The University of British Columbia Board of Governors	**Policy No.:** **118**	**Approval Date:** February 15, 2016
	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 camera systems that are operated by the University, and are configured to capture identifiable images of individuals, are implemented and used in compliance with provincial legislation and University records management requirements.

1. Scope

1.1. This Policy governs the use of all University-operated Camera Systems that are configured to capture identifiable images of individuals, with the exception of systems used for the following purposes:

1.1.1. communications, such as videoconferencing systems;
1.1.2. technical support of information technology, audiovisual and other systems;
1.1.3. academic instruction;
1.1.4. research projects that have received ethics approval;
1.1.5. monitoring traffic, facility usage, road and weather conditions; and
1.1.6. occasions where all individuals whose images may be captured have provided their informed consent.

1.2. All uses of camera systems, including those that fall outside the scope of this Policy, are subject to applicable policies and legislation, including the *Freedom of Information and Protection of Privacy Act* (FIPPA).

1.3. Breaches of this Policy may be subject to disciplinary or other actions, and may also constitute a breach of the FIPPA or other legislation, which could result in sanctions against the University or individuals.

2. Acceptable Uses of Camera Systems

2.1. Subject to Sections 2.2 and 2.3 of this Policy, the University may use Camera Systems to monitor and/or record activities within University-owned or occupied locations:

2.1.1. to assist in the protection of individuals, assets and property;
2.1.2. to assist in the prevention and investigation of:
2.1.2.1. criminal activity, injury and property loss; and

2.1.2.2. violations of University policies related to safety and security;
2.1.3. to facilitate responses to emergencies, natural disasters, and other serious incidents; and
2.1.4. for other purposes that are expressly authorized by law.

2.2. In accordance with section 26(c) of the FIPPA, the University may only collect personally identifying information using Camera Systems when the information relates directly to and is necessary for one or more of the objectives set out in Section 2.1 of this Policy, and only under the following conditions:

2.2.1. other means for achieving the same objectives are substantially less effective than using cameras;
2.2.2. the benefits of using cameras substantially outweigh any privacy intrusion; and
2.2.3. the cameras have been configured to collect the minimum amount of personally identifiable information necessary to achieve the purpose of the collection.

2.3. In accordance with section 32(a) of the FIPPA, the University may only use personally identifying information collected by Camera Systems for one of the objectives set out in Section 2.1 of this Policy, or for a use consistent with those objectives.

2.4. For greater clarity, Camera Systems must not be used as a tool to monitor students, staff, or faculty for the purposes of performance management or detecting academic misconduct.

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 in writing by the relevant Camera Coordinator and the Responsible Executive, in accordance with the Procedures. Such approval will only be granted if the Camera System complies with this Policy, the FIPPA, and any 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, Privacy-Intrusive Camera Systems must also be approved in writing by the Vice-President, Human Resources or their designate, in consultation with any other relevant Vice-President(s).

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. Privacy-Intrusive Camera Systems

4.1. Privacy-Intrusive Camera Systems will only be approved in rare and exceptional cases where clear and specific grounds exist that make it necessary to use them, and only where there is:

4.1.1. a substantial problem justifying their use;
4.1.2. a strong possibility that their use will be effective;
4.1.3. no reasonable alternative to their use in all of the circumstances; and
4.1.4. in the case of Covert Cameras, a reasonable expectation that notification would compromise an investigation or proceeding, or the availability or accuracy of the information to be collected.

4.2. Privacy-Intrusive Camera Systems must be discontinued at the earliest available opportunity. They will only be approved for a maximum period of 6 months, after which the Camera Operator may seek an extension under the approval process set out in Section 3 of this Policy.

5. Public Awareness of Camera Systems

5.1. 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. Where practicable, this signage must provide an internet address for the public notification described in Section 5.2 of this Policy.

5.2. The University must post a public notification on its website of the purpose(s) for the use of its Camera Systems; the legal authority for the collection of information using these Camera Systems; and the title, business address, business telephone number and email address of an employee who can answer questions about the collection.

6. Access to Camera Systems and Camera Data

6.1. Subject to Sections 6.6, 6.7, 6.8, and 6.9 of this Policy, Camera Systems and Camera Data may only be accessed by University employees or contractors who have been authorized to access or operate their Camera Systems by the Camera Operator under Section 8.2.7 of this Policy.

6.2. The Camera Operator is responsible for the secure operation of Camera Systems and the secure storage of recorded Camera Data in accordance with 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*.

6.3. The Camera Operator must keep logs of all access, use, and destruction of recorded Camera Data.

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

6.5. Recorded Camera Data 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 after the date of that decision.

6.6. Requests for recorded Camera Data 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 2.1 of the Policy.

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

6.7.1. the requester has express legal authorization to receive the information; and/or

6.7.2. 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.

6.8. Notwithstanding Section 2.1 of this Policy, the Responsible Executive may authorize the disclosure and use of recorded Camera Data for the purpose of investigating allegations of serious violations of University policy or statutory obligations.

6.9. All other requests for recorded Camera Data will be processed by the Responsible Executive under the terms of the FIPPA.

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, which shall include, for each Covert Camera installation, non-identifying information about the duration and general location of the installation. The Responsible Executive may establish additional requirements for the content and/or format of these reports.

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

8. Administrative Responsibilities

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

- 8.1.1. coordinating the approval of the terms of use for new or expanded Camera Systems in accordance with Sections 3.1, 3.2 and 3.3 of this Policy;
- 8.1.2. overseeing the installation or expansion of Camera Systems;
- 8.1.3. providing guidance on compliance with this Policy;
- 8.1.4. promoting awareness by the University community on the appropriate use of Camera Systems;
- 8.1.5. cooperating in audits of Camera Systems conducted under Section 7.1 of this Policy; and
- 8.1.6. assisting, where appropriate, in the investigation of breaches and potential breaches of this Policy.

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

- 8.2.1. 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, 3.2 and 3.3 of this Policy;

8.2.2. 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;
8.2.3. 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;
8.2.4. cooperating in audits of Camera Systems conducted under Section 7.1 of this Policy;
8.2.5. ensuring the security of their Camera Systems and recorded Camera Data collected using these systems;
8.2.6. maintaining their Camera Systems to ensure they are working properly; and
8.2.7. 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.

9. Definitions

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

9.1.1. the Associate Director, Risk Management and Security Services (on the Okanagan campus), and
9.1.2. the Director, Campus Security (on the Vancouver campus and other University sites).

9.2. *Camera Data* means information captured using Camera Systems.

9.3. *Camera Operators* means the heads of University units that operate Camera Systems, or their delegates.

9.4. *Camera System* means any camera installation, except for one that is configured to prevent the capture of identifiable images of individuals.

9.5. *Covert Cameras* are Camera Systems that are used without notification to the public or the persons being viewed.

9.6. *Privacy-Intrusive Camera Systems* are:

9.6.1. Camera Systems located in areas where there is a reasonable expectation of privacy (e.g. washrooms, change rooms, private work areas, classrooms or offices), and
9.6.2. Covert Cameras in all locations.

9.7. *Responsible Executive* means the University Counsel, or their delegates.

PROCEDURES

Approved: February 15, 2016

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. Elements of Terms of Use for Camera Systems

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).
- 1.1.2.4. What types of Camera Data will be captured (i.e. video, audio or both).
- 1.1.2.5. Any special capabilities of the system (e.g. zoom, facial recognition or night vision features).

1.1.3. Privacy
- 1.1.3.1. How the cameras have been positioned or configured to collect the minimum amount of personally identifiable information necessary to achieve the purpose of the collection.
- 1.1.3.2. How individuals will be notified that they are entering an area that is being monitored.
- 1.1.3.3. Whether and when the cameras will be monitored in real time.
- 1.1.3.4. Whether and when recording of Camera Data will occur.

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