8.7 Video Surveillance Policy

Purpose
To regulate the use of video surveillance and recording on BACI premises (owned and leased). Information obtained through video surveillance will be used exclusively for health and safety, or security and law enforcement purposes, which must relate to the protection of persons served, staff and the general public, or the deterrence or detection of criminal activity, including theft, vandalism, or other property damage.

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 BACI 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.

Scope
This policy applies to video surveillance activities necessary to enhance the health and safety of individuals (persons served, staff, and the public) on BACI premises, and the security of BACI buildings and property.

Prohibited Areas
Cameras are prohibited in washrooms, changing rooms, bedrooms, and any space with a high expectation of privacy. Cameras must not be positioned to capture images of adjacent properties or through windows into private spaces.

Permitted Areas

- Video surveillance may be used to monitor exterior and interior areas of BACI property where there is: No reasonable expectation of privacy.
- Limited expectation for privacy (shared living spaces exclusive of bathrooms).
- An expectation for privacy that is balanced by health and safety expectations.

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

- Video surveillance will be used only where it is demonstrably necessary for the purposes of enhancing the health and safety of persons, or for the deterrence of theft or destructive acts, such as vandalism and graffiti.
- Surveillance 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 principal purpose, which includes the prevention/deterrence of illegal activity and the enhancement of health and safety of persons served and staff.
- Video surveillance must be authorized by the Chief Executive Officer (CEO) and only where less intrusive means of monitoring and deterrence have been shown to be ineffective or unworkable.
- Appropriate signs and notices of video surveillance will be posted in areas subject to video monitoring with consideration of the privacy and confidentiality of persons served residing on the premises.
- Employees and video service providers who require access to information collected through video surveillance will be provided with proper training and orientation regarding this Policy.
- The recording medium must be handled in a manner that maintains the integrity and security of the recorded information. Recordings are stored in encrypted repositories (on location) or hosted in Canadian data centers.

Retention Schedule
Video surveillance recordings will be retained for the following periods based on location type:

- **Program Locations:** Recordings will be retained for a maximum of seventy-two (72) hours. After this period, recordings will be automatically overwritten or securely deleted unless flagged for retention due to a documented incident, investigation, or legal requirement.
- **Administrative Locations:** Recordings will be retained for a maximum of thirty (30) days. After this period, recordings will be automatically overwritten or securely deleted unless flagged for retention due to a documented incident, investigation, or legal requirement.

Where a recording is flagged for extended retention, the reason must be documented in writing by the Senior Manager of IT or the Privacy Officer. Extended retention will be

reviewed every ninety (90) days, and recordings will be securely deleted once the documented need no longer exists.

All deletions, whether automatic or manual, must comply with BACI's records management practices and applicable privacy legislation, including PIPEDA and the BC Personal Information Protection Act (PIPA).

Access Permissions

Access to video surveillance systems and recorded footage is restricted to authorized personnel only. The following controls apply:

- Access permissions will be granted by the Senior Manager of IT, Privacy Officer, or CEO, based on operational need and role requirements. Only staff with a demonstrated, documented need will be provided access to surveillance systems or recordings.
- A current register of all staff and devices granted access to video surveillance systems will be maintained on the Senior Manager's SharePoint site. The register will include the staff member's name, role, date access was granted, and the scope of access provided.
- The access register will be reviewed annually by the Senior Manager of IT, in consultation with the Privacy Officer and CEO, to confirm that all active permissions remain appropriate and aligned with current operational needs.
- Access will be revoked promptly when a staff member changes roles, leaves the organization, or no longer requires access for their duties.
- Any unauthorized access to, or misuse of, video surveillance systems or recordings will be treated as a breach of this policy and may result in disciplinary action up to and including termination.

Responsibilities

Any employee who knowingly or deliberately breaches this policy will be subject to discipline up to and including termination. Failure of a video service provider to comply with this policy will constitute breach of contract and may result in termination of contract and legal action.

Staff assigned by the CEO are responsible for operating and monitoring the video surveillance system(s) as directed:

- The Senior Manager of IT is responsible for oversight of the system and coordinating maintenance of the video surveillance system(s) and training employees who will access the system.
- BACI's Privacy Officers are responsible for ensuring that the system is used in accordance with this policy, particularly with respect to privacy issues.

- Video surveillance with respect to the Rights and Behavioral Intervention policy will be implemented in consultation with the CEO, the Privacy Officer, the designated Senior Manager and the Senior Manager of Quality Assurance.
- The Privacy Officer is responsible for ensuring that the video surveillance complies with BACI's policies and regulations, particularly regarding personal privacy.

Linking Policies

1.8 Code of Ethics
1.11 Risk Management Policy
1.12 Corporate Responsibility Policy
8.1 Privacy Protection for Individuals
8.3 Privacy Protection for Employees
9.7 Behavioural Interventions