



VIDEO SURVEILLANCE POLICY

Policy Type:	Administration	Initially Approved:	07/27/2026 BCM WFN 26/27-07-101
Policy Sponsor:	Administration	Last Revised:	
Primary Contact:	Executive Director	Review Scheduled:	07/2027
Approver:	Chief and Council BCM WFN 26/27-07-101		

1.0 POLICY STATEMENT

Wahnapitae First Nation (WFN) is committed to providing a safe, secure, and welcoming environment for its Members, employees, elected officials, contractors, volunteers, tenants, visitors, and guests while respecting the privacy of individuals.

The use of video surveillance systems supports the protection of WFN employees, community members, facilities, infrastructure, public spaces, campgrounds, and other Nation-owned assets. Surveillance technology is intended to deter criminal activity, promote public safety, assist with investigations, and protect the interests of the Nation.

WFN recognizes that video surveillance involves the collection of personal information. Accordingly, surveillance systems shall only be used where there is a legitimate operational or security purpose and shall be administered in a manner that balances community safety with individual privacy.

2.0 PURPOSE

The purpose of this Policy is to establish standards governing the installation, operation, management, access, retention, and disclosure of video surveillance systems owned or operated by WFN.

This Policy is intended to:

- Enhance the safety and security of Members, employees, visitors, contractors, and the public.
- Protect WFN-owned buildings, infrastructure, vehicles, equipment, campgrounds, and other assets.
- Deter vandalism, theft, trespassing, violence, and other unlawful activities.
- Assist in the investigation of security incidents, workplace incidents, criminal activity, and policy violations.
- Establish clear accountability regarding the use and management of surveillance footage.
- Ensure surveillance technology is used responsibly, transparently, and only for legitimate operational purposes.

3.0 SCOPE

This Policy applies to all video surveillance systems, including Automatic Licence Plate Recognition (ALPR) technology, that are owned, leased, or operated by WFN. It applies to all WFN departments, employees, elected officials, contractors, consultants, volunteers, students, tenants, visitors, and any other individuals who access or are present on WFN-owned or controlled properties where video surveillance is in operation.

This Policy governs the use, management, access, retention, and disclosure of surveillance recordings captured at WFN administrative offices, community buildings, campgrounds, public infrastructure, parking areas, community entrances, and any other locations approved by the Executive Director for legitimate operational, safety, or security purposes.

4.0 DEFINITIONS

Automatic Licence Plate Recognition (ALPR)	means a camera system capable of capturing and electronically recording licence plate information for authorized security and public safety purposes.
Authorized Personnel	means individuals designated by the Executive Director who are permitted to access surveillance equipment or recordings in accordance with this Policy.
Personal Information	means recorded information about an identifiable individual collected through video surveillance.
Surveillance Footage	means any video recording, still image, digital recording, or associated data captured by a WFN surveillance system.
Video Surveillance System	means any camera, recording device, monitoring equipment, or related technology used to observe or record activity on WFN property.

5.0 GUIDING PRINCIPLES

WFN is committed to using video surveillance in a manner that supports the safety and security of the community while respecting the privacy and dignity of individuals. Surveillance systems shall only be used where there is a legitimate operational, safety, or security need and where the benefits of surveillance outweigh any impact on personal privacy.

Video surveillance shall be operated in a fair, transparent, and accountable manner. WFN will

make reasonable efforts to notify individuals when they are entering areas under surveillance through the use of clearly visible signage and other appropriate means of communication. Surveillance systems shall not be used for personal purposes or in a manner that is discriminatory, arbitrary, or inconsistent with this Policy.

The collection, use, retention, access, and disclosure of surveillance recordings shall be limited to what is reasonably necessary to achieve the purposes outlined in this Policy. Access to surveillance systems and recordings shall be restricted to authorized personnel and all recordings shall be treated as confidential information. Video surveillance is intended to protect the community, employees, visitors, facilities, and other WFN assets and shall not be used for routine monitoring of employee performance.

WFN recognizes that individuals have a reasonable expectation of privacy in certain locations. Accordingly, surveillance equipment shall not be installed or operated in areas where privacy is reasonably expected, and every effort shall be made to ensure surveillance activities are conducted in the least intrusive manner possible while still meeting legitimate operational and security objectives.

6.0 PRINCIPLES OF USE

Video surveillance shall be used solely for legitimate operational purposes including community safety, security, and the protection of WFN property.

Video surveillance is not intended to monitor employee productivity or routine work performance.

However, surveillance footage may be reviewed where there is reasonable cause to investigate:

- Criminal activity;
- Theft;
- Vandalism;
- Trespassing;
- Workplace violence;
- Workplace health and safety incidents;
- Policy violations;
- Damage to WFN property;
- Insurance claims; or
- Other legitimate operational matters approved by the Executive Director.

Surveillance systems shall not be used for personal purposes or any purpose inconsistent with this Policy.

7.0 Video Surveillance Locations

Video surveillance systems may be installed and operated at locations where WFN has determined there is a legitimate operational, safety, or security need. Surveillance locations shall be selected based on the protection of employees, Members, visitors, community infrastructure, and WFN property while minimizing impacts on individual privacy.

Video surveillance may be used at, but is not limited to:

- Community entrances and exits;
- Administrative offices and community facilities;
- Public Works facilities;
- Campgrounds and recreational areas;
- Parking lots;
- WFN-owned buildings and infrastructure;
- Storage compounds;
- Other locations approved by the Executive Director.

The installation of additional surveillance cameras shall be based on operational need and approved by the Executive Director or Chief and Council where appropriate.

8.0 Automatic Licence Plate Recognition (ALPR)

WFN may utilize Automatic Licence Plate Recognition (ALPR) technology at approved surveillance locations to enhance community safety, protect WFN assets, and assist with lawful investigations.

ALPR technology may be used to:

- Monitor vehicle traffic entering or exiting the community;
- Assist in investigations involving theft, vandalism, trespassing, or other criminal activity;
- Support investigations involving excessive speeding or other public safety concerns;
- Assist emergency response personnel during emergency situations;
- Protect WFN infrastructure and facilities; and
- Support other lawful operational or security purposes authorized by WFN.

Licence plate information collected through ALPR technology shall only be accessed by authorized personnel for legitimate operational purposes and shall not be used for personal monitoring or unauthorized purposes.

9.0 Signage and Public Notification

WFN is committed to ensuring transparency regarding the use of video surveillance.

Clearly visible signage shall be posted at community entry points where surveillance is in operation and at surveillance locations wherever reasonably practicable.

Signage shall clearly indicate that video surveillance is in use and that recordings may be collected for the purposes of public safety, security, crime prevention, and the protection of WFN property.

Where new surveillance systems are installed, WFN shall make reasonable efforts to notify employees and, where appropriate, the community of the purpose and general location of the surveillance system.

10.0 Privacy Protections

WFN recognizes the importance of respecting the privacy of individuals while maintaining a safe and secure community.

Video surveillance systems shall be operated in a manner that limits the collection of personal information to what is reasonably necessary to achieve the purposes identified in this Policy.

Surveillance recordings shall only be viewed, copied, disclosed, or retained where authorized under this Policy or as otherwise required by law.

Video surveillance shall not be used to monitor individuals for personal reasons or for any purpose unrelated to the legitimate operations of WFN.

11.0 Prohibited Locations

Video surveillance shall not be installed in areas where individuals have a reasonable expectation of privacy.

This includes, but is not limited to:

- Washrooms;
- Change rooms;
- Shower facilities;
- Wellness or counselling rooms;
- Medical examination or treatment areas;
- Private accommodation; and
- Any other location where surveillance would be considered unreasonable or unnecessarily intrusive.

Any exception to this section must be supported by a compelling operational or legal requirement and approved by Chief and Council following consultation with the Executive Director and, where appropriate, legal counsel.

12.0 Access to Surveillance Recordings

Access to surveillance systems and recordings shall be limited to personnel authorized by the Executive Director. The Executive Director shall have primary authority over surveillance recordings and may authorize access to designated Directors or other employees where operationally necessary.

Surveillance recordings shall be reviewed by no fewer than two authorized individuals. Unless otherwise approved, the review shall be conducted by the Executive Director and the Chief, or by the Executive Director and a secondary authorized designate where the Chief is unavailable or where another reviewer is more appropriate to the circumstances. Requiring at least two authorized individuals for access to recorded material is consistent with a recognized control used in some video surveillance policies to strengthen accountability over viewing and use of recordings.

Requests to access or review surveillance footage shall be submitted to the Executive Director or designate as soon as practicable after the incident or concern is identified. WFN shall make reasonable efforts to review or provide authorized access to relevant footage within two (2) business days of receiving the request, provided the request relates to a legitimate purpose under this Policy and the footage is still retained.

Chief and Council may be granted access to surveillance recordings on a case-by-case basis where there is a legitimate governance, legal, or operational purpose.

Surveillance recordings shall only be viewed where reasonably necessary to:

- Investigate criminal activity;
- Investigate theft, vandalism, trespassing, or damage to WFN property;
- Investigate workplace incidents or health and safety concerns;
- Investigate alleged policy violations or misconduct;
- Support insurance claims;
- Respond to legal proceedings or court orders;
- Assist law enforcement agencies; or
- Address other legitimate operational matters approved by the Executive Director.

Whenever practical, a record shall be maintained identifying the individuals who accessed or reviewed surveillance footage, the date of access, the reason for the review, and the names of both reviewers. Maintaining documented access records is also consistent with common video surveillance policy controls for authorized viewing and accountability.

13.0 Disclosure of Surveillance Recordings

Surveillance recordings are confidential and shall not be disclosed except where authorized by this Policy or required by law.

Recordings may be disclosed to:

- Law enforcement agencies;
- Legal counsel acting on behalf of WFN;
- Insurance providers or investigators;
- Courts or tribunals;
- Government agencies with lawful authority; or
- Other parties authorized by the Executive Director in consultation with legal counsel, where appropriate.

Requests from Members of the public or other individuals seeking access to surveillance recordings shall be submitted through the Executive Director or designate and will be considered in accordance with applicable legislation and WFN policies.

14.0 Retention of Recordings

Surveillance recordings shall normally be retained for a period of thirty (30) days, after which they will be securely deleted or overwritten, unless they are required for an active investigation, legal proceeding, insurance claim, or other authorized purposes. Recordings retained for these

purposes shall be securely maintained until the matter has been concluded.

Any person seeking review of footage should submit the request as soon as possible, and preferably within the standard retention period

15.0 Non-Compliance

Unauthorized access to, disclosure of, copying, alteration of, or misuse of surveillance systems or recordings is strictly prohibited.

Any employee, contractor, volunteer, or other authorized user who violates this Policy may be subject to disciplinary action, up to and including termination of employment or contract, and where appropriate, referral to law enforcement authorities.

Any person found intentionally damaging, disabling, obstructing, or tampering with surveillance equipment may be subject to legal action and any other remedies available to WFN.

16.0 Review, Amendments, and Revision History

This Policy shall be reviewed annually to ensure it remains effective, relevant, and consistent with operational requirements and applicable legislation.

Minor or administrative amendments to this policy that do not alter its intention or core criteria may be made with the approval of the Executive Director, without requiring formal review or approval by Chief and Council.

REVISION HISTORY

Date (mm/dd/yyyy)	Band Council Motions