McMaster University

Administration Policy

Complete Policy Title: Closed Circuit Television Surveillance Policy	Policy Number:
Approved by: President	Date of Most Recent Approval: January 21, 2013
Date of Original Approval: January 21, 2013	Supersedes/Amends Policy dated: n/a
Responsible Executive: Terry Sullivan, Director Security	Enquiries: University Secretariat
DISCLAIMER: *If there is a discrepancy between this electronic policy and the written copy held by the policy owner, the written copy prevails.*	

1 Introduction

1.1 McMaster University (the "University") recognizes the need to strike a balance between the individual's right to privacy and the University's duty to promote and maintain a safe and secure environment for students, staff, faculty and visitors.

1.2 The use of closed circuit television surveillance systems ("CCTV") results in the collection of personal information in the form of images and records of the conduct of individuals.

1.3 CCTV systems are employed by the University to record unlawful conduct and breaches of relevant University policies, such as the various Codes of Conduct as well as to prevent and to deter such conduct. Information obtained from CCTV systems is also used as an aid in the investigation of such conduct.

1.4 The University's installation, monitoring and recording of CCTV systems is in accordance with this policy, the *Freedom of Information and Protection of Privacy Act* ("*FIPPA*"), and other applicable Federal legislation and related University policies.

2 Purpose

2.1 The purpose of this policy is to regulate CCTV installations, monitoring and recording on all properties owned or occupied by the University and its affiliates.

2.2 Enhance public safety in areas where the safety and security of the university community may be at risk.

2.3 Prevent and deter crime, thereby reducing the cost and impact of crime to the community.

2.4 Protection of individuals, including students, faculty, staff and visitors.

2.5 Protection of University owned and/or operated property and buildings, including building perimeters, entrances and exits, lobbies and corridors, receiving docks, special storage areas, laboratories and cashier locations.

2.6 Reduce the fear of crime.

2.7 Identify criminal activity and dangerous events.

2.8 Identify suspects and assist in investigations and prosecutions.

2.9 Improve the allocation and deployment of security resources.

2.10 Verification of alarms and access control systems.

2.11 Monitor parking lots, including access and egress control.

2.12 Ensure that all installation and CCTV equipment meets University standards as prescribed by the Technology Administrator.

3 Scope

3.1 This program applies to all CCTV camera monitoring and camera recordings with the exception of CCTV cameras for instructional and research purposes.

3.2 For the purpose of this policy, the University environment includes all University land and buildings both on the main campus and any off site and satellite locations that are occupied in full or part by the University. This includes rented or leased properties occupied by McMaster University.

3.3 For the purpose of this policy, the University environment also includes those areas occupied by Colleges and businesses on properties owned by the University.

3.4 The existence of this policy does not imply or guarantee that CCTV systems will be monitored in real time.

3.5 All existing uses of video monitoring and recordings shall be brought into compliance with this policy within 12 months of the approval of this policy.

4 Definitions

4.1 **CCTV** – closed circuit television.

4.2 **Camera** – a device that converts images into electrical signals for television transmission, video recording, or digital storage.

4.3 **Covert** – concealed; hidden.

4.4 **Designated Managers** – managers who have been designated by the Director of Security Services to view proprietary CCTV systems.

4.5 **Monitoring** – having access to view live video footage.

4.6 **Overt** – Open and observable; not hidden, concealed, or secret.

4.7 **Proprietary CCTV Systems** – systems installed by the Faculty of Health Sciences, Hospitality Services, Housing and Conference Services, McMaster

Libraries, and the McMaster University Student Centre Administration prior to this policy being approved.

4.8 **Technology Administrator** - a McMaster University employee identified to administer and manage security technologies for the McMaster campus.

5 Responsibilities

5.1 McMaster University Security Services is responsible for McMaster University's CCTV program, including ensuring proprietary CCTV systems comply with the terms and conditions of the policy.

5.2 Security Services will:

a Monitor all CCTV cameras and maintain a suitable monitoring station in a controlled, high-security area with access restricted to Security Services.

b Ensure that all recordings are kept in a locked receptacle located in a controlled-access area. Each storage device that has been used will be dated and labeled with a unique, sequential number or other verifiable symbol.

c Ensure that the implementation and operation of all CCTV Systems comply with this policy.

d Ensure that appropriate signage is in place at all entrances to the University advising of the use of CCTV cameras and providing contact information for the person responsible for the program.

e In cooperation with the Technology Administrator, conduct a documented operational audit of the CCTV program annually.

f Ensure all personnel monitoring the CCTV cameras are appropriately trained and supervised in the responsible use of cameras and recording equipment.

g Manage the secure storage and tracking of all images including copied data recordings required for investigative/or evidence purposes.

h Be responsible for the management and administration of the University CCTV systems, reporting annually to the Vice-President (Administration).

i Be responsible for the disclosure of all images.

5.3 The Technology Administrator will:

a Install systems only under the guidance of Security Services.

b Ensure all CCTV cameras are recording all monitored activity.

c Ensure the safe and secure storage of all CCTV recordings.

d Conduct a documented operational audit of the CCTV program annually in cooperation with Security Services.

e Ensure that cameras are electronically restricted from focusing through windows of a residential dwelling (including a University residence) or any non-University location where an individual has a reasonable expectation of privacy.

f Provide a copy of all recordings when requested by McMaster Security Services to aid in an investigation.

g Ensure that all persons who access records log all activities relating to such access, including the time and purpose, and that a log book will be maintained for this purpose.

h Ensure that all persons who are involved in the installation, servicing, monitoring and recording of CCTV systems have signed an agreement regarding their duties and responsibilities under this policy and FIPPA, including an undertaking that they will maintain confidentiality, both during and after their relationship with the University ends ("Confidentiality Agreement").

i Take all reasonable efforts to ensure the security of records in his/her control or custody and ensure their safe and secure disposal. Old storage devices will be disposed of in accordance with the applicable technology asset disposal processes, ensuring personal information is erased prior to disposal and cannot be retrieved or reconstructed. Disposal methods may include shredding, burning, or erasing depending on the type of storage device.

6 Policy

6.1 Installation

a Departments wishing to install CCTV systems or to monitor CCTV systems shall make a request to the Director of Security Services. All CCTV device installations must be approved by the Director of Security Services.

b All CCTV installation requests shall be reviewed by the Security Manager and the Technology Administrator who will determine best practices, advice on locations, and assist in completing a CCTV Certificate of Installation. (see Appendix A)

c The University will make every effort to position cameras so that they only cover University premises or occupied spaces.

d CCTV cameras will be installed in public areas, such as hallways, common areas, parking lots and walkways.

e Video surveillance for the purpose of monitoring work areas or sensitive areas should only occur in special circumstances where approved by the Director of Security Services and Vice-President (Administration). Where CCTV is to be installed in Residence areas the Director of Housing and Conference Services will be involved.

f All CCTV areas will be marked with signage to ensure that people entering the area are aware that video recordings are in operation, except in circumstance related to approved covert cameras.

6.2 Covert Cameras

Covert cameras will only be installed with the written authorization of the Vice-President (Administration), where:

a Covert camera approval form has been completed. (see Appendix B)

b Installation is for law enforcement purposes.

c Informing the individual(s) concerned that the recording is taking place would seriously prejudice the reason for making the recording.
d There is good cause to suspect that an illegal or unauthorized action(s) is taking place or is about to take place.
e A written investigative plan has been completed and approved by the Director of Security Services.
f Any such monitoring will only be carried out for a limited and reasonable amount of time, consistent with the objectives of the monitoring, and only for a specific unauthorized activity. In such cases, no signage will be posted.

6.3 Monitoring

a All video monitoring locations are to be approved by the Director of Security Services.
b Video monitoring shall be conducted in a professional, ethical and legal manner by University personnel who have signed a Confidentially Agreement.
c Personnel involved in monitoring will be appropriately trained and supervised in the lawful and responsible use of this technology.
d Persons who regularly monitor CCTV will be subject to a criminal background check by the University, which will include a police services vulnerability screening. The cost of obtaining a criminal background check shall be paid for by the University.
e Monitoring shall be limited to uses that do not violate a person's reasonable expectation to privacy.

6.4 Securing and Retaining Images

a Recordings which have not been viewed for law enforcement or public safety purposes will be deleted after 7 days unless an extension is authorized by the Director of Security Services.
b No recording is to be retained after 7 days unless requested by McMaster University Security Services, solely for the purpose of an investigation.
c Copies of recordings shall be controlled by Security Services, shall be recorded in the log book in Security Services, and shall only be made for investigative and/or evidence purposes except as outlined in 6.5.c.
d Recording used for law enforcement or public safety purposes will be destroyed in a secure manner after one (1) year from the time they were used, or following the court proceeding and the expiry of any relevant appeal period, whichever occurs later.

6.5 Disclosure of Images

a Information obtained through video monitoring shall be used exclusively for security and law enforcement purposes, except as outlined in 6.5.c.
b No attempt shall be made to alter any part of a recording.

c Video recordings will not be shown or provided to anyone other than Security Services personnel except in the following circumstances:
   i Law enforcement agencies for the purpose of an investigation.
   ii For use at a formal University proceeding such as a Student Code of Conduct hearing.
   iii To assist in the identification of individuals relating to a criminal incident.
   iv To comply with a Freedom of Information request by the person whose identity has been recorded who shall have the right to access such information, unless an exemption under FIPPA applies.
   v Other circumstances as approved by the Director of Security Services.

d Video recordings from proprietary CCTV systems may be viewed by Designated Managers provided the following:
   i The viewing is conducted in a professional, ethical and legal manner
   ii A signed Confidentially Agreement is on file with Security Services.
   iii Appropriate training and supervision in the responsible use of this technology is provided.
   iv A successful criminal background check, including a police service vulnerability screening, is completed by the University.
   v Viewing is limited to uses that do not violate a person's reasonable expectation to privacy.
   vi Individual password log-ins are used.

e Disclosure of video recordings to third parties will only be made in accordance with the purpose(s) for which the system was installed, and will be limited to:
   i Police and other law enforcement agencies, where the images recorded could assist in a specific criminal enquiry and/or the prevention of terrorism and disorder.
   ii Prosecution agencies.
   iii Relevant legal representatives.
   iv People whose images have been recorded and retained, unless an exemption under FIPPA applies.
   v In exceptional cases, to assist in the identification of a victim, witness or perpetrator in relation to a criminal incident.
   vi Members of staff involved in University disciplinary processes.

7 Non-Compliance with this Policy

7.1 Any non-compliance of this policy by departments, individuals or third party suppliers shall be reported to the Director of Security Services.

7.2 The Director of Security Services will review all reports of non-compliance and advise the Vice-President (Administration) to determine the appropriate resolution or sanctions.

8 Related Procedures or Documents

8.1 *Freedom of Information and Protection of Privacy Act* ("*FIPPA*")

8.2 *Ontario Information and Privacy Commissioner's Guidelines for the Use of Video Surveillance Cameras in Public Places*

APPENDIX A – CCTV PROGRAM INSTALLATION APPROVAL FORM

CCTV Camera – Certificate of Installation

Date of Request: _____ Installation Date: _____

Department Making Request: _____

Purpose for installation:

_____

Monitoring Requirements/Expectations/Designated Manager for viewing

_____

Security and UTS Comments:

_____

CCTV Location:

Building: _____ Room Number or Area: _____

CCTV Type *ie: Fixed / PTZ* _____ Retention Length _____

Reviewed By: **Approved By:**

_____	_____	_____
Security Manager	Technology Administrator	Director of Security

APPENDIX B – COVERT CAMERA APPROVAL FORM

Covert Camera Installation Approval Form

Date of Request: _____ **Security I/R Number:** _____

Person Making Request: _____

Location of Camera: _____

Installation Date: _____ **Removal Date:** _____

Reason for Request and supporting evidence:

_____

APPROVALS:

Director of Security: _____

VP (Administration): _____