# Video Surveillance on Campus Procedures

| | |
|---|---|
| **Document Number:** | #7-11-1P1 |
| **Related Policy:** | 7-11 Video Surveillance on Campus |
| **Effective Date:** | January 7, 2025 |
| **Approval Date:** | January 7, 2025 |
| **Supersedes:** | New |
| **Administrator Responsible:** | Vice President, Finance and College Services |
| **Associated Documents:** | |

## 1. Surveillance System Management

The Director, Facilities, Safety & Security is responsible for the installation, management and operation of NIC's surveillance system(s). This includes:

- Ensuring that the system complies with NIC policies and applicable law, including FOIPPA.
- Training all authorized personnel.
- Overseeing the security, retention and disposal of all recorded information.
- Managing the access and disclosure of any recorded information.
- Auditing and upgrading the system.

## 2. Privacy Impact Assessment

Following consultation with the Operations Team, the Director, Facilities, Safety & Security will conduct a privacy impact assessment (PIA), a step-by-step risk management and compliance review process used to identify and address potential information privacy and security issues, prior to the approval and installation of any new surveillance systems or cameras at NIC locations. The PIA must be approved by the Director responsible for FOIPPA and the Director, Facilities, Safety & Security.

## 3. Public Awareness of Surveillance

Signage will be posted to notify the public when they are entering a zone which is monitored by video surveillance equipment. Signage will include a URL or link to where the individual can access the following information:

- the purpose and legal authority for the collection of surveillance recordings;
- the intended use for the recordings; and
- the person(s) to contact if they have any questions about the collection, including the title and contact details for that person.

## 4. Access to Surveillance Systems and Data

Only authorized employees or contractors who have been authorized to do so will be able to operate the surveillance system and access recordings.

All personnel who are authorized to operate surveillance systems and access surveillance footage will receive regular training related to video surveillance and privacy.

Authorized employees may access recordings to facilitate or document an investigation or legal proceeding.

Real-time monitoring may be permitted by authorized employees or authorized security. The purpose of real-time monitoring is to identify problems that require immediate intervention and for the safety of the premises and people on the premises.

**5. Security and Retention of Surveillance Recordings**

All recordings of surveillance footage will be stored securely in compliance with FOIPPA.
Surveillance system recordings will be kept for 30 days, with the following exceptions:

- if it is needed to facilitate or document an investigation or legal proceeding, the recording may be retained for as long as required for that purpose; or,
- if it has been used to make a decision that directly affects an individual, the recording must be retained for at least one year after the date of that decision.

When retained recordings are no longer required, they must be securely destroyed.
The NIC Facilities department must maintain logs of all access, use, disclosure and destruction of surveillance system recordings.

**6. Access to and Disclosure of Recorded Information**

Access to recorded information is only permitted in accordance with this policy and with FOIPPA.
Access to recorded information is restricted to:

- authorized personnel as outlined in section 4 of these Procedures;
- those responsible for the administration of the college surveillance system;
- individuals seeking images or recordings in which they themselves appear, under FOIPPA;
- law enforcement agencies granted access to recorded images to assist in a specific investigation;
- or as required by law.

Requests from the public or College community for access to surveillance system recordings must be approved by the Director, Facilities, Safety & Security or the Vice President, Finance & College Services.

All disclosures of surveillance system recordings must be logged including time, date, appropriate approvals and overview of disclosure. Names of authorized parties disclosing recordings as well as third party viewers must be logged.

**7. Auditing and Oversight**

The Vice President Finance & College Services will oversee an audit on the video surveillance system at least annually, including cameras and storage systems, to determine whether any changes need to be made in the use or configuration of the systems and will review and update these Procedures as needed.

The audit will include the use and effectiveness of the video surveillance system and include details about any problems and privacy issues that have arisen. The report will also include the outcome of any self-assessment audit that has taken place.