VIDEO SURVEILLANCE & RECORDING POLICY

PURPOSE

The purpose of this Policy is to outline the responsible use of Video Surveillance System (the "System") as it is used for recording, monitoring and storing video on all properties owned or leased by Brock University (the "University") for the express purposes of enhancing safety and security of all persons and property, including preventing and deterring crime, identifying suspects, and gathering evidence.

SCOPE

This policy applies to all employees, agents and volunteers of Brock University, including any individual or entity permitted to use or have access to the System, in the use and installation of video recording and surveillance technology. Use of video surveillance technology for research purposes is not covered by this Policy. This Policy applies to all University owned or leased land and buildings ("University Premises").

POLICY STATEMENT

The University recognizes the need for synergies between an individual's right to privacy and the University's duty to promote and maintain a safe and secure environment. The use of closed circuit television surveillance systems ("CCTV") results in the collection of personal information in the form of images (both still and live) of individuals and conduct.

The University will only permit the use of CCTV for the purpose of safety and security of persons and property. CCTV systems will only be used by the University to:

a) provide a record of unlawful acts and breaches of University policies, such as the various Codes of Conduct;
b) prevent or deter such activities; and
c) aid in the investigation of such breaches.

General Information

1. Brock University Campus Security Services (CSS) has the primary responsibility for crime prevention, law enforcement, and other public safety and security matters on University Premises. CSS is committed to enhancing its public safety efforts through the use of digital video recording and/or surveillance under appropriate circumstances.

2. All existing uses of video recording and surveillance will be brought into compliance with this Policy. All departments with existing equipment must work with CSS to integrate their CCTV systems with the CSS standard with the exception of approved research initiatives.

Responsibilities

1. CSS is the only department authorized to oversee and coordinate the use of video recording for safety and security purposes at the University. All University employees using video recording are responsible for complying with this Policy in their respective operations. CSS has primary responsibility for disseminating the Policy and assisting other units in implementing the Policy and procedures.
2. Employees wishing to install a system or to monitor (live view only) a system shall make a request to the Director, Campus Security Services (or designate) at which time the request will be reviewed and approved based on leading practices and this Policy. In deciding whether to approve the request, CSS will consider the reasonable privacy expectations of individuals who may work, use or otherwise occupy the space, which is the subject of the request, as well as the nature of the space under observation, the closeness of the proposed surveillance and reasonable safety and security risks.
3. Any academic or administrative unit of the University with cameras installed in their respective area(s) will be permitted viewer access to recorded images in real-time, only. CSS will limit access to members of the unit who have a need to know the information for the purposes of their employment duties. The ability to provide access to any recorded image or to reproduce any recorded image shall rest solely with CSS, which shall grant access only in accordance with the University's Access to Information and Protection of Privacy Policy.
4. The University will make every effort to position cameras so that they only cover University Premises; CCTV cameras may be installed in public areas, such as hallways, common areas, parking lots and walkways where there is a concern for the safety or security of persons or property. If there is a concern that the CCTV will record spaces which have not been identified as requiring video surveillance, CSS will consider ways to minimize the amount of personal information recorded by the cameras, including but not limited to, blacking out parts of the camera's view, limiting

the number of cameras, or restricting the operation of the video surveillance equipment.

5. Video surveillance and recording for the purpose of monitoring work areas or sensitive areas should only occur in special circumstances where approved by the Director, Campus Security Services (or designate) and Vice-President, Administration.

In addition, where the surveillance footage is recorded, the location must be accompanied by clearly visible signage which provides faculty, staff, students and members of the public with advance notice that video surveillance is being used in the area. This may include facility or public space entrances. Notices should provide a graphical depiction of a video camera and who to contact for further information.

Monitoring

Personnel involved in monitoring will be appropriately trained and supervised in the lawful and responsible use of this technology by the Department's management staff. If the equipment is in any way adjustable by the operators, these capabilities will be restricted to the extent possible to prevent adjustments, zooming in or other manipulations of the equipment.

Securing and Retaining Images

1. Video recordings shall be maintained in a secure environment by CSS and at no time will attempts be made to alter any part of a recording.
2. Recordings that are not viewed will be retained for a period of no more than 180-days.
3. Recording will be disposed of in such a way that personal information cannot be reconstructed or retrieved.
4. Recordings viewed for any purpose will be retained for a minimum period of one year from completion of use.
5. Where the recording forms part of the evidence in court or tribunal proceedings, recordings will be kept for a minimum of one year following final disposition of the matter including any court reviews and appeals.
6. All access to and use of recordings will be done in accordance with CSS Video Surveillance Procedures.
7. Keep auditable logs of all accesses, uses and disclosures of video footage.

Disclosure of Video Recordings

Video recordings will not be disclosed to anyone other than Security Services personnel except in accordance with the University's Access to Information and Protection of Privacy Policy. For example:

- When it is required by law;
- When disclosure is to a law enforcement agency for law enforcement investigations or proceedings;
- When it is required by a University employee who needs it to perform their duties and the disclosure is necessary and proper in the discharge of the University's functions – e.g. use at a formal University proceeding such as a Student Code of Conduct hearing;
- When disclosure is necessary to comply with a Freedom of Information request by the individual whose identity has been recorded in the CCTV footage;
- In compelling circumstances, involving an individual's health or safety;
- In exceptional cases, to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident.

DEFINITIONS

Reception Equipment refers to the equipment or device used to receive and/or record the recorded information collected through a video surveillance system.

Record, means any record of information, however recorded, which may include, but not limited to in printed form, or by electronic means.

Storage Device refers to a computer disk or other device used to store the recorded data or other images captured by the system.

Video Surveillance System refers to a video surveillance system that enables continuous or periodic recording, observing or monitoring of persons and facilities on the University property.

COMPLIANCE AND REPORTING

CSS will ensure compliance with this Policy through employee training and periodic security assessments. Non-compliance of this Policy by departments or individuals shall be reported to

the Director, Campus Security Services (or designate) who will review the case and determine the appropriate resolution.

Policy owner:	Donna Moody, Director, Campus Security Services
Authorized by:	Board of Trustees
Accepted by:	Senior Administrative Council
Effective date:	November 2018
Next review:	November 2021
Revision history:	Version 2
Related documents:	1. *Freedom of Information and Protection of Privacy Act ("FIPPA")* 2. *Ontario Information and Privacy Commissioner's Guidelines for the Use of Video Surveillance*