

UNIVERSITY OF MANITOBA POLICY

Policy:	CLOSED CIRCUIT TV (CCTV) MONITORING
Effective Date:	October 1, 2012
Revised Date:	November 20, 2012
Review Date:	October 1, 2022
Approving Body:	Board of Governors
Authority:	<i>The University of Manitoba Act, Section 16(1)(b)</i> Vice-President (Administration) Bylaw, Section 9 <i>The Privacy Act (Manitoba), RSM 1987, c. P125</i> <i>The Freedom of Information and Protection of Privacy Act (FIPPA), SM 1997, c. 50</i> <i>Criminal Code (Canada), RSC 1985, c. C-46</i>
Responsible Executive Officer:	Vice-President (Administration)
Delegate:	Chief Risk Officer
Contact:	Chief Risk Officer
Application:	Board of Governors members; Senate members; Faculty/School Councils; Department Councils; Students; All University employees, student and employee organizations; Contractors working full-time on University property

Part I Reason for Policy

- 1.1 The purpose of this Policy is to provide guidance regarding the use of video, or closed circuit TV (CCTV), security monitoring in areas owned or leased by the University of Manitoba. CCTV is used to enhance security, safety and the quality of life of the campus community through state-of-the-art technology to afford:
- (a) Enhancement to the protection of individuals, property and buildings;
 - (b) A visual deterrent to crime;
 - (c) Confirmation of alarms;
 - (d) Virtual patrol of public areas;

- (e) To assist in the identification of individuals who may breach University policies;
- (f) Assistance in the investigation of criminal activity.

Part II Policy Content

- 2.1 Video monitoring shall not be used to evaluate employee performance or for any surveillance purpose contrary to this Policy or related procedures.
- 2.2 Notwithstanding sections 1.1 and 2.1, video monitoring for the following purposes is not subject to the provisions of this Policy:
 - (a) Cameras used for academic purposes. Cameras used for research would be governed by other policies involving human subjects and are, therefore, excluded from this Policy.
 - (b) The use of video equipment to record public performances or events, interviews, or other use for broadcast or educational purposes.
 - (c) Automated teller machines (ATMs), which may utilize cameras, are exempt from this Policy.
- 2.3 The Director, Security Services, is responsible for all CCTV monitoring for the purposes of enhancing safety and security on University campuses and University locations where CCTV cameras are used. Security Services is responsible for the administration and daily operation of all CCTVs. Supervisors of the monitoring centers on all campuses and locations where CCTV cameras are used will be responsible for proper camera monitoring practices.
- 2.4 Only Security Services staff or other staff as designated by the Director, Security Services, trained in the use of the CCTV system will be authorized to operate or monitor cameras at any time.
- 2.5 Information Services & Technology (IST) is responsible for the development and update of CCTV specification standards; camera and related infrastructure; installation of video recording devices and related maintenance; and video data storage. IST is responsible for training personnel in the use of this technology and will provide on-line and remote access to individuals authorized to operate or monitor the cameras.
- 2.6 Security Services will be responsible for ensuring that the implementation and operation of each camera complies with this Policy and related procedures.

Camera Installation

2.7 Requests for CCTV installation and monitoring must be made to the Director, Security Services:

- (a) Deans, Directors or Department Heads may request permanent CCTV installations in areas under their responsibility to the Director, Security Services.
- (b) Security Services will assess any requests using accepted Crime Prevention Through Environmental Design (CPTED) techniques in consultation with the FIPPA Unit Liaison. A recommendation would then be made to the Associate Vice-President (Administration) regarding when and how equipment should be deployed. No installation will be made without consultation of the Deans, Director or Department Head, as the case may be, that oversees or manages the area where cameras are to be placed.
- (c) If there is reason to suspect that criminal or illegal activity may be occurring, the Director of Security Services may make a request to the Associate Vice-President (Administration) for temporary or covert installation of CCTV cameras. In such cases, the appropriate Dean, Director or Department Head would be notified of the installation.

Note: Canadian criminal law does not allow for the monitoring of any person engaged in activity in circumstances in which the person has a reasonable expectation of privacy unless authorities have obtained a warrant allowing them to do so.

- (d) All requests for CCTV funding must be made to the Associate Vice-President (Administration), who will review these requests and prioritize them in consultation with the Director, Security Services, the Chief Information Officer (CIO), Information Services & Technology Services, and the Dean, Director or Department Head that oversees or manages the area where cameras are to be placed. Any new building construction or major renovation must include in its capital budget an allowance for CCTV installation.

Access to Video Surveillance Information

2.8 The Director, Security Services may disclose information in relation to a criminal investigation, including any surveillance camera recordings to the Winnipeg Police Service, other law enforcement agency, subject to section 5.2 of this Policy.

2.9 All requests for information will require a University of Manitoba Law Enforcement Disclosure form to be completed by the representative of the public

body making the request. A copy of the completed form will be sent to and kept on file in the Access and Privacy Office.

- 2.10 All other requests for access to information under FIPPA and PHIA, including surveillance camera recordings, and law enforcement requests not relating to criminal investigations shall be facilitated by the Access and Privacy Office.
- 2.11 FIPPA/PHIA Unit Liaison Members or Sub-Unit Liaisons, where appropriate, may facilitate the viewing of recordings made in areas within their units, but only for the purposes set out under this Policy.

Part III Accountability

- 3.1 The Office of Legal Counsel is responsible for advising the Vice-President (Administration) that a formal review of this Policy is required.
- 3.2 The Chief Risk Officer is responsible for the implementation, administration and review of this Policy.
- 3.3 Board of Governors members, Senate members, Faculty/School Councils, Department Councils, Students, All University employees, student and employee organizations, and Contractors working full-time on University property are responsible for complying with this Policy.

Part IV Authority to Approve Procedures

- 4.1 The Vice-President (Administration) may approve Procedures, if applicable, which are secondary to and comply with this Policy.

Part V Review

- 5.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Policy is October 1, 2022.
- 5.2 In the interim, this Policy may be revised or repealed if:
 - (a) the Vice-President (Administration) or Approving Body deems it necessary or desirable to do so;
 - (b) the Policy is no longer legislatively or statutorily compliant; and/or
 - (c) the Policy is now in conflict with another Governing Document.

- 5.3 If this Policy is revised or repealed, all Secondary Documents will be reviewed as soon as reasonably possible in order to ensure that they:
- (a) comply with the revised Policy; or
 - (b) are in turn repealed.

Part VI Effect on Previous Statements

- 6.1 This Policy supersedes all of the following:
- (a) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and
 - (b) all previous Administration Governing Documents on the subject matter contained herein.

Part VII Cross References

- 7.1 This Policy should be cross referenced to the following relevant Governing Documents, legislation and/or forms:
- (a) [Security, Surveillance and the Release of Information Policy](#);
 - (b) [FIPPA and PHIA Policy, related to Procedures and Information Sheets](#);
 - (c) [Administrative Bulletin No.76 \(until superseded\)](#);
 - (d) [Closed Circuit TV \(CCTV\) Monitoring Procedures](#);
 - (e) [The Ethics of Research Involving Humans Policy and related Administrative Bulletin \(No.79\)](#).