University of Guelph
1.2.54 Video Surveillance System Standard Operating Procedure

Approved by: AVP, Physical Resources
              Director, Campus Community Police, Emergency Services and Fire Safety
Policy Effective Date: June 26, 2017
Revised: May 19, 2017
Distribution: Internal – Physical Resources, Campus Community Police, VP, FA&R
Signatory:


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

Contents:

1.0 Purpose
2.0 Scope
3.0 Procedures
   3.1 Video Surveillance Coordination Group
   3.2 Request Process
   3.3 Approvals
   3.4 Covert Devices
   3.5 Funding
   3.6 Training
   3.7 Collection & Privacy
   3.8 Use
   3.9 Disclosure
   3.10 Storage
   3.11 Exporting of Data
   3.12 Installation
   3.13 Audits
   3.14 Public Notices and Signage
   3.15 Non Functioning Cameras

Appendix A: Internal Process Overview
1.0 Purpose & Scope
The purpose of this standard operating procedure (SOP) is to outline how requests for the Video Surveillance System (VSS) are managed by Video Surveillance Coordination Group and to outline additional aspects of how the VSS is administered at the University. This SOP is internal to Campus Community Police and Physical Resources and supplements the Video Surveillance System Policy.

2.0 Definitions
For clarity on terms and definitions, refer to the Policy document.

3.0 Procedures

3.1 Video Surveillance Coordination Group (VSCG)
The Video Surveillance System is administered jointly between Campus Community Police (CCP) and Physical Resources (PR). Members of the VSCG are designated by the Director CCP and Director Finance/Administration (PR). Typically members will include the following:
- The Manager of Operations, CCP;
- A designated Sergeant or Officer;
- The Manager, Information Systems, PR;
- The Analyst III, Electronic Access Unit, PR;
- Additional representatives as required

The VSCG is responsible for the coordination and administration of the VSS for campus, this includes but is not limited to:
- Receiving requests for VSS;
- Evaluating and approving requests for VSS;
- Assessing technical requirements for system and devices;
- Procuring systems and devices;
- VSS Website management;
- Managing of VSS resources;
- Developing training, policies and procedures related to the VSS;
- Completing system audits and assessments.

3.2 Request Process
Requests for video surveillance (e.g. cameras) are submitted via online form (Appendix D). This form is
then emailed to the VSCG and a Campus Community Police representative will be assigned to review the request. In order for a request to be evaluated it must first have the approval of the Dean (academic unit) or Director (administrative unit). Requests are evaluated by a set criteria as well as other factors detailed in the Video Surveillance Request Evaluation (See Appendix F).

VSS installations are prioritized based on the needs of the campus community and the University’s overall safety/security strategy.

3.3 Approval Process
Campus Community Police will review requests initially and complete an evaluation. If approved, the request will then be forwarded to Physical Resources for final approval. Installations of video surveillance will only commence once Physical Resources has evaluated and approved technical and financial feasibility.

3.4 Covert Device
Covert Device requests must be submitted in writing for approval to the Director Campus Community Police (Appendix E). Ultimate approval for Covert Devices rests with the Vice President, Administration, Finance and Risk in consultation with other senior administrators where appropriate.

3.5 Funding
Typically, departments requesting VSS are responsible for all related costs. Coding must be submitted with a work order to Physical Resources following initial approval from Campus Community Police. Limited central funding may be available for VSS that are deemed to be a campus safety priority.

3.6 Training

3.6.1 Authorized User Training
A department with access to the VSS must identify who will be designated as an Authorized User and provide appropriate training as identified by the VSCG. Training materials and resources are available on the VSS website and also outlined in Appendix C. Depending on the nature of the VSS, Campus Community Police, Physical Resources Electronic Access Unit, and the University’s Privacy Office are also available for additional consultation on training.

3.6.2 Video Surveillance Coordination Group- VSCG Training
Training for the VSCG (i.e. Campus Community Police and Physical Resources), is the responsibility of the Physical Resources Director, Finance and Administration and the Director Campus Community Police.

3.7 Collection & Privacy
Collection of data from VSS will be in accordance with FIPPA and the University’s Privacy Policy. If video surveillance equipment is used for reasons other than the purposes outlined in the VSS Policy 1.2.53 it may be considered a breach of the Criminal Code of Canada, University Privacy Policy or
Privacy Legislation. Privacy breaches may result in disciplinary action. All privacy breaches must be reported to the University Privacy Officer no less than 24 hours after incident.

3.8. Use
Viewing of video must be limited to a specific event/activity and be limited to an appropriate timeframe for investigative purposes related to the activity/event. Additional regulations on use of data collected from VSS is detailed in FIPPA.

3.9 Disclosure

3.9.1 Internal Use/Release
A University administrator who requires access to video surveillance data for the purpose of fulfilling their duties must submit a request to the Director of Campus Community Police who will determine, in consultation with other University staff (e.g. Privacy Officer, Legal Counsel) as required, if the request meets the criteria for releasing information.

3.9.2 External Disclosure
External Disclosure will be handled in accordance with the University’s Privacy Policy and regulations under FIPPA. External data disclosures shall be directed to the Director of Campus Community Police. The Director CCP will consult with other University senior administrators as appropriate.

3.10 Storage

3.10.1 Access to Storage Devices
Access to VSS storage devices (i.e. archiver) is only permitted by authorized personnel (e.g. Physical Resources IT Managers, Computing and Communications Services).

3.10.2 Storage Areas
Storage systems and devices (e.g. archiver) shall be stored securely and in a controlled area.

3.10.3 Retention of Records
Physical Resources retains data from VSS normally for no longer than 30 days at which time it is destroyed, unless otherwise required. If a record is required for longer than 90 days by Campus Community Police or an investigative body or as part of FIPPA requirements then this shall be directed to PR Electronic Access Unit. Video which has been used as part of the University’s judicial system will be kept for a period of one year in accordance with FIPPA. All other data and records will be maintained in accordance with FIPPA regulations and University policies.

3.11 Exporting of Data
Exporting of video surveillance data should be limited whenever possible. In cases where exporting data is required, authorized individuals (as determined by the Director CCP) must export data to an approved encrypted device and which is securely maintained until destroyed.

3.12 Installation
Following a recommendation and initial approval from Campus Community Police to install a
camera/VSS device, Physical Resources will assess technical requirements and determine next steps for installation.

3.12.1 Major Renovations and New Construction
VSSs for major renovations or new construction projects is managed through a Physical Resources (DEC) Project Manager in consultation with the Director Campus Community Police and Physical Resources Electronic Access Group.

3.13 Auditing and Evaluation

3.13.1 Audits
Audits will be conducted by the VSCG when requested. An audit may include a review of Authorized Users, roles and responsibilities, incident data involving VSS, and practices surrounding the VSS to ensure compliance with the policy and procedures. The Director Campus community Police, and AVP Physical Resources will review audit findings and relay significant recommendations to the Vice President, Admin, Finance and Risk.

3.14 Public Notice and Signage

3.14 Signage
Signage for VSS will be in accordance with FIPPA legislation and be provided by the VSCG. Typically signage will include a clear, language-neutral graphical depiction of the use of video surveillance and shall be prominently displayed at the perimeter of the monitored areas and at key locations within the areas (with the exception of approved covert cameras). Signage will also include basic information to clarify that video surveillance is being used in the area. The signage will also include where additional information or questions can be directed.

3.14.2 Damaged or Missing Signs
Damaged or missing signs are to be reported to Physical Resources via a work order request.

3.15 Non-Functioning Cameras
To avoid giving the public a false sense of security, use of dummy cameras is prohibited. Therefore, non-functioning cameras will be repaired within a reasonable timeframe, typically (15) fifteen business days. If a camera cannot be repaired within this timeframe, the camera shall be removed or dismantled to avoid creating a “dummy camera”.

To receive this document in an alternative format please contact wo@pr.uoguelph.ca
Appendix A: Internal Process Overview

CCP = Campus Community Police
PR = Physical Resources
(Electronic Access and/or
Electrical Design Technologist

User request submitted (online submission via VSS website)

- CCP designate will review camera request and may schedule a site visit (Crime Prevention Through Environmental Design (CPTED) principles are also a consideration)

- CCP designate evaluates request (typically within 15 business days) based on camera criteria

  - If APPROVED, request along with CCP assessment is forwarded to Physical Resources
  - Assessment will include a recommendation on central funding support if applicable
  - If request is DENIED or not supported by CCP, CCP will communicate this to requester and provide a rationale.

User will be instructed to complete a work order and must provide coding prior to installation.

Physical Resources will prioritize requests based on CCP recommendation and evaluation criteria.

Central funding may be approved by AVP Physical Resources OR VP Admin, Finance, Risk; for cameras that are mostly exterior to buildings or considered a priority for campus (e.g. crime deterrence or exteriors.)
Appendix B: VSS User Overview

- Request for camera(s) submitted by department and signed off by Director/Dean/Chair

- Departmental user completes online request form on VSS website

- CCP may request additional information to evaluate request.

- CCP will conduct a site visit with or without 'Contact Person' to evaluate request, purpose and location etc.

  - Evaluation is then forwarded to Physical Resources for installation (if approved).
  - If not approved, CCP will notify the requester and provide a rationale.

- Department will be required submit a work order with coding prior to installation.
Appendix C: Training Guidelines for VSS Authorized Users

It is the responsibility of the Dean/Director/Chair to ensure that a) an up to date list of authorized users for their specific VSS is maintained and b) that these users receive the appropriate training given the access/use they have been granted. The Video Surveillance Coordination Group (VSCG) will retain a list of all authorized users for the VSS. This requirement is outlined in the University of Guelph Video Surveillance Policy as well as the Information and Privacy Commissioner of Ontario Guidelines for Video Surveillance Cameras in Public Places.

The VSCG recommends that Deans/Directors/Chairs or their designate follow the training criteria list below with any authorized users in their respective area. Additional training can be supported by the VSCG or the University Privacy Office. For questions regarding training please contact the VSCG by visiting the video surveillance website.

Training Criteria:

1. Authorized Users are provided with a copy of the VSS Policy and instructed that this is to be read and kept on file.

2. Authorized Users are instructed how to manage a privacy breach depending on departmental procedures (e.g. contact their supervisor immediately).

3. Roles and responsibilities of Authorized Users which are listed in the Video Surveillance Policy are specifically reviewed.

4. Authorized Users are instructed in what situations the VSS may be accessed and for what purposes, as approved by Campus Community Police. Authorized Users are instructed that accessing or using the VSS for any other purpose is not permitted and may result in disciplinary action.

5. Authorized Users are instructed that cameras or devices may not be moved, altered, or interfered with once installed by Physical Resources. Physical Resources must be contacted for any adjustments or modifications.

6. Authorized Users are instructed that they are responsible for reporting any problems or damage to camera by emailing the eaccess@pr.uoguelph.ca.

7. Authorized Users are instructed that VSS signage must always be prominently displayed per the Video Surveillance Policy in any surveillance area. If signage is missing or damaged this is to be reported to eaccess@pr.uoguelph.ca immediately.

8. Authorized Users are instructed that their use of equipment, monitoring, and access may be reviewed for the purpose of an audit or if there is a concern the system is not being utilized for an approved use.
9. Authorized Users sign a confidentiality statement and/or complete a criminal background check if required by internal policies.

11. Authorized Users are instructed that copying, downloading, printing data or images from the VSS is not permitted and may result in disciplinary action. Providing content or data to other parties (within or outside of the University is strictly prohibited).

12. Authorized Users are made aware that the VSS is strictly for University business and shall never be accessed for reasons that are not explicitly authorized (e.g. personal reasons).

13. Authorized Users shall be provided with an area that is concealed as much as possible for viewing or monitoring of VSS equipment so that the general public or unauthorized individuals cannot view footage or data.

14. Authorized Users are made aware that all requests for footage shall be directed to the Director of Campus Community Police, in writing.

The above training criteria will be included in training for any Authorized User within ______________________(department/area).

__________________________________________
Signature (Dean/Director/Chair) or designate

__________________________________________
Date
Appendix D: Request for VSS Form (online submission)

University of Guelph
Video Surveillance System (VSS) Request Form

Date: _________________________

Requesting Department: _________________________________

Approving Dean/Director/Chair: _________________________________

Contact Person: _________________________________ (name)
                        _________________________________ (email)
                        _________________________________ (phone)

Each camera request must be listed separately for individual evaluation. Please indicate the specific location and purpose for each request:

Camera # 1:     <blg> <floor> <area> <rm#>       Purpose: Loss/theft prevention: _____
                                Personal Safety:      _____
                                Remote Door Monitoring: _____
                                Intellectual Security: _____
                                Other:       _____

<Add Camera Request>

Please describe the general purpose or goal of camera request and any supporting documentation:
Covert Camera Installation Approval Form

Date: _________________________

Requesting Department: _________________________________

Dean/Director/Chair: _________________________________

Contact Person: _________________________________ (name)
______________________________ (email)
______________________________ (phone)

Each camera request must be listed separately for individual evaluation. Please indicate the specific location and purpose for each request:

Location Camera # 1: <blg> <floor> <area> <rm#>

Purpose: Prohibited Behaviour: _____
Personal Safety: _____

Installation Date: _________________________ Removal Date: _________________________

Reason for request and supporting documentation (please attach if needed):
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________
____________________________________________________________________________________

Approved by:

______________________________________________________________ (dd/mm/yy)

Director Campus Community Police:

______________________________________________________________ (dd/mm/yy)

VP Finance, Admin & Risk:

______________________________________________________________ (dd/mm/yy)
Appendix F: Video Surveillance Request Evaluation (completed by CCP and PR staff- phase 2 & 3)

Campus Community Police
Video Surveillance Request Evaluation

Camera installation would (please indicate which criteria apply):
____ Enhance public safety in an area where there is a perceived or real risk;
____ Prevent and deter behaviour that may be contrary to the criminal code or University policy
____ Assist in the protection of property
____ Other: __________________________________________________________

Has there been previous incidents in this area?
Yes ____       No_____
If yes, please provide detail on occurrence type, frequency and timing:

Site Visit Checklist

○ Positioning of Camera ________  ○ Controlled Access on Doorway___________
○ Obstructions ________________  ○ Risk to Privacy____________________
○ Angle Required ______________  ○ Current Signage_____________________
○ Nature Egress_______________  ○ Isolation________________________
○ Lighting _________________  ○ Other (please list and make additional
                                     comments as required) ________________________________

Comments and Evaluation

Primary Purpose of Camera (e.g. door monitoring, high traffic area, high incidents, loss prevention, asset protection etc.):
____________________________________________________________________________________
____________________________________________________________________________________

Primary Visual Target of Camera (e.g. equipment, person, large grouping):
Visual Acuity Required (e.g. face recognition, general situational awareness)

Lighting

Possible Obstructions (e.g. bulkheads, signage)

Required Operational Hours (e.g. activity triggered, evening, after closure):

Would you support central funding for this request?  
Yes _____ No ______

Based on evaluation the priority level consideration would be:
Urgent (e.g. high risk, threat)_____High _____ Medium _____ Low_____ No Priority_____

Installation Request Date: (if applicable): (dd/mm/yy)____________

Additional Comments:

Initial Approval: _____ Granted _____ Denied

Reviewed by:  

CCP Officer (dd/mm/yy)
Physical Resources (Electronic Access) Assessment

Work Order Submitted: (dd/mm/yy)__________

CCTV Type: ____________________________________________

Range of Shot __________________________________________

Zoom ________________________________________________

Repositionable __________________________________________

Sensitivity _____________________________________________

Interior/Exterior ________________________________________

Proposed Framing of Camera Attached? _____ YES _____ PENDING

Layout Drawing Attached? _____ YES _____ PENDING

Approved by:

____________________________________________________

Signature (dd/mm/yy)