*Procedure*

| Procedure Name | **Surveillance Systems** | | |
|---|---|---|---|
| Procedure # | CS 1.2 | Parent Policy | CS 1.0 Campus Security |
| Policy Owner | Vice President Administration and Chief Financial Officer | Effective Date | September 1, 2020 |
| Procedure Owner | Executive Director, Risk Management Services | Review Date | September 1, 2025 |
| Approved by | Executive Director, Risk Management Services | Approval Date | August 17, 2020 |

## 1.0 Purpose/ Background

1.1 NAIT has a surveillance camera system known colloquially as the “CCTV system” across its campuses and properties. The surveillance system is owned and managed by NAIT, and the system operates 24 hours a day, every day of the year across academic, administrative and commercial sites to meet the requirements of the institution.

1.2 This procedure details the purpose, use and management of the surveillance system at NAIT and details the procedures to be followed in order to ensure that the NAIT community complies with all relevant legislation and the current guidance issued by the Office of the Information and Privacy Commissioner of Alberta.

1.3 NAIT will have due regard to the *Freedom of Information and Protection of Privacy Act* of Alberta (FOIP Act) and any subsequent data protection legislation. NAIT will also have due regard to the Guide to Using Surveillance Cameras in Public Areas (Service Alberta, June 2004) and the guiding principles contained therein.

1.4 The purpose of the NAIT surveillance system is as follows:

- 1.4.1 The prevention, reduction, detection and investigation of crime and other incidents.
- 1.4.2 To promote the safety of staff, students and visitors.
- 1.4.3 Monitor the security of NAIT buildings and areas.
- 1.4.4 The monitoring and enforcement of traffic-related matters.

1.5 This procedure applies to all NAIT surveillance systems.

1.6 Excluded from the procedure are any recordings associated with academic, research or marketing programs.

## 2.0 Definitions

| Term | Definition |
|---|---|
| Covert Surveillance | Refers to the secretive continuous or periodic observation of persons, vehicles, places or objects to obtain information concerning the activities of individuals, which is then recorded in material form, including notes and photographs. |
| Disclosure | Refers to the release of relevant information. Disclosure includes viewing or making a copy of a recording of images and/or audio. |
| Personal Information | Is defined in section 1(n) of the FOIP Act (Alberta) as recorded information about an identifiable individual, including the individual's race, colour, national or ethnic origin; the individual's age or sex; the individual's inheritable characteristics; information about an individual's physical or mental disability; and any other identifiable characteristics listed in that section. |
| Reception Equipment | Refers to the equipment or device used to monitor, or record information collected through a surveillance system. |
| Record | Is defined in section 1(q) of the FOIP Act (Alberta) as a record of information in any form and includes notes, images, audio-visual recordings, x-rays, books, documents, maps, drawings, photographs, letters, vouchers and papers and any other information that is written, photographed, recorded or stored in any manner, but does not include software or any mechanism that produces records. In the context of this procedure, "record" includes digitally recorded or stored media such as images and/or audio. |
| Storage Device | A mechanical or electronic device or system used to store the recorded visual images and/or audio from a surveillance system. |
| Surveillance System | A mechanical or electronic system or device that enables monitoring, recording, recognition or analysis of visual images and/or audio. Image recognition is the ability of the system to recognize and identify objects, places, people, text and actions through software and artificial intelligence. Surveillance systems include Automatic Number Plate Recognition (ANPR), License Plate Recognition Cameras (LPR), body-worn cameras, covert installations. |

## 3.0 Procedures

### 3.1 General Procedures

3.1.1 NAIT recognizes the need to strike a balance between the individual's right to be free from unwarranted invasion of privacy and the duty to promote a safe environment for all community members.

3.1.2 NAIT considers its premises to be a supervised environment where a reasonable and limited degree of monitoring, as outlined in this procedure, is appropriate.

3.1.3 Surveillance equipment will be placed only in public areas where those under surveillance would have no reasonable expectation of privacy.

3.1.4 NAIT seeks to operate its surveillance system in a manner that is consistent with respect for the individual's privacy. Any proposed new installation shall be subject to a Surveillance Camera Privacy Impact Assessment Questionnaire.

3.1.5 Compliance with Data Protection Legislation.

3.1.5.1 In its administration of the surveillance system, NAIT complies with the Freedom of Information and Protection of Privacy Act of Alberta and Guide to Using Surveillance Cameras in Public Areas (Service Alberta, June 2004). Due regard is given to the data protection principles embodied in the guide. These principles require that:

a) No personal information shall be retained beyond a reasonable timeframe unless the information is necessary for the operating and activity of NAIT.

b) Surveillance cameras should be used only where conventional means for achieving the same objectives are substantially less effective than surveillance, and the benefits of surveillance substantially outweigh any reduction of privacy in the existence and use of the system held only for specified purposes and not used or disclosed in any way incompatible with those purposes.

c) The use of a surveillance camera should be able to be justified on the basis of verifiable, specific reports of incidents of crime (e.g. vandalism, theft), safety concerns or other compelling circumstances.

d) A Surveillance Camera Privacy Impact Assessment Questionnaire should be completed by NAIT Protective Services to assess the effects that the surveillance system may have on privacy and the ways in which any adverse effects can be mitigated.

e) Consultation will be conducted with relevant stakeholders as to the necessity, and acceptability of the proposed surveillance.

f) The proposed design and operation of the surveillance system creates no greater privacy intrusion than is absolutely necessary to achieve its goals.

3.1.6 Monitoring Compliance.

3.1.6.1 The Executive Director, Risk Management Services is responsible for the overall management and operation of the surveillance system, including activities relating to installations, recording, reviewing, retention, monitoring and ensuring compliance.

3.1.6.2 All staff involved in the operation of NAIT's surveillance system will be instructed on this procedure and will only be authorized to use the system in a way that is consistent with the procedure and the Code of Practice. Any unauthorized use will be subject to disciplinary action up to and including dismissal and may be referred for criminal investigation if used for illegal purposes.

3.1.6.3 All staff with responsibility for accessing, recording, disclosing or otherwise processing images will be required to undertake annual FOIP awareness training in addition to public space surveillance operators training.

**3.2 Signage**

3.2.1 Signage will be placed at pedestrian and vehicular entrances to inform staff, students, visitors and members of the public that surveillance is in operation and shall indicate a 24-hour contact number for NAIT Protective Services Security Operations Centre (SOC) in keeping with current Provincial Privacy Legislation.

**3.3 Monitoring and Recording.**

3.3.1 Cameras are monitored in the SOC, which is a secure area staffed 24 hours a day.

3.3.2 Images are recorded on secured servers and are viewable in the SOC by all NAIT Protective Services staff.

3.3.3 The cameras installed provide images that are of suitable quality for the specified purposes for which they are installed and all cameras are checked regularly by NAIT Protective Services to ensure that the images remain fit for purpose, the recording function is working and that the date and time stamp recorded on the images is accurate.

3.3.4 All images recorded by the surveillance system remain the property and copyright of NAIT.

**3.4 Retention of images.**

3.4.1 Unless required for evidential purposes, the investigation of an offence or as required by law, images will be retained for 30 days from the date of recording.

3.4.2 Where an image is required to be held more than the retention period referred to in 4.4.1, the Executive Director, Risk Management Services will be responsible for authorizing such a request.

3.4.3 Images held more than their retention period will be reviewed every 90 days and any not required for evidential purposes will be deleted.

3.4.4 Access to retained images is restricted to the Executive Director, Risk Management Services, and other persons as required and authorized by the Executive Director, Risk Management Services.

3.4.5 Average retention rates will be checked monthly and any reduction in average retention shall be reviewed to determine if additional storage is required to bring the average retention back to 30 days if/as determined by the Executive Director, Risk Management Services.

**3.5 Use of surveillance images.**

3.5.1 Access to recorded information is only permitted in accordance with this Procedure. Images may not under any circumstances be sold or used for commercial purposes or for the provision of entertainment.

3.5.2 In limited circumstances, it may be appropriate to disclose images to a third party, such as when a disclosure is required by law, including any administrative legal proceeding, in relation to the prevention or detection of crime, misconduct that results in disciplinary action or in other circumstances where the *FOIP* either requires or allows discretion to disclose personal information. Such disclosures will be made at the discretion of the Executive Director, Risk Management Services, and where necessary, following advice from the office of General Counsel Services.

3.5.3 Where a reasonable suspicion of employee misconduct arises and at the formal request in writing of the Director, Employee & Labour Relations, Human Resources, the Executive Director, Risk Management Services may provide access to images for use in staff disciplinary cases. These images will form part of the investigation and will be disposed of in accordance with NAIT's record retention policies and any applicable collective agreement.

3.5.4 Where a suspicion of student misconduct arises and at the formal request in writing of the Executive Director, Student Wellbeing and Community Administration, the Executive Director, Risk Management Services may provide access to images for use in student disciplinary cases. These images will form part of the investigation and will be disposed of in accordance with NAIT's record retention policies.

3.5.5 In the course of an investigation of an event that constitutes a criminal offence, and following consultation with the FOIP Coordinator, the Executive Director, Risk Management Services may make public the surveillance image of a suspect or person of interest for the purpose of identification.

3.5.6 A record of any disclosure made under this procedure will be held by the Executive Director, Risk Management Services itemizing the date, time, camera, requestor, authorizer and reason for the disclosure. The record will be retained for a period of three years following the disclosure.

3.5.7 The accepted process by which images from the system will be provided will be determined by the Executive Director, Risk Management Services, at the time of request or need. The most common method may include the extraction of single images from the video stream captured for physical reproduction and editing to remove any personal information not relevant to the subject matter in question. The extraction of a video clip from the recorded stream will be at the discretion of the Executive Director, Risk Management Services, as appropriate.

**3.6 Covert Cameras.**

3.6.1 The use of covert cameras will be restricted to exceptional circumstances when a series of criminal acts have taken place within a particular area that is not otherwise fitted with surveillance cameras. A request for the use of covert cameras will clearly state the purpose and reasons for use and the authority of the Executive Director, Risk Management Services, will be sought before the installation of any covert cameras. The Executive Director, Risk Management Services should be satisfied that all other physical methods of prevention have been exhausted prior to the use of covert cameras.

3.6.2 Covert recordings will only take place if informing the individual(s) concerned would seriously prejudice the reason for making the recording and where there are reasonable grounds to suspect that illegal or unauthorized activity is taking place. All such monitoring will be fully documented and will only take place for a limited and reasonable period.

**3.7 Body-worn cameras.**

3.7.1 Body-worn cameras may be used during NAIT Protective Services patrol duties. The downloading of images from such cameras will only be conducted by trained staff and cameras will be erased following each shift. NAIT Protective Services staff wearing body-worn cameras will disclose when approaching persons that they are being videoed and audio recorded.

**3.8 Applications for disclosure of images.**

3.8.1 Requests by individuals for images relating to themselves (data subject) should be submitted in writing to General Counsel Services with proof of identification. In order to locate the images on the surveillance system, enough detail must be provided by the data subject to allow the relevant images to be located and the data subject to be identified.

3.8.2 The accepted process by which images from the system will be provided will be determined by the Executive Director, Risk Management Services, at the time of the request or need. The most common method may include the extraction of single images from the video stream captured for physical reproduction and editing to remove any personal information not relevant to the subject matter in question. The extraction of a video clip from the recorded stream will be at the discretion of the Executive Director, Risk Management Services, as appropriate.

**3.9 Concerns and Complaints**

3.9.1 Any concern or complaint regarding a NAIT surveillance system is to be referred to the Executive Director, Risk Management Services.

3.9.2 All appeals of a decision of the Executive Director, Risk Management Services, regarding a NAIT surveillance system shall be made in writing to the Associate Vice President, Facilities Management & Development.

**3.10 Code of Practice.**

3.10.1 The Executive Director, Risk Management Services shall establish a Code of Practice for operators of the NAIT surveillance system which shall be reviewed annually with reference to the relevant legislation or guidance in effect at the time.

3.10.2 The Executive Director, Risk Management Services will audit the use and security of surveillance equipment. An audit report will be provided annually to the Associate Vice-President Facilities Management & Development and General Counsel.

**4.0 Exceptions to the Procedure**

4.1 Exceptions to this procedure must be documented and formally approved by the Policy Lead.

Procedure exceptions must include:

- The nature of the exception
- A reasonable explanation for why the procedure exception is required
- Confirmation that the exception aligns with the general principles
- Any risks created by the procedure exception and how they will be managed.

**5.0 Related Documentation**

5.1 CS 1.0 Campus Security Policy

5.2 Surveillance of Public Areas Code of Practice

***Document History***

| *Date* | *Action/ Change* |
|---|---|
| August 2, 2023 | Updated review date (5 years) and procedure owner |
| July 18, 2024 | Minor revisions to align positions to the Organizational Chart. |