C-42

CANADORE COLLEGE

OPERATIONAL POLICY MANUAL

TITLE: **Security Video Surveillance, Recording, and Storage Policy**

EFFECTIVE DATE: **November 9, 2020**

1. SCOPE

1.1. Authority

This policy is issued under the authority of the President.

1.2. Application

This policy applies to all employees, students, visitors, and contractors who would be on any campus location of Canadore College of Applied Arts and Technology (hereafter referred to as “Canadore” or “the College”).

2. PURPOSE AND PRINCIPLES

2.1. The Purpose of this policy is to ensure transparency to the intent and use of the surveillance security system used on the premises of Canadore College as well as to ensure compliance to the Municipal Freedom of Information and Protection of Privacy Act, R.S.O. 1990, c. M.56 (MIFIPPA).

2.2. This policy outlines the responsible use of the Video Surveillance System (the “System”), both overt and covert, as it is used for recording, monitoring and storing video on all properties owned or leased by Canadore College, as well as in service to, for the express purposes of enhancing safety and security of all persons and property, including preventing and deterring crime, evidence gathering, prevention of theft or vandalism, reduction of workplace safety related incidents, and assist with identification of intruders or those who have been trespassed from the properties owned or leased by Canadore College.

2.3. This policy describes the types of systems involved with the capture of video surveillance, storage database, and analytics employed to enhance the safety of individuals and the security of assets.

2.4. Any recorded data of an identifiable individual qualifies as "personal information" under MFIPPA. Security cameras will be used to collect personal information about identifiable individuals. The College has determined that it has the authority to collect this personal information in accordance with the MFIPPA. Pursuant to section 28(2) of the Ontario MFIPPA, the College deems it necessary and reasonable to ensure the safety and

security of its employees, students, and members of the public. In doing so the College will consider the necessity of the collection from the following aspects:

2.4.1. The means used to collect the personal information;
2.4.2. The sensitivity of the personal information; and
2.4.3. The amount of personal information collected.

3. POLICY

3.1. Video surveillance will be used only where it is demonstrably necessary for the purposes of enhancing the safety of persons, during workplace incident investigations, or for the deterrence of theft or destructive acts, such as vandalism and graffiti. This includes:

3.1.1. Outdoor campus areas consisting of fixed, Pan Tilt Zoom (PTZ) cameras, and Artificial Intelligence (AI) specialty cameras in parking lots, roadways, common areas, building perimeter, walkways, and areas in which vandalism or theft have occurred;

3.1.2. Indoor campus areas consisting of fixed and specialty AI cameras in hallways, labs, gyms, lounges, library, common areas, cafeteria, lounges, Admissions Office, high value areas such as server rooms, equipment rooms, finance, shipping and receiving, post production suites, computer areas, and areas in which vandalism or theft have occurred. Additional consideration will be applied for cameras installed in classrooms with justification as to the purpose and previous history for the area specified. Approval must be obtained from Organizational Development and Talent Management (Human Resources); Vice President, Academic; and Director of Campus Safety, Security, Environmental and Corporate Services; and

3.1.3. Residence areas consisting of fixed cameras in hallways, lounges, entryways, and parking lots.

3.2. Video surveillance will be used only by Campus Security or employees of Canadore College and Nipissing University authorized by the Director of Campus Safety, Security, Environmental and Corporate Services, and only where less intrusive means of deterrence, such as monitoring by Security Guards, is ineffective due to the size or nature of the area in question.

3.3. Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring other than on the campus grounds / parking lots in which a single sign at the entrances to the campus will be installed.

3.4. Security employees and video service provider(s) will have access to information collected through video surveillance only where necessary in the performance of their duties and in accordance with the provisions of this Policy. Every effort will be made to single source security equipment service providers while remaining within compliance of the College's financial policies.

3.5. Any private area in which the cameras have incidental access will be digitally blocked out to prevent either recording or live view into the area. This includes cameras which

have the ability to zoom through residence rooms, change rooms, or areas deemed private.

3.6. Employees and video service providers who may require access to information collected through video surveillance will be provided proper training and orientation with regards to this Policy and their obligations under this Policy and the Act, and will provide written acknowledgment that they have read and understood the contents of this Policy. Any employee who knowingly or deliberately breaches this Policy or the Act will be subject to discipline up to and including termination. Failure of a video service provider to comply with this Policy or the Act will constitute breach of contract and may result in termination of contract and legal action.

3.7. The recording medium must be handled in a manner that maintains the integrity and security of the recorded information.

3.8. All recorded information shall be overwritten with approximately three months history and no more than 6 months recording history. This will be controlled by the amount of digital memory installed on the Network Video Recorders (NVR).

3.9. Any information specifically awaiting review by law enforcement agencies, information seized as evidence, or information that has been duplicated for use by law enforcement agencies shall be completed according to the Act under conditions set forth in item 4.3.

3.10. Reception equipment locations and operation shall be limited to visual access of areas where there is no reasonable expectation of privacy. Video surveillance for the purpose of monitoring work areas, social areas, or sensitive areas will only occur in special circumstances, and must be consistent with this Policy's principle purpose, which includes the prevention/deterrence of illegal activity and the enhancement of safety.

3.11. When video surveillance footage is being displayed by authorized employees on a video monitor, the monitors will be in a position that cannot be viewed by others. A list of these areas will be maintained by security.

3.12. The video surveillance system will be subject to periodic audit.

4. <u>Types of Equipment</u>

4.1. Fixed cameras are used in indoor or outdoor areas and may have the capability of high definition or manual zoom.

4.2. Pan Tilt Zoom Cameras (PTZ) will only be located in outdoor areas and will have the capability of high definition zoom and panning.

4.3. Data storage devices or Network Video Recorders (NVR) will be located in the security office with a controlled access point permitting only those who have permission to gain access to the storage room.

4.4. Covert camera – hidden cameras will be used for investigative purposes in the event that a repeat offence is, or is likely, to be committed.

4.5. Software analytics used to monitor crowd size, behaviours, and predictive event modelling.

4.6. Artificial intelligence (AI) software systems to recognize facial or body features of individuals who have been trespassed from College properties, or have been identified as missing, or wanted in a BOLO circulation (Be On the Look Out for). Software may also be programmed to scan license plates for vehicles that are not permitted to be on premises.

4.7. During pandemic events while active screening is required during a restricted access process, the use of thermal imaging cameras to assist with active screening will be used. These cameras will be used to identify facial covering compliance as well as identify anyone with an elevated body temperature who may be at higher risk of illness transmission. A camera used to assist with entry protocols will be used for the purpose of combating illness transmission on campus. These cameras will be used rather than individual body temperature scanning instruments as consideration of privacy concerns that may arise during the access process.

5. Restrictions

5.1. Employees are prohibited from viewing video information for personal interest and, under no circumstances, will copy or transmit video information to anyone except as stated explicitly in this Policy.

5.2. Under no circumstances will cameras be directed through windows of any residential dwelling or any campus or non-campus locations where persons have a reasonable expectation of privacy.

5.3. No attempt will be made to alter any part of a recording. Proper evidence collection, release, and capture techniques are used to corroborate what is on the video especially if the video is captured on a separate recording device.

5.4. Thermal imaging will only be used for access processes with limited storage capabilities and decreased storage times to facilitate entry screening only. Images will not be stored longer than between 5 – 7 days.

6. Records and Access

6.1. Old storage devices will be wiped clean and rendered unserviceable before disposal. A written record describing the date, method and location of the disposal will be retained for seven years.

6.2. Where a review of recorded information indicates that unlawful activity has occurred or is suspected, law enforcement agencies will be informed who may view that recorded information. When a recording is seized as evidence, the name of the investigating officer and date and time of seizure will be recorded and retained in a case file, which will be retained for seven years.

6.3. Copies which are made of specific segments of recorded information for purposes of an official investigation will be dated and labeled with the police occurrence number, a case file is created, and access to these copies will be limited to authorized personnel.

Case files will be kept of all instances of access to, and use of, these stored copies, to provide for a proper audit trail.

6.4. These stored copies will be retained for at least one year as per section 5(1) of Ontario Regulation 460 under FIPPA. The length of this retention period may be reduced by way of formal resolution by the College or the courts.

6.5. Under the discretion of the Director of Campus Safety, Security, Environmental and Corporate services, access requests for reception equipment will be considered in accordance with the following criteria:

6.5.1. When requested by law enforcement, that a police occurrence number is obtained to confirm the recording will, or is likely to, be used in a court proceeding.

6.5.2. Other measures to protect public safety, detect or deter, or assist in the investigation of criminal activity have been considered and rejected as unworkable.

6.5.3. The use of each video surveillance camera should be justified on evidence-based criminal or safety concerns.

6.5.4. The video recorded must be vetted by the security officer copying the recording by watching and validating the video from both the NVR source and the recorded copy, and validating that they are consistent.

6.6. Security guards will only view recorded video information to monitor the premises, investigate an incident, when an emergency phone is activated or a call for service is received, when a safety hazard or imminent threat exists for a particular area, or as directed by the Security Manager or Director of Campus Safety, Security, Environmental and Corporate Services.

6.7. Security guards will be trained on pandemic access procedures and the limited use of thermal cameras.

7. ROLES AND RESPONSIBILITIES

7.1. The President is responsible for the overall management and operation of the College. The President will ensure that the policy is implemented and that compliance is monitored.

7.2. Security Guards, both full-time and part-time, are responsible to operate and monitor the video surveillance system(s) when and as directed to fulfill the requirements of their shift duties. Will be responsible for on-the-job training of the part-time staff who will access the video surveillance system with consistency to this standard.

7.3. The Security Lead Hand is responsible to manage and coordinate maintenance of the video surveillance system(s), train full-time employees who will access the system and ensure that the system is used in accordance with this Policy.

7.4. The Director of Campus Safety, Security, Environmental and Corporate Services is responsible for oversight of the system, especially with respect to privacy issues,

arranging periodic audits of the system, and recommending new video installations and system upgrades through the budget process.

8. EVALUATION

This policy will be evaluated every 3 years

9. REFERENCES

- Information and Privacy Commissioner of Ontario – Guidelines for Use of Surveillance Video 2015
- A Guide to the Personal Information Protection and Electronic Documents Act, 2018 Edition, Timothy M. Banks
- Canadian Privacy, Data Protection Law and Policy for the Practitioner, Kris Klein, Second Edition