University of Guelph
1.2.53 Video Surveillance System Policy

Approved by:	Vice President, Finance, Administration and Risk
Policy Effective Date:	September 1, 2017
Distribution:	Public
Signatory:	
Applicable Policies:	1.2.54 Video Surveillance Systems Procedure University Privacy Policy FIPPA

Disclaimer: If there is a discrepancy between this electronic Standard Operating Procedure and the written copy held by the Signatory, the written copy prevails.

Contents:

1.0 Purpose
2.0 Scope
3.0 Applicable Policies and Legislation
4.0 Definitions
5.0 General
6.0 Responsibilities
7.0 Policy

1.0 Purpose

The purpose of this policy is to provide guidelines around how the University's Video Surveillance System (VSS) is installed, monitored and utilized. This Policy, in accordance with FIPPA legislation, will outline how data is collected, used, disclosed and stored. Additionally, this Policy outlines roles and responsibilities for those administering the VSS and those using the VSS.

2.0 Scope

This policy applies to all VSS that are owned and used on University owned or occupied properties, the Authorized Users and administrators of the VSS.

3.0 Applicable Policies and Legislation

This Policy shall be in accordance with, but not limited to this policy and applicable federal legislation as well as:

- Acquisition and Implementation of Main Campus Networked Computerized Systems
- Freedom of Information and Protection of Privacy Act (FIPPA)
- VSS Operating Procedure
- University of Guelph's Privacy Policy, as well as other applicable University policies, Federal and Provincial legislation.

4.0 Definitions

4.1 Authorized User*:*
University departmental staff that have been designated and approved by their Dean or Director (for administrative units) to access their department's VSS.

4.2 Camera:
A camera is a device that converts images into electrical signals for transmission and recording.

4.3 Covert device:
A covert device is a concealed or hidden surveillance device where no signage is posted to make individuals aware a surveillance device is in place and operational.

4.4 Dummy Cameras**:**
A dummy camera (i.e., a fake, simulated, or decoy camera) is a non-functional camera designed to mislead a person who sees it into believing the area is being watched or recorded.

4.5 Monitoring*:*
The term monitoring implies having access to view video. Live monitoring is typically only permitted for Campus Community Police or for reception video equipment with restricted capabilities.

4.6 Perimeter Access:
Perimeter Access refers to a point of entry or egress equipped with a door access control system. Perimeter Access may be connected into the VSS for some operational functions (i.e. door alarms that trigger a video image).

4.7 Video Surveillance System (VSS):
Refers to devices that enable continuous or periodic video recording, Monitoring of individuals in campus buildings and on the University main campus premises. The Information and Privacy Commissioner/Ontario includes in the term video surveillance system thermal imaging technology or any other component associated with recording the image of an individual. VSS used within a department may also include video analytics (i.e., Perimeter Access reports/queries) as part of other integrated systems.

4.8 Video Surveillance Coordination Group (VSCG)
The VSCG is responsible for the coordination and administration of the Video Surveillance on campus and is comprised of representatives from Campus Community Police and Physical Resources Electronic Access Unit. Additional representatives from campus stakeholder groups may also be included to assist with coordination needs.

5.0 General
The University of Guelph will uphold an individual's reasonable expectation of privacy as defined by law, and the University's obligation to maintain a safe and secure environment for students, staff, faculty and visitors. The VSS may result in the collection of personal information (e.g. images, data) and records of conduct that may be considered breaches of law or University policies or which may compromise the security of our campus or facilities. Video recording for security purposes will be conducted in accordance with applicable legislation.

Authorized departments using Video Surveillance may introduce additional policies and internal procedures, with approval from the VP Administration, Finance and Risk, for the operation of their unique environments provided that any policies/procedures meet the standards described in this policy as well as other applicable University policies or standard operating procedures.

The VSS on campus and is evaluated based on the following criteria:

a) Enhance public safety in areas where there is a perceived or real risk;

b) Prevent and deter behavior that may be contrary to applicable legislation, law or University policies;

c) Provide a tool to enhance personal safety and protection of property;

d) Assist with investigations and follow up to behavior.

6.0 Responsibilities

6.1 The VSCG (i.e. Campus Community Police and Physical Resources Electronic Access Unit) is jointly responsible for the administration of the VSS including but not limited to the installation, use, data storage, and management of Authorized Users and access. Specific responsibilities are listed below and also outlined in the Video Surveillance System Standard Operating Procedure.

6.2 The VSCG will conduct an audit of the VSS when required and provide information to the VP Administration, Finance and Risk.

6.3 The VSCG will provide guidelines and resources for VSS user training. Additional training may also be provided by the University's Privacy Office.

6.4 Campus Community Police has specific responsibility for the following:

a) Receiving, evaluating and providing initial approval for VSS requests;
b) Exporting and releasing data/video for external disclosures which have been approved by the Director Campus Community Police (in consultation with other University personnel as required);
c) Providing Authorized Users with this Policy and information on responsibilities;
d) In consultation with Vice President Administration, Finance and Risk approve use of Covert Devices.

6.5 Physical Resources has specific responsibility for the following:

a) Installing VSS devices after initial approval from Campus Community Police;

b) Managing data storage in a secured area in accordance with the University's data retention and privacy policies;

c) Providing the proper functioning and recording of approved VSS in cooperation with the University's Computing & Communications Services department;

d) Administrating the Perimeter Access software as it relates to VSS;

e) Managing the life cycle of authorized VSS equipment and software (e.g. equipment standards, maintenance, replacement, disposal and related requirements);

f) Providing signage and ensuring it is posted and visible in areas where VSS Camera(s*)* is/are in use.

6.6 Authorized Departments are responsible for:

a) Authorized Users complying with this policy;

b) Providing Authorized Users with proper training materials, guidelines and resources as outlined by the VSCG;

c) Utilizing the VSS for the purpose authorized by Campus Community Police;

7.0 Policy

7.1 Any requests for VSS must first have the approval from the applicable Dean or Director. Following departmental approval, requests are submitted to Campus Community Police for evaluation and approval. Campus Community Police will approve the use and location of Video Surveillance in consultation with other members of VSCG.

7.2 No department on campus will be extended viewing rights (i.e. Monitoring) unless approved by the Director Campus Community Police.

7.3 All VSS devices will not normally be installed where the public and employees of the University have a reasonable expectation of privacy (e.g. change room, washrooms) unless otherwise approved by the Director of CCP and VP Finance, Administration and Risk. VSS is installed in public areas, such as hallways, common areas, parking lots and walkways.

7.4 Covert Devices are not permitted unless approved by the Director of Campus Community Police and VP Administration, Finance and Risk. Depending on the circumstances, consultation with other senior leadership may also occur. Covert Devices will only be used in circumstances where:

a) There are reasonable grounds given the nature and severity of circumstances to warrant such action;

b) Covert Devices are only carried out for a limited and reasonable amount of time;

7.5 To avoid giving the public a false sense of security, use of Dummy Cameras on campus is prohibited.

7.6 All departmental areas shall be signed to ensure individuals entering a video surveillance area are aware of video recordings, with the exception of any approved covert Cameras. All signage will be prominently displayed at the perimeter of the monitored areas and at key locations. Signage will include a contact as to where additional information or questions can be directed.

7.7 The existence of this policy does not imply that a VSS is being monitored in real time although Campus Community Police is authorized to monitor in real time (when in a secure and restricted area) as required.

7.8 External Disclosure: The University of Guelph adheres to FIPPA legislation and the University's Privacy Policy regarding the way that personal information is disclosed. A request for external disclosure may be submitted to the Director CCP who will review the request in consultation with other senior university administrators as appropriate.

Internal release: may be requested from the Director Campus Community Police (CCP) by a University Administrator for the purposes of fulfilling their duties. The Director CCP, in consultation with other University staff (as required), will determine if the request meets criteria for internal release.

7.9 Any exporting of video surveillance data for the purposes of disclosure or retention of records must be exported to an encrypted device and securely maintained.

7.10 Data from the VSS is retained for no longer than 30 days (i.e. time of retention before data is overwritten),

unless otherwise requested by Campus Community

Police or Senior University Administrator for investigative purposes or as required by law. Any data that has been accessed or disclosed will be maintained and disposed of in accordance with FIPPA regulations and University policies.

7.11 Video Surveillance equipment used for reasons other than the purposes outlined in section 5.0 and as authorized by Campus Community Police may be a breach of the Criminal Code of Canada, University Privacy Policy or Privacy Legislation. Privacy breaches may result in disciplinary action in accordance with University policies and procedures. Privacy breaches of any kind, must be reported to the University Privacy Officer no less than 24 hours after incident.