Closed Circuit Television Protocol
# TABLE OF CONTENTS

1.0 **PURPOSE** ................................................................. Page 1

2.0 **SCOPE** ........................................................................ Page 1

3.0 **DEFINITIONS** ............................................................ Page 1

4.0 **PROTOCOL**

4.1 Use of CCTV ................................................................. Page 2
4.2 CCTV Monitoring ........................................................... Page 3
4.3 Use and Distribution of Recorded Images ....................... Page 4

5.0 **RESPONSIBILITIES** .................................................. Page 5

6.0 **REFERENCES** ............................................................ Page 6

7.0 **PROTOCOL HISTORY** .............................................. Page 6
1.0 PURPOSE

1.1 McGill University Security Services employs closed circuit television (CCTV) cameras in public areas for the purposes of safety and security of the McGill community and for the protection of University property. The goal of this protocol is to outline how CCTV shall be used so that it complies with all existing federal and provincial laws and is consistent with its stated purpose.

2.0 SCOPE

2.1 The protocol set out in this document applies to all members of the McGill Community, schools and centers of McGill University in the use of CCTV monitoring and recording.

2.2 Video monitoring for the following purposes is not subject to the provisions set out in this document:

2.2.1 where it is being used as part of the teaching or research responsibilities of a member of the academic staff of the University;

2.2.2 where it is being used for video conferencing; and

2.2.3 where it is used by Parking Services to assist customers at gates and pay stations.

3.0 DEFINITIONS

3.1 Access Act - refers to R.S.Q., chapter A-2.1, An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information, which generally declares confidential the records, documents and information concerning staff and students. The use of CCTV is subject to this Act.

3.2 CCTV [closed circuit television] is a generic term used to describe a variety of video surveillance technologies. More specifically, CCTV refers to a system in which one or more video cameras are connected in a closed circuit or loop, with the images produced being sent to a central television monitor or recorded. As used in this document, the term CCTV applies only to video monitoring and recording. The electronic interception and/or recording of audio are generally much more legally restrictive and are outside the scope of this document.
3.3 Covert CCTV Equipment – A camera is covert when it is hidden from normal view or otherwise secreted away, and at least one of the individuals to be recorded has a reasonable expectation of privacy.

3.4 McGill Community – refers to McGill faculty, staff, students, contract employees, visitors or any other person on University property.

3.5 Overt CCTV Equipment – A camera is overt when it is not hidden from general view, regardless of whether or not an individual actually sees the monitoring device or knows of its existence. Examples of overt surveillance devices include:

3.5.1 CCTV mounted in hallways, parking lots, waiting rooms, etc.; and

3.5.2 CCTV equipment mounted in a patrol car.

4.0 PROTOCOL

4.1 Use of CCTV

4.1.1 McGill University Security Services administers the University’s central security system, which includes the security camera network. As such, it is the only University unit authorized to implement, oversee and coordinate the use of video recording for safety and security purposes at the University. The procurement and installation of video cameras and monitoring equipment is strictly controlled and all installations must be approved by Security Services in accordance with the Security Device Installation Protocol.

4.1.2 McGill University Security Services utilizes closed circuit television (CCTV) to enhance personal safety, deter and investigate crime, and protect University property. The use of CCTV will be conducted in manner compliant with all existing federal and provincial laws and consistent with the values of the University so as to minimize the intrusion of the privacy of faculty, staff, students, and visitors in their personal and professional activities. It will be used for legitimate safety and security purposes only, which include but are not limited to the following:

i. monitoring building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, and laboratories;

ii. monitoring streets, sidewalks, parking lots, courtyards, and intersections;
iii. monitoring restricted access transactions at entrances to buildings and other areas;
iv. monitoring locations protected by intrusion alarms, exit door controls, security tabs, panic and hold-up alarms;
v. monitoring ATM stations and other areas where funds are exchanged such as a business office, campus store, and other cashier locations;
vi. monitoring public areas using CCTV as a patrol technique;
vii. reviewing recorded images as part of a criminal or security breach investigation; and
viii. conducting surveillance for areas prone to on-going criminal activity.

4.1.3 Public area video monitoring will be conducted only in areas where the public does not have a reasonable expectation of privacy. Cameras will not be directed at private locations, such as a home, residential apartment windows, shower rooms, toilet stalls or locker rooms.

4.1.4 Hidden or covert cameras will not to be installed unless there is a demonstrated need to assist authorities in collecting evidence in a criminal investigation. Such installations will be authorized only by the Associate Director, University Safety (Security Services) or the Security Services Operations Manager acting in his/her stead. Any exception to this article must also be approved similarly.

4.1.5 CCTV shall not be utilized to monitor employee or student performance except where employee or student conduct constitutes criminal behaviour or negligent behaviour where it places others at risk.

4.1.6 Security Services shall ensure that members of the University community are aware of the presence and purpose of CCTV systems through appropriate signage and information on the department’s website.

4.2 CCTV Monitoring

4.2.1 The monitoring of CCTV systems by Security Services shall be conducted in a professional, ethical, and legal manner, and in accordance with all University policies. Personnel involved in video monitoring shall be appropriately trained and continuously supervised in the responsible use of this technology.

4.2.2 Personnel who monitor cameras must receive a copy of this document and the procedures developed under it and provide written acknowledgment that they have read and understood their contents.
4.2.3 Violations of the established procedures for video monitoring referenced in this document will result in disciplinary action.

4.2.4 Where appropriate, Security Services may award live viewing rights to other University personnel where it serves to enhance the safety and security of the local area. These individuals will be subject to the same standards of training and conduct as Security Services personnel. Violations of the established procedures for video monitoring referenced in this document will result in having their viewing rights revoked. Examples of personnel who may be awarded live viewing rights include, but are not limited to:

i. building directors;

ii. front desk staff of residences; and

iii. supervisors of areas with customer service counters;

4.3 Use and Distribution of Recorded Images

4.3.1 Security Services is responsible for ensuring that access to recorded images is severely restricted and the secure storage of data recordings is consistent with University policies and procedures concerning data protection and records management. Recorded images are kept for a limited period of time (usually thirty days) before they are recorded over.

4.3.2 The use of recorded images to conduct investigations of possible misconduct or illegal activity is limited to Security Services personnel or persons authorized by Security Services.

4.3.3 Network and Communication Services personnel are permitted to view recorded images only for the purposes of repair and maintenance to the CCTV network.

4.3.4 Security Services will provide information, including any surveillance camera recordings to le Service de police de la Ville de Montréal (SPVM), or other law enforcement agencies as required for the purpose of investigation of an offence.

4.3.5 Requests from members of the McGill community or from representatives of outside agencies to view or receive recorded footage will be approved on a case-by-case basis. Situations where such approval may be provided include, but are not limited to:

i. University disciplinary officers in cases of student discipline where Article 4.1.5 of this document applies;
ii. The Department of Human Resources in cases of employee discipline or arbitration hearings where Article 4.1.5 of this document applies;

iii. Risk Management or Legal Services to defend against claims and lawsuits;

iv. employees or students wishing to use video to prove their innocence in legal or campus judicial proceedings where Article 4.1.5 of this document applies; and

v. McGill community members who were victims of crimes.

4.3.6 Nothing in Article 4.3.5 is designed to contravene the Access Act, which stipulates that a person is entitled to access to the information concerning him/her, including access to recordings made of him/her. Nonetheless, the Access Act does specify restrictions to the right of access, and any denial of access shall be in accordance with those specifications.

4.3.7 Any request for video footage from an individual or agency for purposes not addressed in Articles 4.3.4, 4.3.5 or 4.3.6 will require a search warrant or subpoena.

4.3.8 Requests to view or receive recorded images under Articles 4.3.5 and 4.3.6 will be submitted in writing that clearly identifies the reason for the request. Authorization to release recorded video footage or to permit viewing thereof is restricted to the following personnel:

i. the Security Services supervisor responsible for investigations;

ii. the Operations Administrator - Statistical Analysis & Prevention, when replacing the Security Services supervisor responsible for investigations;

iii. the Security Services supervisor responsible for the University’s CCTV network;

iv. the Associate Director of University Safety (Security Services); and

v. the Security Services Operations Manager, when replacing the Associate Director of University Safety (Security Services);

5.0 RESPONSIBILITIES

5.1 McGill University Security Services shall be responsible for the application and administration of this protocol.
5.2 McGill University Security Services shall develop procedures that will govern the approval, installation, operation and management of video monitoring equipment, and for the proper training of University staff using such equipment. The procedures shall be consistent with the provisions of this document.

6.0 REFERENCES

6.1 La Commission d'accès à l'information du Québec, Rules for use of surveillance cameras with recording in public places by public bodies (June 2004).


7.0 HISTORY

Amended:
22 July 2013 – Modified the document format to incorporate the new McGill Security Services logo; added a history section to the document to track changes.

Amended:
04 October 2012 – Added definition of Access Act and the McGill Community; stipulated that recorded images are retained for a limited period of time (usually 30 days); specified how Access Act applies.

Effective:
23 April 2010