SUBJECT: VIDEO SURVEILLANCE POLICY

1. Purpose

The purpose of this policy is:

To improve personal safety on the University campus by deterring people from committing acts of harassment, assault, vandalism, and theft through the use of video technology.

2. Scope

The University recognizes the need to strike a balance between the individual's right to be free from invasion of privacy and the institution's duty to promote a safe environment for community members and protect University property.

Video surveillance technology has been in use for many years by many institutions to serve as a deterrent and to record significant events, breaches of University policy, and crimes.

This policy has been developed to comply specifically with the *Freedom of Information and Protection of Privacy* Act, Federal legislation, and to be consistent with other related University policies.

It is necessary to standardize procedures so that all members of the University community can expect consistent and ethical use and implementation of this surveillance equipment..

3. Authority / Responsibility

The University collects personal information by CCTV (Closed Circuit Television) utilizing visible and covert camera systems in accordance with sections 26 and 27 of the *Freedom of Information and Protection of Privacy* Act.

The authorization for the installation and practices lies with the Chief Financial Officer. The Chief Financial Officer can delegate responsibility for the day-to-day procedures to the appropriate Dean, Chair, or Director. A manager may be assigned the supervision of the operation of a covert camera system by the Dean, Chair, or Director. In this case the manager will administer the operations of the CCTV equipment and recorded information outlined in this policy.

4. Use of cameras

Signage will be posted indicating that surveillance cameras are in use in University Buildings and properties.

Video surveillance cameras may be used to monitor and/or record activities persons within University owned or occupied locations.

Video surveillance camera locations must be authorized by the Chief Financial Officer or designate.

Before video surveillance is introduced to a site, a report must be provided to the Chief Financial Officer explaining its necessity and identifying any less invasive options. The report must include the requestors name, position, and rationale for the request. It must identify, if camera is covert, who will be notified of the installation. .If installation is not covert, signs must be prominently displayed clearly indicating to the public that the area is under video surveillance.

If installation is for, but not limited to, a time-limited specific investigation into criminal conduct, it must be approved by the Chief Financial Officer. This will be approved only if covert surveillance is essential to the investigation and outweighs the privacy issues of those that could be observed. Covert surveillance will NOT be authorized on ongoing basis.

Generally, video surveillance is NOT to be used in locations where appropriate confidential or private activities or functions are normally carried out (e.g. washrooms, change rooms, private work areas or offices) Any exception must be approved by the University President on the basis that no other option is feasible, the need is pressing (personal safety) and the privacy rights are outweighed. Surveillance of such locations may not be authorized on an ongoing basis.

5. Security

Video surveillance cameras will be installed only by a designated employee or agent of the University, and will be approved by the Chief Financial Officer or designate. Only designated individuals shall have access to the video surveillance equipment.

The Chief Financial Officer or designate shall be responsible for designating access to the video surveillance equipment to employees or agents of the University.

Video files or images and equipment shall be stored in a locked and secure area not normally accessible to students or the public.

Recorded video files may never be sold, publicly viewed or distributed in any other fashion.

6. **Viewing of Tapes**

6.1 Monitors used to view video should not enable public viewing.

6.2 Video may only be viewed by:

- The individual authorizing camera installation;
- A University employee with a direct involvement with the recorded contents of the specific video
- Individuals responsible for technical operations of the system (for technical purposes only);
- Director and/or Manager of Campus Security

7. Retention of Video files

7.1 Video files shall be erased with in one month, unless it is retained at the request of the Chief Financial Officer, or the individual involved for documentation related to a specific incident.

7.2 Video files retained as per 7.1 shall be erased as soon as the incident in question has been resolved, with one exception. If the video has been used to make a decision about an individual, the file must be kept for a minimum of one year as per the *Freedom of Information and Protection of Privacy* Act.

8. Audit

8.1 The Chief Financial Officers office shall conduct an annual audit to ensure that this policy and regulations are being followed, and the policy reflects current legislation.