EXECUTIVE SUMMARY

INTRODUCTION:

The Office of the Chief Risk Officer works collaboratively with the Memorial University community to provide a safe, secure and healthy environment with a managed, proactive approach to risk through engagement and education that supports teaching, learning, living and working on campus. Accordingly, the university uses security cameras to monitor public areas in order to deter crime and assist CEP and law enforcement in maximizing the safety of individuals and property that are part of the university community. Any diversion of Memorial CEP technology for purposes other than those listed herein would undermine the acceptability of these resources for critical safety goals and is therefore strictly prohibited.

PURPOSE:

The purpose of these guidelines is to outline the responsible use and design of a Video Monitoring System (the "system") as it is used for recording, monitoring and storing video on all properties owned or leased by Memorial University (the "university") for the express purposes of enhancing safety of all persons and property, including preventing and deterring crime, identifying suspects, and gathering evidence.

The purpose of video monitoring at the university to:

- Promote a safe environment for the university community and the security of assets and property by deterring criminal acts and mischief;
- Summon emergency assistance or deploy security resources;
- Help first responders (i.e. police, fire and paramedic vehicles) navigate across campus;
- Verify alarms and door access control systems; and
- Assist law enforcement in investigations and prosecutions of criminal activity, including identifying suspects and potential witnesses.

Video monitoring for Memorial CEP purposes will be conducted in a professional, ethical and legal manner. Personnel involved in active video monitoring will be appropriately trained in the responsible use of this technology.

SCOPE:

These guidelines have been developed by the Office of the Chief Risk officer and Campus Enforcement and Patrol to ensure that it collects, uses, discloses, retains and disposes of personal information in compliance with the Access to Information and Protection of Privacy Act (ATIPPA) and to ensure that the Department balances the protection of individuals and assets with the protection of privacy. These guidelines complement and build on the policies outlined by Memorial University's Information Access and Privacy Office and The Office of the Information and Privacy Commissioner Guidelines for the Video Surveillance by Public Bodies in Newfoundland and Labrador (2015).

Who should use these Guidelines?

This guideline only applies to areas of the St. John's campus that are monitored by the St. John's unit of Campus Enforcement and Patrol and does not apply to Memorial's Recreation Complex, the Grenfell Campus, Marine Institute or the Harlow campuses.

These guidelines **do not apply** to video camera usage for the following purposes:

1. *Academic Use*. This standard does not apply to legitimate academic use of video cameras for educational purposes.

2. *Research Use*. This standard does not apply to video cameras or video data collected for research purposes.

3. *Private Video Cameras*. This standard does not apply to private video cameras owned and operated by members of the campus community.

4. *Law Enforcement Surveillance*. This standard does not apply to cameras used covertly by law enforcement for criminal surveillance.

5. *Unrelated to Safety and Security Monitoring:* This guideline does not apply to video cameras specifically used or established for reasons unrelated to the safety and security and installed outside CEP video monitoring system.

Any video recording devices that are introduced on campus should be reviewed by the Office of the Chief Risk Officer.

DEFINITIONS:

CEP: Campus Enforcement and Patrol

Application Administrators: responsible for the coordination and administration of the VMS on and are comprised of representatives from the OCRO, Technical Services and Information Technology Services. Application administrations are responsible for the functioning and maintenance of the VMS and all its associated hardware.

Public Area: An open or common area where the expectation of privacy is not violated by what could normally be observed, such as the campus grounds, hallways, common areas, circulation spaces, classrooms, libraries, retail spaces, study rooms, or computer labs..

Private Area: An interior, closed-off area where there is an expectation of privacy. This includes the interior of student residence space and areas where an individual might change clothing, such as bathrooms, shower areas, locker and changing rooms. This would also typically include private office spaces; however, exceptions are appropriate in areas where monetary transactions occur or where the use of CCTV is needed to safeguard money or supplies from theft, destruction or tampering.

Video Management System (VMS): An application comprised of hardware and software for the purposes of viewing, recording, storing, and/or analyzing CCTV video, and/or controlling CCTV system cameras.

Video Monitoring System / Technology: Any item, system, camera, technology device, communications device, software, or process, used along or in conjunction with a network, for the purpose of gathering, monitoring, recording, or storing an image or images of facilities and/or people. Images captured by video monitoring technology may be real-time or preserved for review at a later date.

SECTION 1: CAMERA PLACEMENT AND DEFINING NECESSITY

The quantity and specific placement of CCTV cameras will vary with each project, and will depend on pre-determined considerations, including:

1. Area of concern / interest: in the placement of each camera, this is the first and fundamental consideration, i.e. what specifically is to be viewed or recorded.

2. Camera function: Recognition vs. identification – is the intended function of a camera to identify the presence of a person, vs. the ability to recognize a face. In general, it is the intention/requirement of the Memorial University to identify the presence of a person or persons, **facial recognition software is not to be used on campus in relation the security cameras.**

3. Level of risk: CEP: in most cases, a minimal number of cameras may be required to cover points of entry or similar. However, in other cases, additional cameras may be required – areas of higher risk (i.e. where money and/or valuable assets are present).

4. Access / Serviceability: For future maintenance and access to cameras, placement of each shall take into consideration the ease of future access.

5. Audio Recording: If present, all audio recording functions are to be completely disabled both at the camera and the video management system software. Audio recording devices on CCTV cameras is prohibited on campus. Audio recording is NOT permitted for security purposed on campus.

In consultation with CEP, the following are intended to provide a minimum coverage of high risk areas. The placement and field of view (FoV) of each camera is decided so that it will least impact privacy of building occupants.

1. *Public Areas*: Except where approved by CEP, camera placement shall generally be restricted to public areas and areas commonly used by university community groups. These include, but are not limited to, the following:

    a. Hallways and common/circulation areas
    b. Points of entry/exit (i.e. public entrances)
    c. Elevator lobbies
    d. Retail areas, including vending machines and similar
    e. Areas where money is handled (cash handling, ATMs, and similar)
    f. Dining facilities
    g. Laboratories (special circumstances/requirements only)
    h. Library interiors
    i. Building exteriors – points of entry/exit – cameras typically mounted at roof level or high on exterior walls

j. Loading docks/shipping and receiving areas (interior and exterior as applicable)
k. Sidewalks, and other pedestrian walkways
l. Parking areas (surface and underground), including points of entry/exit, and pay points

2. *Private Areas*: Subject to direction / approval by the Chief Risk Officer, video monitoring is limited to those areas where individuals would not have a reasonable expectation of privacy. Video monitoring shall **not** be approved in the following locations:

    a. Residence or similar – living spaces
    b. Public restrooms – toilet stalls / urinals
    c. Locker / changing spaces (where showering or disrobing is routine)
    d. Individual offices (exceptions to include with occupant's permission, and if the space is subject to exceptions such as handling money, documents or supplies).

3. *Residential Housing*: CEP shall ensure that camera positions and views of residential housing (both on and off campus) are limited, and that any such views are no better than what is available with unaided vision. Furthermore, the view of a residential housing facility must not violate the reasonable expectation of privacy in that area.

4. . Security cameras will not be positioned to look through windows or adjacent property, or those areas will be blocked from view or blacked out. If video surveillance cameras are adjustable, these capabilities will be restricted, to the extent possible, so that operators cannot monitor unintended areas. Where the placement of a camera may impact privacy, data masking will be used to block recording in areas where privacy cannot be maintained

SECTION 2: NOTICE OF COLLECTION

Notice of collection of personal information will be provided on the Department's website. The following information will be easily accessible:

1. The legal authority for the collection of personal information;

2. The principle purpose(s) for which the personal information is intended to be used; and

3. The title, business address and business telephone number of a public official who can answer questions about the collection of personal information.

The Department will prominently display signs at the perimeter of monitored areas and at key locations within the areas to provide notice that video monitoring is, or may be, in operation. Appropriate signs and notice of video monitoring must be posted in areas subject to video monitoring. At minimum, signs will be posted at the entrance doors of buildings and the parameter of campus. This is to notify people entering that there is recording in place. All signage must have the web address to access more information about the video monitoring at the University and these guidelines.

Examples of sign templates can be found in Appendix A

SECTION 3: DISCLOSURE AND ACCESS TO RECORDS

Because community members may be present on campus 24 hours a day, video recording systems may operate at any time in a 24-hour period. All video monitoring equipment will be in a secure, access-controlled area with restricted access.

Access to and Review of (Historic) Recordings

The review of camera recordings will only be completed by CEP when investigating an allegation of a criminal offence, policy / code breach or safety concern.

To further their investigation, CEP may allow others to review specific recordings in an attempt to identify people and understand activities;

CCTV recordings will only be available for viewing and monitoring by CEP. In the event of an investigation, CEP will review any footage and provide a summary report of the video contents to the interested parties.

The dispatch center will monitor live streaming of CCTV cameras unsystematically as part of their job duties.

Any information obtained through CCTV systems may only be used for purposes of assisting in the identification of individuals who commit a crime or who have been identified as a risk to the university community; and to assist law enforcement in the investigation of any crime. The following controls shall be in place for the protection of the live stream of video footage.

1) Access based permissions for user accounts.
2) Restricted access to areas that house monitors streaming live video.
3) The university will not use video cameras to monitor employee or student performance;
4) An individual's or a group's behavior may warrant monitoring with safety in mind. However, the university will not selectively monitor people in a discriminatory way based on the Human Rights Act protected grounds (e.g. age, ancestry, citizenship, colour, creed, disability, ethnic origin, family status, gender identity, gender expression, sex, and sexual orientation, and marital status, place of origin or race).
5) The review of camera recordings will only be completed by CEP Management, trained dispatchers and supervisors when investigating an allegation of a criminal offence, policy breach or safety concern
6) Viewing of the recorded and live video stream information will be limited to the following authorized university personnel:
    a) Campus Enforcement Dispatchers
    b) CEP Corporals
    c) Application Administrator
    d) Manager, Campus Enforcement Patrol
    e) Assistant Manager, CEP
    f) Director, Campus Enforcement Patrol

g) Chief Risk Officer

h) Other university personnel under exceptional circumstances which is directly relevant to an investigation, as approved by the Chief Risk Officer based on legal and legislative requirements.

Disclosure of Information

Any information obtained through CCTV systems will be considered confidential and will only be disclosed in accordance with ATIPPA 2015 and in the following circumstances:

- When disclosure is to a law enforcement agency for law enforcement investigations or proceedings;
- When disclosure is necessary to comply with an ATIPPA request by the individual whose identity has been recorded in the CCTV footage. Any such request would be managed by the Information Access and Privacy Office:
- To employees who need access to perform their duties and where access is necessary and proper in the discharge of the University's functions; and
- In exceptional circumstances, involving an individual's health or safety.

Procedure for Disclosure:

Release of Information from the video management system must be approved by the Chief Risk Officer (or designate).
The release request will include:

1) The case occurrence number;
2) The name, contact information and badge number of the investigating officer; and
3) A description of the requested information.

If access is authorized, then the following will be logged on the Release of Information form:

4. The date of release;
5. The name of the Director of Campus Enforcement or designate who authorized disclosure;
6. The name of the Department staff member who released the record; and
7. The name and badge number of the officer that disclosure was made to. Copies of records for purposes of a criminal investigation will be dated and labelled with a unique, sequential number or other verifiable symbol.

To maintain a proper audit trail, logs will be kept of all instances of access to these copies.

SECTION 4: PRIVACY ATIPPA (Access to Information and Protection of Privacy).

The university recognizes the need to strike a balance between the individual's right to be free from invasion of privacy and the institution's duty to promote a safe environment for all community members. In light of this recognition, the university will use CCTV to enhance safety and the quality of life of the campus community by integrating the best practices of electronic security and CEP with state-of-the-art technology. CCTV technology will extend the protection of the university.

The university is authorized to collect personal information using this Camera System under section 61(c) of the Newfoundland and Labrador Access to Information and Protection of Privacy Act (ATIPPA), i.e. the information relates directly to and is necessary for an operational program or activity of the university. The university is authorized to use this personal information under section 66 of ATIPPA, i.e. for one of the purposes set out in these guidelines, or for a use consistent with one of those purposes. Disclosure of any video recording will also be in full compliance section 68 of ATIPPA.

To request information, individuals can refer to Memorial's Information Requests policy.

SECTION 5: RETENTION AND DISPOSAL OF RECORDS

All video records are recorded on VMS storage, where it will be retained for a maximum of thirty (30) days at full image quality, subject to limitations on storage capacity and other factors. A second (N+1) storage archiver has been deployed as a failover for system redundancy and will follow the same retention schedule. .

Used video images (i.e., those viewed for incident-driven, law enforcement purposes) for a maximum of one year;

Only retain unused images for a maximum of 72 hours (overwriting unused footage every 15 hours);

In the event of an incident investigation, exported video may be kept in accordance with the retention schedule for the incident file and will fall under the information retention schedule for incident reporting.

SECTION 6: COMPLIANCE AND CONTINUOUS IMPROVEMENT

Compliance with these guidelines is the responsibility of all individuals considering the use of video monitoring technology on Memorial's owned and leased property and sites. The OCRO will periodically undertake a risk-based, self-assessment audit to ensure adherence to these guidelines, and will also review and update these guidelines as needed. Any suggestions for improvements to the guidelines are welcome and should be sent by email to OCRO@mun.ca for consideration.

Appendix A : Signage

4”x4” Door decals

10.5”x14.5” Larger Exterior Signs