The University of British Columbia Board of Governors	**Policy No.:** **118**	**Approval Date:** xxxxx
	Responsible Executive: University Counsel	

Title:

Safety and Security Cameras

Background and Purposes:

Camera technology is employed by the University to enhance the safety and security of those who work, study, visit and live on our campuses and to protect the University's assets and property. The University is committed to using this technology in a way that respects and safeguards the privacy of members of the University community.

This policy is intended to ensure that the University implements and uses Camera Systems, and manages records created using these systems, in compliance with provincial legislation and University records management requirements.

1. General

1.1. Camera Coordinators, in consultation with the University Counsel, shall perform a coordinating role on their respective campuses in the implementation, administration, and support of this Policy by:

1.1.1. coordinating the approval of the terms of use for new or expanded Camera Systems in accordance with Sections 3.1 and 3.2 of this Policy;
1.1.2. overseeing the installation or expansion of Camera Systems;
1.1.3. providing guidance on compliance with this Policy;
1.1.4. promoting awareness by the University community on the appropriate use of Camera Systems;
1.1.5. cooperating in audits of Camera Systems conducted under Section 7.1 of this Policy; and
1.1.6. assisting, where appropriate, in the investigation of breaches and potential breaches of this Policy.

1.2. Camera Operators are responsible for the planning, installation and operation of Camera Systems within their areas of responsibility, including:

1.2.1. evaluating the need for new or expanded Camera Systems and securing approval of the terms of use for these systems in accordance with Section 3.1 and 3.2 of this Policy;
1.2.2. installing and operating their Camera Systems in compliance with this Policy, other relevant UBC policies, applicable legislation, and the terms of use approved for these systems;
1.2.3. regularly evaluating the need for their Camera Systems and, when a system is no longer required, informing the Camera Coordinator that the system is being discontinued;
1.2.4. cooperating in audits of Camera Systems conducted under Section 7.1 of this Policy;
1.2.5. ensuring the security of their Camera Systems and recorded Camera Imagery collected using these systems;
1.2.6. maintaining their Camera Systems to ensure they are working properly; and
1.2.7. designating employees or contractors who are authorized to access or operate their Camera Systems, and ensuring that these individuals are familiar with this Policy, the approved terms of use, and their legal obligation to protect personal privacy.

1.3. Breaches of this Policy may be subject to disciplinary or other actions.

1.4. Breaches of this Policy may also constitute a breach of the *Freedom of Information and Protection of Privacy Act* or other legislation, which could result in sanctions against the University or against individual staff or faculty members.

2. Acceptable Uses of Camera Systems

2.1. Camera Systems may only be used when:

2.1.1. other means for achieving the same objectives are substantially less effective than using cameras; and
2.1.2. the benefits of using cameras substantially outweigh any privacy intrusion.

2.2. Subject to Section 2.1 of this Policy, the University may use Camera Systems to monitor and/or record activities within University-owned or occupied locations:

2.2.1. to assist in the protection of individuals, assets and property;
2.2.2. to assist in the prevention and investigation of:
2.2.2.1. criminal activity, injury and property loss; and
2.2.2.2. violations of University policies related to safety and security;
2.2.3. to facilitate responses to emergencies, natural disasters, and other serious incidents;
2.2.4. to monitor traffic, facility usage, road conditions and weather related issues; and
2.2.5. for other purposes that are expressly authorized by law.

2.3. Notwithstanding Section 2.1 and 2.2 of this Policy, Camera Systems should not be used as a tool for continuous, real-time monitoring of students, staff, or faculty for the purposes of performance management or detecting academic misconduct. They may, however, be used in the investigation of allegations of misconduct provided that clear and specific grounds exist that make it necessary to use them for this purpose.

2.4. For privacy reasons, Camera Systems should be configured to collect the minimum amount of personally identifiable information necessary to achieve the purpose of the collection.

3. Approval of Terms of Use for Camera Systems

3.1. Camera Systems may not be installed or expanded until their terms of use have been approved by the relevant Camera Coordinator and the University Counsel in accordance with the Procedures. Such approval will only be granted if the Camera System complies with this Policy and other relevant policies and legislation, and may be withdrawn if the system ceases to be compliant.

3.2. Camera Operators who have a Camera System in operation on the date this Policy comes into force must seek approval of this system's terms of use in accordance with Section 3.1 of this Policy within 6 months of that date. After seeking approval, the Camera Operator may continue to operate the system until an approval decision is made, unless otherwise directed by the Camera Coordinator.

3.3. In addition to the requirement to secure approval under Section 3.1 of this Policy, Camera Systems located in areas where there is a reasonable expectation of privacy (e.g. washrooms, change rooms, private work areas, classrooms or offices), as well as Covert Cameras in all locations, must also be approved by the Vice-President, Human Resources or their designate, in consultation with any other relevant Vice-

President(s). As these uses of Camera Systems are more privacy-intrusive, they will only be approved where clear and specific grounds exist that make it necessary to use them, and only on a short-term basis.

3.4. When operating a Camera System, the Camera Operator is responsible for complying with this Policy and the terms of use approved for that system.

4. Public Awareness of Camera Systems

4.1 Except for Covert Cameras, Camera Systems must not be hidden or disguised. Signage must also be posted to notify the public of camera location(s) so that individuals have ample warning before entering a monitored area.

5. Access to Camera Systems and Camera Imagery

5.1. Camera Systems and Camera Imagery may only be accessed by individuals who are authorized by

5.1.1. the Camera Operator under Section 1.2.7 of this Policy;
5.1.2. the relevant Camera Coordinator; or
5.1.3. the University Counsel.

5.2. The Camera Operator must take reasonable steps to ensure that unauthorized individuals do not operate or disable Camera Systems or view Camera Imagery.

6. Management of Recorded Camera Imagery

6.1. The Camera Operator is responsible for the secure storage of recorded Camera Imagery. If the recorded Camera Imagery is stored in electronic format, it must be secured in a manner prescribed by the Information Security Standards approved by the Chief Information Officer under the authority of Policy 104, *Acceptable Use and Security of UBC Electronic Information and Systems.*

6.2. The Camera Operator must ensure that recorded Camera Imagery is not accessed, used or disposed of except as authorized under this Policy and its Procedures.

6.3. The Camera Operator must keep logs of all access, use, and disposal of recorded Camera Imagery.

6.4. When it is no longer required, the recorded Camera Imagery must be securely overwritten or destroyed.

6.5. Recorded Camera Imagery may not be retained for more than 30 days, with the following exceptions:

6.5.1. if it is needed to facilitate or document an investigation or legal proceeding, it may be retained for as long as required for that purpose; and
6.5.2. if it has been used to make a decision that directly affects an individual, it must be retained for at least one year from the date of that decision.

7. Auditing and Oversight of Camera Systems

7.1. The Responsible Executive must ensure that periodic audits of Camera Systems, including monitors and storage systems, are conducted to determine:

7.1.1. whether any changes need to be made in the use or configuration of the systems; and
7.1.2. whether the systems should be terminated because

7.1.2.1. their terms of use have not received the required approval;
7.1.2.2. they are not being used in accordance with the approved terms of use;
7.1.2.3. they have proven ineffective in addressing the problem they were intended to address;
7.1.2.4. the problems that justified the systems' use in the first place are no longer significant; or
7.1.2.5. there is any other reason that justifies their termination.

7.2. The Camera Coordinator and Camera Operators must promptly and effectively address any concerns that are raised by audits conducted under Section 7.1.

7.3. The Camera Coordinator will prepare annual reports on the use of Camera Systems, including non-identifying information about the use of Covert Cameras.

7.4. Audits and reports produced under Section 7.1 and 7.3 will be published on the University Counsel's website, except for information the disclosure of which could reasonably be expected to compromise privacy, safety or security.

8. Definitions

8.1. *Camera Coordinator* means the following, or their delegates:

8.1.1. the Associate Director, Risk Management and Security Services (on the Okanagan campus), and
8.1.2. the Director, Campus Security (on the Vancouver campus).

8.2. *Camera Imagery* means images captured using Camera Systems.

8.3. *Camera Operators* means the heads of University units that operate Camera Systems.

8.4. *Camera System* means any camera installation that is intended to capture information about identifiable individuals, but for greater clarity does not include systems used exclusively for:

8.4.1. communication purposes, such as videoconferencing systems;
8.4.2. academic instruction;
8.4.3. traffic monitoring or control; and
8.4.4. any purposes where the system is configured to prevent the capture of identifiable images of individuals.

8.5. *Covert Cameras* are cameras that are used without notification to the public or the persons being viewed.

PROCEDURES

Approved: [DATE]

Pursuant to Policy #1: Administration of Policies, "Procedures may be amended by the President, providing the new procedures conform to the approved policy. Such amendments are reported at the next meeting of the Board of Governors." Note: the most recent procedures may be reviewed at http://universitycounsel.ubc.ca/policies/index/.

1. Approval Procedure for Installation or Expansion of Video Surveillance

1.1. Under Section 3 of the Policy, Camera Operators who wish to install or expand a Camera System must submit draft terms of use for that system to the Camera Coordinator for approval. These terms of use should include the following information:

1.1.1. Rationale
- 1.1.1.1. The purpose/objective for installing these cameras.
- 1.1.1.2. The necessity for the use of cameras in this area.
- 1.1.1.3. What less privacy-intrusive alternatives to the use of cameras have been considered and why they have been rejected.

1.1.2. Scope
- 1.1.2.1. Description of area(s) to be monitored and placement of cameras, including diagrams where feasible.
- 1.1.2.2. How many cameras will be installed.
- 1.1.2.3. Whose activities will be viewed by these cameras (e.g. public, employees, students).

1.1.3. Privacy
- 1.1.3.1. How the cameras have been positioned to ensure that there is minimal intrusion to personal privacy.
- 1.1.3.2. How individuals will be notified that they are entering an area that is being monitored.

1.1.4. Security of Camera Imagery
- 1.1.4.1. Arrangements in place to protect against unauthorized viewing of the Camera Imagery.
- 1.1.4.2. How the recorded Camera Imagery will be stored.
- 1.1.4.3. The protocol for accessing and viewing the recorded Camera Imagery.
- 1.1.4.4. Technical and physical security arrangements in place to protect against unauthorized access or disclosure of the recorded Camera Imagery.
- 1.1.4.5. The protocol for logging access, use and disposal of the recorded Camera Imagery.

1.2. Before approving the draft terms of use, the Camera Coordinator will consult with the University Counsel or their designate to ensure that these terms of use comply with this Policy, the *Freedom of Information and Protection of Privacy Act*, and any other relevant policies or legislation.

2. Requests for Access to Recorded Camera Imagery

2.1. Requests for recorded Camera Imagery from University employees acting in the course of their duties will be processed by the Camera Operator, who may disclose the requested information on a "need-to-know" basis for any of the purposes set out in Section 2.2 of the Policy.

2.2. Requests for recorded Camera Imagery from public bodies or law enforcement agencies in Canada will be processed by the Camera Coordinator, who may disclose the requested information if

2.2.1 the requester has express legal authorization to receive the information; and/or
2.2.2 the request is made to assist in a specific investigation undertaken with a view to a law enforcement proceeding, or from which a law enforcement proceeding is likely to result.

2.3. All other requests for recorded Camera Imagery will be processed by the University Counsel or their delegate under the terms of the *Freedom of Information and Protection of Privacy Act*.