is authorized by the police or RCMP or similar authorities, by legislation, or by court order.

*The official controlled version of this document is held in the Board of Governors Office.*

## PROCEDURE

### A. CCTV Surveillance Equipment Set-Up and Maintenance

1. The manager of Security and Emergency Services or designate must approve the installation and use of all video surveillance equipment, as well as the disabling or disconnection of CCTV surveillance.
2. The Information Systems department and Security will coordinate all testing of and repairs to the CCTV surveillance system. Security will test the operation of all cameras and related equipment monthly or as it deems reasonable and will immediately report any malfunctions or concerns to Information Systems.

### B. Use and Monitoring of Records Obtained through CCTV Surveillance

1. The manager of Security and Emergency Services is responsible for the supervision of the use of CCTV surveillance equipment and records.
2. Information obtained through the CCTV surveillance system will only be released or disclosed upon the authorization of the manager of Security and Emergency Services or designate, and in accordance with the provincial protection of privacy legislation.
3. All records created by CCTV surveillance equipment will be utilized and stored in a restricted-access area. Access to this space is restricted to authorized members of Security and Information Systems personnel. CCTV surveillance equipment, or any records therefrom, may only be removed from the restricted-access area upon the written authorization of the manager of Security and Emergency Services or designate.
4. Monitoring of CCTV surveillance shall only be conducted by authorized members of Security. The manager of Security and Emergency Services or designate must ensure that those members of Security authorized to monitor the CCTV surveillance are aware of the privacy considerations and obligations owing to individuals pursuant to provincial legislation.
5. All staff authorized to utilize the CCTV surveillance system will be trained and continuously supervised in the responsible use of this technology in accordance with this procedure as well with applicable legislation.
6. Violations of standard operating practices or the misuse of any equipment associated with the CCTV surveillance system will result in disciplinary action up to and including

***The official controlled version of this document is held in the Board of Governors Office.***

dismissal or removal from the SAIT campus premises, as per the provisions of procedure [HR.4.4.1 Corrective Action Procedures](#) and any applicable agreements and contracts.

### **C. Retention Period**

1. If a CCTV surveillance record is not viewed for law enforcement purposes or for the purposes set out in Governing Principle 1 of this procedure, the record shall be retained for a period of 21 calendar days and then deleted or otherwise disposed of by Security.
2. If a CCTV surveillance record has been reviewed for law enforcement purposes or for the purposes set out in Governing Principle 1 of this procedure, the record shall be retained for the longer of:
  - a) One year from the date of viewing; or
  - b) One year from the date of final resolution of the incident.

Should this section conflict with any SAIT records retention policy or procedure or with any applicable legislation, the records retention policy or procedure or applicable legislation, as the case may be, shall prevail.

### **D. Protection of Privacy**

1. Surveillance cameras and equipment must not be positioned towards property or windows adjacent to SAIT-owned or operated property.
2. CCTV surveillance equipment may be installed in private offices where there is a pending security concern and the manager of Security and Emergency Services has received written notice of consent from the office's occupant, or due to reasons of law enforcement.
3. CCTV surveillance monitors must be located in a secure, restricted-access location, away from public view.

*The official controlled version of this document is held in the Board of Governors Office.*

**E. Notice**

1. Signage will be prominently displayed throughout campus at appropriate locations, including all general entrances, to provide individuals with notice that:
  - a) There may be video surveillance cameras in all public areas of campus, as well as on or in SAIT-owned or operated property, that may be used to record and monitor activity.
  - b) Personal information collected through the video surveillance system may be disclosed for disciplinary, legal or public safety and security purposes or in accordance with any court order or subject to SAIT's policies or procedures or applicable legislation.
  - c) Individuals may contact Security should they require additional information or have concerns regarding CCTV surveillance.
2. CCTV surveillance shall not be used to monitor any specific person unless the individual is engaged in suspicious or criminal behavior that may threaten the safety and security of the SAIT community or its buildings or assets.

**F. Access to Records**

1. Requests for access to the recorded CCTV surveillance images must be submitted in writing to the manager of Security and Emergency Services or designate. Disclosure will be approved only if the applicant demonstrates a legitimate right of access to the information in accordance with applicable legislation.
2. Breaches of this procedure, including the unauthorized installation or use of CCTV surveillance, shall be addressed through the provisions of procedure [HR.4.4.1 Corrective Action Procedures](#) and through any applicable agreements and contracts.

**POLICY/PROCEDURE REFERENCE**

AD.4.4            Closed Circuit Television Video Surveillance policy

*The official controlled version of this document is held in the Board of Governors Office.*