UNIVERSITY OF MANITOBA

UNIVERSITY OF MANITOBA
PROCEDURE

Procedure:	**Closed Circuit TV (CCTV) Monitoring**
Parent Policy:	Closed Circuit TV (CCTV) Monitoring Policy
Effective Date:	October 1, 2012
Revised Date:	
Review Date:	October 1, 2022
Approving Body:	Vice-President (Administration)
Authority:	Closed Circuit TV (CCTV) Monitoring Policy
Responsible Executive Officer:	Vice-President (Administration)
Delegate:	Chief Risk Officer
Contact:	Chief Risk Officer
Application:	Board of Governors members; Senate members; Faculty/School Councils; Departmental Councils; Students; all University Employees; Students and Employee Organizations; Contractors Working Full Time on University Property

Part I
Reason for Procedure

1.1 These procedures accompany the Policy on CCTV usage. Video applications are powerful tools that raise complex issues in terms of privacy, access and disclosure.

1.2 The University of Manitoba reserves the right to review and approve any proposed installation of video applications on properties owned, leased or controlled by the University of Manitoba. All video applications must conform to relevant laws in addition to University policy. As the primary use of CCTV applications is for safety and security, Security Services is charged with the responsibility of reviewing, recommending, and approving proposed video applications under the CCTV Policy.

Part II
Procedural Content

Operational

2.1 Security Services will monitor new developments in the relevant law and security industry best practices to ensure that CCTV monitoring on University property is consistent with the highest standards and protections.

2.2 Video monitoring for security purposes will be conducted in a professional, ethical, and legal manner. Monitoring individuals based solely on race, gender, religion, ethnicity, political belief, sexual orientation, disability or other similar characteristic is prohibited.

2.3 All personnel involved in CCTV monitoring will perform their duties in accordance with the CCTV Policy and these Procedures.

2.4 The Director, Security Services, will conduct an annual audit and inspection to assure that responsible and proper camera monitoring practices are being followed and that each camera is still reasonably necessary to accomplish the purpose for which it was installed.

2.5 Security Services will be responsible for the secure storage of all captured images. Recording devices will be located in secure locations with access by authorized staff only. Logs shall be kept of all instances of access to, and use of, recorded material.

2.6 Security Services will be responsible for regular testing of the video systems. In the event that a camera or associated CCTV system component requires repair or has otherwise rendered the device non-functioning, the camera shall be immediately removed. Repairs and removal/replacement of cameras are the responsibility of Physical Plant. Information Services and Technology (IST) is responsible for maintenance and support of the recording devices and related infrastructure.

Location and Signage

2.7 Security Services will be responsible for ensuring appropriate signage in all areas monitored by CCTV cameras, except where approval has been received from the Associate Vice-President (Administration) for covert monitoring.

2.8 Excluding specific investigations that require covert CCTV applications, the following signage should be clearly posted at any public location visible by a camera application:

THIS AREA IS SUBJECT TO VIDEO MONITORING:

For more information, contact Security Services at (204) 474-9312

2.9 Cameras will be situated in identified public areas. Cameras will not monitor areas where individuals have a reasonable expectation of privacy. Places where there are reasonable expectations of privacy include, but are not limited to locker rooms, washrooms, shower facilities, private offices, private residences or properties neighbouring the University.

2.10 Cameras must be placed strategically and must not be deployed in a "wholesale" manner. Excluding specific investigations that require covert CCTV applications, cameras must be located in visible locations as to not be seen as being covert.

2.11 No attempt shall be made to alter any part of an original recording and cameras must be located securely such that they are not easily tampered with.

2.12 The Director, Security Services, shall submit a written, annual report to the Associate Vice-President (Administration) on all camera locations, a list of trained personnel, the number of access and disclosure requests for video images and, where relevant, statistics relating to criminal behaviour on campus.

Image Storage and Retention

2.13 All video or digital recordings, whether maintained by IST or Security Services will be deleted or erased after thirty (30) days, unless retained as part of a criminal investigation, pending court proceedings (criminal or civil), or other bona fide use as approved by the Director, Security Services.

2.14 Recordings used for evidence in any criminal or civil proceedings will be retained until any subsequent appeal periods have expired.

2.15 Recordings used to make a decision that directly affects an individual will be retained for a reasonable period of time which will be determined by approved records authorities' schedules.

Part III
Accountability

3.1 The Office of Legal Counsel is responsible for advising the Vice-President (Administration) that a formal review of this Procedure is required.

3.2 The Chief Risk Officer is responsible for the implementation, administration and review of this Procedure.

3.3 Board of Governors members, Senate members, Faculty/School Councils, Departmental Councils, Students, all University Employees, Students and Employee Organizations, and Contractors Working Full Time on University Property are responsible for complying with this Procedure.

Part IV
Review

4.1 Governing Document reviews shall be conducted every ten (10) years. The next scheduled review date for this Procedure is October 1, 2022.

4.2 In the interim, this Procedure may be revised or repealed if:

(a) the Vice-President (Administration) or Approving Body deems it necessary or desirable to do so;

(b) the Procedure is no longer legislatively or statutorily compliant;

(c) the Procedure is now in conflict with another Governing Document; and/or

(d) the Parent Policy is revised or repealed.

Part V
Effect on Previous Statements

5.1 This Procedure supersedes all of the following:

(a) all previous Faculty/School Council Procedures stemming from the Faculty/School Council Bylaw and academic and admission Regulations and any resolutions on the subject matter contained herein;

(b) all previous Board of Governors/Senate Governing Documents on the subject matter contained herein; and

(c) all previous Administration Governing Documents on the subject matter contained herein.

Part VI
Cross References

6.1 This Procedure should be cross referenced to the following relevant Governing Documents, legislation and/or forms:

(a) FIPPA and PHIA Policies, related Procedures and Information Sheets;

(b) Administrative Bulletin No.76 (until superseded);

(c) Closed Circuit TV (CCTV) Monitoring Policy;

(d) Security, Surveillance and Release of Information Policy;

(e) Ethics of Research Involving Humans Policy and related Administrative Bulletin (No.79).