Video Surveillance

Category: Operations
Approval: pvp
Responsibility: VP Finance and Administration
Date: Date initially approved: November 5, 2013
Date of last revision: same

Definitions:

Reception equipment: any device capable of capturing and/or recording images, including audio and thermal imaging devices.

Video Surveillance System: refers to a video, physical or other mechanical, electronic, digital or wireless surveillance system or device that enables continuous or periodic video recording, observing or monitoring of specific locations on Trent University property and the actions of individuals in those locations.

Personal Information: is recorded information about an identifiable individual which includes, but is not limited to, the individual’s race, colour, national or ethnic origin, sex and age.

Purpose/Reason for Policy:

This purpose of this policy is to regulate the use of video surveillance and recording on Trent University premises.

Information obtained through video surveillance will be used exclusively for security and law enforcement purposes, which must relate to the protection of students, staff, faculty, and the public, or the deterrence or detection of criminal activity, including theft, vandalism, or other property damage.

Scope of this Policy:

Video surveillance may be used for purposes relating to safety of individuals and security of buildings and property. In furtherance of these purposes, video surveillance may be used to monitor exterior and interior areas of Trent property where there is no reasonable expectation of privacy.

This policy only applies to video surveillance activities necessary to enhance the security and safety of people and property on Trent premises. This policy does not apply to Trent owned property that is being leased or rented to a tenant.

This policy has been created in accordance with the Guidelines for Using Video Surveillance Cameras in Public Places as issued by the Information and Privacy Commissioner of Ontario, September, 2007 and the Ontario Freedom of Information and Protection of Privacy Act (the Act), both of which outline the obligations imposed on institutions with respect to the protection of the privacy interests of individuals.
**Policy Statement:**

Video surveillance of Trent premises will be conducted in a professional, ethical and legal manner, in accordance with the following principles:

a) Video surveillance must be conducted in accordance with the laws of Ontario and Canada;

b) Video surveillance will be used only where it is demonstrably necessary for the purposes of enhancing the safety of persons, or for the deterrence of theft or destructive acts, such as vandalism and graffiti.

c) Video surveillance will be used only by Campus Security or Trent employees authorized by the Director, Risk Management, and only where less intrusive means of deterrence, such as monitoring by Security Guards, has been shown to be ineffective or unworkable.

d) Appropriate signs and notice of video surveillance must be posted in areas subject to video monitoring;

e) Employees and video service provider(s) will have access to information collected through video surveillance only where necessary in the performance of their duties and in accordance with the provisions of this Policy.

f) Employees and video service providers who may require access to information collected through video surveillance will be provided proper training and orientation with regards to this Policy and their obligations under this Policy and the Act, and will provide written acknowledgment that they have read and understood the contents of this policy and procedure. Any employee who knowingly or deliberately breaches this policy or the Act will be subject to discipline up to and including termination. Failure of a video service provider to comply with this policy or the Act will constitute breach of contract and may result in termination of contract and legal action.

g) The recording medium must be handled in a manner that maintains the integrity and security of the recorded information;

h) All recorded information shall be destroyed after three months excepting information specifically awaiting review by law enforcement agencies, information seized as evidence, or information that has been duplicated for use by law enforcement agencies.

i) Reception equipment locations and operation shall be limited to visual access of areas where there is no reasonable expectation of privacy. Video surveillance for the purpose of monitoring work areas, social areas, or sensitive areas will only occur in special circumstances, and must be consistent with the policy’s principle purpose, which include the prevention/deterrence of illegal activity and the enhancement of safety;

j) When video surveillance footage is being displayed by authorized employees on a video monitor, the monitors will be in a position that cannot be viewed by others.

k) The video surveillance system will be subject to periodic audit.

**Responsibilities:**

Security Guards, Dispatchers and Risk Management Staff are responsible to operate and monitor the video surveillance system(s) when and as directed.

The Security Manager is responsible to manage and coordinate maintenance of the video surveillance system(s), train employees who will access the system and ensure that the system is used in accordance with this policy.

The Director, Risk Management is responsible for oversight of the system, especially with respect to privacy issues, arranging periodic audits of the system and recommending new video installations and system upgrades through the budget process.

<table>
<thead>
<tr>
<th>Contact Officer</th>
<th>Director, Risk Management</th>
</tr>
</thead>
</table>

2
<table>
<thead>
<tr>
<th><strong>Date for Next Review</strong></th>
<th><strong>November 5, 2016</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Related Policies, Procedures and Guidelines</strong></td>
<td>Policy on the Protection of Personal Information</td>
</tr>
<tr>
<td><strong>Policies Superseded by This Policy</strong></td>
<td>N/A</td>
</tr>
</tbody>
</table>
# PROCEDURE

## CREATING AND REVIEWING UNIVERSITY POLICY

**Contact Officer**
Manager, Records & Policy

<table>
<thead>
<tr>
<th>Purpose</th>
<th>This procedure outlines specific responsibilities and protocols for managing video surveillance systems and for handling the information gathered by such systems.</th>
</tr>
</thead>
</table>
| **Procedure** | **Security Manager** Ensure all Risk Management staff and service providers are trained in the responsible operation of video surveillance systems, have read and understand this policy and understand their legal obligations under FIPPA. Video recordings contain personal information and should not be viewed by unauthorized persons.  

Ensure dispatchers, guards and Risk Management Department staff only view video information to investigate an incident, when an e-phone is activated or a call for service is received, when a safety hazard or imminent threat exists for a particular area or as directed by the Security Manager or Director, Risk Management. Employees are not to view video information for personal interest and are under no circumstances to copy or transmit video information to anyone else except as provided for explicitly in this policy.  

Ensure other university employees who may be required to view video information to perform their duties have read and understand this policy and their legal obligations under FIPPA. All persons authorized to access video information are to sign confidentiality agreements.  

Ensure the url password is changed whenever the employment of someone with access to the system is terminated and at least every year.  

Inform the Director, Risk Management, of any employees or service providers who do not comply with this policy or the Act. Also inform the Privacy Coordinator if a privacy breach has occurred, or may have occurred. |
| **Security Manager** | Ensure the video surveillance system is maintained in good working order.  

Ensure reception equipment is placed in accordance with the policy provisions regarding privacy and only in areas where they are necessary for safety or security reasons and are suitable for the conditions (exterior, interior, low light, PTZ etc.)  

If reception equipment is adjustable by operators, this practice will be restricted, wherever possible, so that operators cannot adjust or... |
| Security Manager | Where a review of record information indicates that unlawful activity has occurred or is suspected, law enforcement agencies will be brought in to view that recorded information. Video evidence will be stored securely until law enforcement responds. When a recording is seized as evidence, the name of the investigating officer and date and time of seizure will be recorded and retained in a log book, which will be retained for seven years.

Copies which are made of specific segments of recorded information for purposes of an official criminal investigation will be dated and labeled with the police occurrence number, a unique, sequential number or other verifiable symbol, and access to these copies will be limited to authorized personnel. Logs will be kept of all instances of access to, and use of, these stored copies, to provide for a proper audit trail.

These stored copies will be retained for at least one year as per section 5(1) of Ontario Regulation 460 under FIPPA. The length of this retention period may be reduced by way of formal resolution by the university or the courts.

Refer requests for access to or copies of video information to the Director, Risk Management. |
| Director, Risk Management | Assess requests for reception equipment in accordance with the following criteria:
- other measures to protect public safety, detect or deter, or assist in the investigation of criminal activity have been considered and rejected as unworkable.
- The use of each video surveillance camera should be justified on evidence based criminal or safety concerns.
- Assess the privacy implications to minimize intrusiveness.
- Consultation with stakeholders has occurred.

Recommend installations and system enhancements through the budget process.

Assess and approve or deny requests for access to or copies of video information by in consideration of: |
• Applicable laws (external requests)
• Need to know to perform authorized university functions
• The provisions of this policy

Ensure compliance with this policy.

Director, Risk Management

Arrange periodic audits of the video surveillance system to ensure compliance with this policy and procedure.

<table>
<thead>
<tr>
<th>Date Approved</th>
<th>November 5, 2013</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval Authority</td>
<td>PVP</td>
</tr>
<tr>
<td>Date of Commencement</td>
<td>November 5, 2013</td>
</tr>
<tr>
<td>Amendment Dates</td>
<td>N/A</td>
</tr>
<tr>
<td>Date for Next Review</td>
<td>November 5, 2016</td>
</tr>
<tr>
<td>Related Policies, Procedures and Guidelines</td>
<td>Policy on the Protection of Personal Information</td>
</tr>
</tbody>
</table>
NAME OF GUIDELINE

Contact Officer  Security Manager

Purpose
To provide guidelines for notifying the public of areas under video surveillance, including web postings.

Guideline
The following wording will be used on signage posted at the perimeter of all video surveillance areas. Signs will be AODA compliant.

“This area may be under video surveillance by Campus Security. Questions can be directed to 705-748-1328 or security@trentu.ca

Video files related to the use of the CCTV at this site are recorded under the authority of the Trent University Act s. 18(3).”

The Campus Security website will include the above information.

Related Policies / Procedures
Policy on the Protection of Personal Information

Links
http://www.trentu.ca/security/

Date Approved  November 5, 2013
Approval Authority  PVP