VIDEO SURVEILLANCE POLICY

Policy Type:	Institutional	**Initially Approved:**	April 8, 2025
Policy Sponsor:	Vice President, Finance and Operations	**Last Revised:**	April 8, 2025
Responsible Unit:	Campus Operations	**Review Scheduled:**	April 2028
Approver:	President and CEO		

A. PURPOSE

The Alberta University of the Arts (AUArts) utilizes Video Surveillance as part of its security operations to enhance the safety and security of the University Community, as well as to protect University property. This policy sets out responsible use of the Video Surveillance in compliance with applicable municipal, provincial, and federal privacy legislation. AUArts is committed to balancing security needs with individuals' rights to privacy and ensuring that Video Surveillance is conducted in a lawful, ethical, and transparent manner.

B. SCOPE

This policy applies to all individuals involved in the operation, maintenance, and oversight of Video Surveillance at AUArts, including University employees, contracted security personnel, and third-party service providers. It is relevant to all members of the AUArts community, including students, faculty, staff, visitors, and other users of University facilities.

Use of video surveillance technology for research purposes is not covered by this Policy and must adhere to the Research Ethics Board Policy and Procedure.

C. POLICY STATEMENT

1. PURPOSE FOR SURVEILLANCE

1.1 The use of Video Surveillance is intended to:

a) Enhance the safety and security of the university community by deterring unlawful or disruptive behavior on university premises.
b) Support a safe and secure environment for students, faculty, staff, and visitors.
c) Assist in responding to observed or reported security incidents in a timely and effective manner.

2. VIDEO SURVEILLANCE EQUIPMENT SET-UP AND MAINTENANCE

2.1 The installation, use, disabling, or disconnection of video surveillance equipment must be approved by the Director of Campus Operations, with authorization from the President & CEO and consultation with the Privacy Officer.

2.2 Campus Operations, in consultation with Campus Technology Services (CTS), is responsible for the installation and configuration of all video surveillance equipment. Recorded footage will be stored on a secured server.

2.3 Campus Operations is responsible for the regular testing, maintenance, and repair of video surveillance equipment. Routine checks will be conducted to ensure that the equipment is functioning properly, including verification of recording quality, proper time and date stamping, and compliance with operational standards.

2.4 Video Surveillance receiving equipment (e.g., monitors, laptop) will be placed in a secure, controlled-access area that is not visible to the public. Access to these systems will be restricted to authorized personnel only.

3. USE AND MONITORING OF RECORDINGS OBTAINED THROUGH VIDEO SURVEILLANCE

3.1 All Public Areas of the University are subject to Video Surveillance. Surveillance will not be placed in or on areas in which individuals have a reasonable expectation of privacy, including but not limited to washrooms.

3.2 Video Surveillance is used for purposes related to safety, security of individuals, and the protection of university property, including:

a) monitoring building perimeters, entrances, exits, lobbies, corridors, receiving docks, storage areas, areas where University-related activities, functions, performances and events are held, and other high-risk areas;
b) verifying security, fire, emergency, and other alarms or alerts;
c) conducting video patrols of public areas integrated with University property;
d) assisting criminal and other law enforcement investigations and proceedings, legal proceedings and internal investigations and proceedings under applicable University policies, including but not limited to the *Code of Conduct Policy, Respectful Workplace Policy, Gender-based and Sexual Violence Policy, Student Conduct Policy, Health and Safety Policy* and the *Fraud and Irregularity Procedure;*
e) assessing and analyzing data related to the use of University property to support campus planning, facility management, and developing or otherwise managing University property and security.

3.3 Video Surveillance equipment may be installed in private offices where there is a verified security concern, and only with the written consent of the office occupant(s) and approval from the Director of Campus Operations

3.4 The Director of Campus Operations, or their designate are authorized to access Video Surveillance remotely in accordance with purposes outlined in Section 3.2. and 3.3 remote access must be conducted in a private space utilizing the University's secure network connection.

3.5 Video monitoring will not be used to monitor employee or student performance.

3.6 Live video feeds, displayed in real-time or with minimal delay, will be monitored by authorized campus security personnel and recorded using an Internal Protocol Camera system. Due to the inherent limitations of surveillance

technology, video monitoring should not be relied upon as a sole security measure but rather as one component of AUArts' comprehensive security strategy.

3.7 Access to video surveillance footage is restricted to authorized personnel within Campus Operations. The Director of Campus Operations, or a designated individual, will ensure that authorized personnel receive appropriate training on privacy obligations, data security, and the responsible use of surveillance systems. Misuse of Video Surveillance equipment or records will result in disciplinary action.

3.8 If an incident involving potential misconduct is observed during regular monitoring of Video Surveillance, the Director, Campus Operations, will notify the relevant unit and confirm the existence of the video footage.

4. PUBLIC NOTICE AND SIGNAGE

4.1 Signage is prominently displayed at the University at appropriate locations, including general entrances, to provide individuals with notice that:

a) there may be Video Surveillance cameras in all public areas of campus, that may be used to record and monitor activity,
b) personal information collected through Video Surveillance may be used or disclosed for Public Security Purposes,
c) individuals may contact Campus Operations should they require additional information or have concerns regarding Video Surveillance,
d) the collection of personal information is authorized in accordance with applicable laws,
e) The contact information identifying an individual who can answer questions about Video Surveillance.

5. ACCESS TO RECORDS

5.1 Recorded images from Video Surveillance are classified as confidential information and Internal Use-Protected in accordance with the Information Classification Procedure.

5.2 The Director of Campus Operations is the Records Custodian responsible for the supervision of Video Surveillance records.

5.3 All Video Surveillance records are stored and accessed in a restricted-access server area. Access to this space is restricted to authorized members of the University's Campus Operations and Information Technology Services personnel.

5.1 Requests for Video Surveillance records may be submitted in writing to the Director of Campus Operations and may be routinely disclosed only if the applicant demonstrates a legitimate right of access to the information in accordance with applicable policy and/or legislation.

5.2 Disclosure will be documented and will include the name of the individual to whom the information is disclosed and the date and time of access, removal, or copying.

a) If the Video Surveillance records being requested captures additional third parties, the requestor has the right to submit a formal access-to-information request.

6. RETENTION PERIOD

6.1 Recorded images will be deleted after 35 calendar days unless needed for a law enforcement purpose.
6.2 Recordings viewed for any purpose other than that referenced in 6.3 will be retained for a minimum period of one year from completion of use.
6.3 Where the recording forms part of the evidence in court or tribunal proceedings, recordings will be kept for a minimum of one year following final disposition of the matter including any court reviews and appeals.

D. DEFINITIONS

Disclosure:	refers to the release of relevant information. Disclosure includes viewing a recording as well as making a copy of a recording.
Law Enforcement:	means policing, including but not limited to, criminal investigations or proceedings having the potential of leading to penalties or sanctions.
Privacy Officer	A role within the Office of the Secretariat responsible for privacy practices ensuring compliance with relevant laws and regulations and serving as the point of contact for privacy-related issues.
Public Areas	means any area of campus including but not limited to building perimeters, entrances, exits, lobbies, corridors receiving docks, storage areas, and areas where activities, functions, performances and events are held in other high-risk areas.
Public Security Purpose:	means a use or Disclosure relating to disciplinary, legal or public safety and security purposes or in accordance with any court order of subject to the University's policies or procedures or applicable legislation.
University:	means Alberta University of the Arts.
University Community	includes AUArts Board of Governors, faculty, staff, students, third-party agents, volunteers and persons visiting the University campus.
Video Surveillance:	means a network-based video surveillance system that uses Internet Protocol (IP) cameras to capture and transmit digital video footage over a local secure network, allowing authorized users to monitor video feed for observing and monitoring space.

E. RELATED POLICIES

- Access to Information and Protection of Privacy Policy
- Code of Conduct Policy
- Gender-based and Sexual Violence Policy
- Health and Safety Policy
- Information Security Policy
- Respectful Workplace Policy
- Student Conduct Policy

F. RELATED LEGISLATION

- Alberta, Freedom of Information and Protection of Privacy Act

G. RELATED DOCUMENTS

- Fraud and Irregularity Procedure
- IT: Backup, Retention and Disposal Procedure
- IT: Information Classification Procedure

H. REVISION HISTORY

Date (mm/dd/yyyy)	Description of Change	Sections	Person who Entered Revision (Position Title)	Person who Authorized Revision (Position Title)
04/08/2025	New Policy	All	Director, Campus Operations	Vice President, Finance and Operations