City of St. John's

Electronic Surveillance Policy

Policy #

ST. JOHN'S

Contents

CITY OF ST. JOHN'S CORPORATE AND OPERATIONAL POLICY MANUAL	
Policy Title: **Electronic Surveillance Policy**	Policy #:
Last Revision Date: **06 June 2012**	Policy Section: **05-01-15**
Policy Sponsor: **Manager Emergency Preparedness and Business Continuity**	

1. POLICY STATEMENT

1.1 PURPOSE

To provide a balanced approach between the protection of privacy and the need for a safe and secure environment through the provision of guidelines for the use of Electronic Surveillance on City of St. John's owned or occupied facilities or properties, and in compliance with the Privacy Act, Access to Information and Protection of Privacy Act, 2015, and other applicable legislation. This policy governs the installation and operation of equipment, the collection and use of personal information and the custody, control, retention, dissemination and disposal of information obtained through electronic surveillance.
In any instance where this policy contradicts approved legislation, the legislation shall take precedence.

1.1.1 USE OF ELECTRONIC SURVEILLANCE INFORMATION

The information collected through Electronic Surveillance shall be used:

a) To assess the effectiveness of safety and security measures.
b) To investigate an incident involving the safety and security of people, facilities or assets.
c) To provide evidence in a legal matter.

1.1.2 INSTALLATION, RETENTION AND CONTROL

a) All electronic surveillance installations shall be approved by the City Manager. Signs will be posted where electronic surveillance is in place. The signage shall state that the surveillance is being conducted by City of St. John's and direct enquiries to 311.
b) Usage of a mobile device to capture images, video or audio. Refer to Policy: 02-01-14, Use of Mobile Devices in the Workplace Sec 4.3 (f)
c) Covert electronic surveillance will not be installed in City facilities unless it is associated with an investigation which may result in legal action.
d) Only personnel who are authorized by Council shall have access to the electronic surveillance monitors or to the data obtained through electronic surveillance.
e) Personal information shall not be disclosed except in accordance with applicable legislation.
f) The City of St. John's as well as agencies, boards and commissions over which the City has authority shall maintain a record detailing who has accessed electronic surveillance data; if that

data has been disclosed; the authority under which data has been disclosed; and to whom the data has been disclosed. **(Appendix "A")**

g) All breaches or perceived breaches must be reported to the Office of the City Clerk so that it can be reported to the Office of the Information and Privacy Commissioner as required under the Access to Information and Protection of Privacy Act, 2015.

h) All electronic surveillance data containing "Personal Information" may have a retention period of up to Ninety (90) days from the date of recording except as outlined in this policy.

i) Data obtained through electronic surveillance that has been used or is being used by the City in relation to an ongoing investigation or legal proceeding by the City or law enforcement officials shall be retained for a period not exceeding Seven (7) years or until the legal proceedings are concluded.

j) The following employees will have access to live viewing, playback, copying and disclosing recorded data.
    - City Manager
    - City Clerk
    - Designated Deputy City Manager responsible for Corporate Security
    - Manager of Emergency Preparedness and Business Continuity
    - Manager of Corporate Security

k) Designated managers specifically for;
    - Installation of covert cameras for the purpose of investigating unlawful dumping of refuse.
    - Regional Waste and Recycling (Robin Hood Bay)
    - Electronic Surveillance Equipment used by Parking Services.
    - Water and waste water operations

l) The following persons shall have access to live viewing and playback of recorded data.
    - Mayor and Councillors
    - Deputy City Managers
    - Managers and Department Heads
    - Employees of Contracted Security Service
    - Employees identified by Department Managers and supported by line Deputy City Manager, who require access to perform job function, for example, Community Services.

2. APPLICATION

This policy applies to:

a) All electronic surveillance cameras, monitors and camera recording devices and hardware, including city owned devices (i.e.: Cellular Phones, IPads etc.) at City of St. John's owned or leased facilities, properties, vehicles and events, or assigned city business.
b) Mayor and Councillors of the City of St. John's
c) All employees of the City of St. John's
d) Agencies, boards, commissions, foundations and corporations over which the City of St. John's has authority, as well as their employees.
e) Contractors and visitors of the City of St. John's

3. RESPONSIBILITIES

3.1 CITY COUNCIL

- Approve access to Electronic Surveillance Data as outlined within policy.

3.2 EMPLOYEES AND ELECTED OFFICIALS

- Complying with all aspects of this policy and requesting clarification from their supervisor(s) or Corporate Security, as required.
- Reporting any concerns regarding use or maintenance of Electronic Surveillance to the Manager of Corporate Security.
- Review related city policy on Mobile Devices

3.3 CITY MANAGER

- Approve installation of all Electronic Surveillance Cameras except as provided for in Paragraph 3.C.ii.
- Approval authority for the installation of covert cameras used for the detection of unlawful disposal of refuse may be delegated to the unit manager in charge of this function.
- Return all approved and non-approved requests for Video Surveillance to Manager of Corporate Security, who will record status and return request to originator.
- Initiate Investigations of alleged privacy breaches.

3.4 CITY CLERK

- Process all applications with respect to "Access to Information Requests" for stored recorded digital data with the following exception;
- Refer requests by Law Enforcement Agencies for stored digital data to the Manager of Corporate Security.

3.5 HEAD OF DEPARTMENT OR DESIGNATE

- Ensure compliance with all aspects of this policy with respect to monitoring, storage, retention, disclosure and destruction.
- Endorse support for Electronic Surveillance Equipment and give financial approval for associated costs.
- Consult with Manager of Corporate Security when considering deployment of Electronic Surveillance Equipment.
- Complete Risk Assessment prior to requesting Electronic Surveillance. **Appendix "B & C"**
- Prepare request for Electronic Surveillance equipment purchase and installation. **Appendix "D"**
- Obtain support and financial approval from applicable Deputy City Manager and forward to the Manager of Corporate Security.
- Maintain records of activities for audit purposes.

3.6 DIRECTOR, CORPORATE INFORMATION SERVICES

- Review all requests for Electronic Surveillance.
- i) Provide feedback on Electronic Surveillance request.
  ii) Provide IP addresses for networked Electronic Surveillance Equipment.
  iii) Provide IT standards for Electronic Surveillance Equipment networking components.

3.7 CORPORATE SECURITY MANAGER

- Maintain a list of all Electronic Surveillance cameras in use at City facilities.
- Identify members of contracted security for monitoring and viewing of Electronic Surveillance monitors.
- Ensure data is removed from the Central Storage system as per policy.
- Forward request for Video Surveillance to Manager of Information Technology for review and support.
- Ensure Video Surveillance request from Manager of Information Technology is forwarded to City Manager with recommendations.
- Forward both approved and non-approved requests to originating Department Head.
- Provide advice regarding the potential impact of the installation of Electronic Surveillance at a location on personal privacy.
- Advise on appropriate training for City Employees who have designated responsibility under this policy
- Investigate any reports of breach of policy or legislation and document findings.
- Conduct audits on the documentation, usage and management associated to Electronic Surveillance.
- Process requests for Electronic Surveillance Data from Law Enforcement agencies.

3.8 DIVISION HEAD OF PARKING SERVICES OR DESIGNATE

- Ensure all Traffic or Park Patrol vehicles equipped with Vehicle Mounted Electronic Surveillance equipment have appropriate signage attached.

- Ensure compliance with all aspects of this policy with respect to monitoring, storage, retention, disclosure and destruction.
- Ensure adequate documentation is in place to identify when the cameras are in use and the operator(s) are identified and maintain records for audit purposes.

3.9 ELECTRONIC SURVEILLANCE OPERATORS/MONITORS

- Monitor Electronic Surveillance systems.
- Secure Electronic Surveillance monitors, in order to prevent viewing of the monitors by unauthorized persons.
- Ensure that all aspects of the Electronic Surveillance system are functioning properly.
- Ensuring that no Personal Information is disclosed without the approval of Corporate Security, by taking all reasonable steps to prevent the copying of data/ images in any format (hardcopy, electronic copy etc.) from the monitors without the approval of Corporate Security.
- Document all information regarding the use, maintenance, and storage of records, including all instances of access to, and / or use of, recorded material to enable a proper audit trail.

3.10 DESIGNATED AUTHORIZED PERSONNEL

- Complying with all aspects of this Policy
- Ensuring that no personal information or digital recording is disclosed without the approval of persons authorized to provide disclosure.
- Documenting all information regarding the use, maintenance and storage of records, including all instances of access to, and / or use of, recorded material to enable a proper audit trail.
- Complying with all aspects of this policy and requesting clarification from their supervisor(s) or Corporate Security, as required.
- Reporting any concerns regarding use or maintenance of Electronic Surveillance to the Manager of Corporate Security.

3.11 PROJECT MANAGERS

- Ensuring Contractors who are designated as Authorized Personnel comply with City of St. John's Electronic Surveillance Policy.
- Working with Corporate Security during facility design, construction and/or renovation, in order to ensure Electronic Surveillance standards are met.

3.12 ASSOCIATED CORPORATIONS AND REGIONAL DEPARTMENTS

All arm's length corporations or entities that operate separate from the City but fall under City of St. John's Infrastructure shall designate a manager to be responsible for the Electronic Security management. The designated manager shall develop local protocols that are in compliance with applicable legislation and this policy. A copy of the protocols as well as the name and contact numbers for the designated manager will be provided to the Manager of Corporate Security for the City of St. John's.

a. This would include but is not limited to:
    - St. John's Sports and Entertainment (Mile One and Convention Centre)
    - Metro Bus Transit
    - Railway Coastal Museum Foundation

b. The following Regional Departments shall fall under this policy and follow the City policy as outlined:
    - Regional Water and Wastewater
    - Regional Waste Management (Robin Hood Bay)
    - St. John's Regional Fire Dept.

4. DEFINITIONS

- **"Authorized Personnel"** means an Employee or Contractor who has been granted access to Electronic Surveillance Equipment for one or more of the following purposes: to retrieve, download and / or view a Digital Recording to perform maintenance / repairs. The list and responsibilities of Authorized Personnel will be determined by Corporate Security, in consultation with the relevant Business Unit Director.
- **"ATIPPA, 2015"** means Access to Information and Protection of Privacy Act, 2015.
- **"City"** means the City of St. John's.
- **"City of St. John's property**" includes City facilities, buildings, infrastructure, assets, vehicles and events, including the facilities of Metro Bus Transit and St. John's Sports and Entertainment Ltd, Railway Coastal Museum.
- **"Contractor"** means a company or individual hired by the City of St. John's for a term of service that requires access to a City facility or property.
- **"Department Head"** is any position which would be considered the head of a department.
- "**Designate"** Any employee who has been delegated responsibility for specific action. For the purpose of this policy, the designate would be an employee with similar or higher authority or a committee which has been given responsibility for decisions pertaining to this policy.
- **"Digital Recording(s)"** means the images, data and associated records created and / or stored as a result of the use of Electronic Surveillance.
- **"Electronic Surveillance"** means closed circuit television (CCTV) camera(s) and associated equipment, which allow continuous or periodic remote viewing. Electronic Surveillance devices usually involve a recording ability and include the storage device(s) used to retain Digital Recordings. Electronic Surveillance may be viewed in real time or as a recording.
- **"Electronic Surveillance Operators"** are employees or contractors, designated by Corporate Security, in consultation with the relevant unit managers, who are responsible for the monitoring of Electronic Surveillance cameras at a given location. These may be security guards, receptionists, managers or other employees.
- **"Employee"** includes any person categorized as a permanent, term, part-time, casual, contract, seasonal, temporary or student worker in the employ of the City of St. John's and members of City Council.

- **“Metro Bus Transit”** is a public transport system owned by the City of St. John's, and is operated by the St. John's Transportation Commission, a board consisting of six members from various areas of the region.
- **“Personal Information”** is any recorded information about an identifiable individual.
- **“Railway Coastal Museum”** is a Foundation that is separate from the City of St. John’s but relies on the City to perform administration function such as payroll etc. It has a governing board on which there are representatives from council.
- **“Retention Period”** refers time maximum time personal information may be held on Surveillance Data records unless otherwise retained as per policy. The length of retention may vary between departments depending on operational needs and storage capacity.
- **“St. John’s Sports and Entertainment Ltd”** is a separate corporation that operates Mile One Centre and the St. John’s Convention Centre on behalf of the City of St. John’s. The operations of the facilities are overseen by a Board of Directors.
- **“Water and Wastewater”** refers to the processes of providing potable water and to the treatment of wastewater.
- **“Visitor”** is a guest to a City of St. John’s property, facility, bus or and includes a passenger on a vehicle operated by Metro bus.

5. REFERENCES

- Access to Information and Protection of Privacy Act, 2015.
- Guidelines for Video Surveillance by Public Bodies in NL
- Corporate and Operational Policy Manual; Policy: 02-01-14 Use of Mobile Devices in the Workplace.
- City Hall Post Orders
- Municipal Depot Post Orders

6. APPROVAL

- Policy Sponsor/Owner; Manager Business Continuity and Emergency Preparedness.
- Policy Writer; Manager Corporate Security
- Approval Date;
- Corporate Policy Committee/ Senior Executive Committee_____
- Finance and Administrative Committee_____
- St. John’s City Council_____

7. MONITORING AND CONTRAVENTION

- All monitoring shall comply with all applicable legislation and the provisions of this policy. The City shall maintain a record detailing who has accessed electronic surveillance data; if that data has been disclosed; the authority under which that data was disclosed; and to whom the data has been disclosed.

- Any employee breaching this policy or disclosing recorded data intentionally or otherwise unless authorized to do so may be subject to disciplinary action up to and including dismissal.

8. REVIEW DATE

This policy was revised and update in July 2016. Recommended review date is July 2019.

POLICY APPENDICES

Appendix A
Request for Search and Disclosure Log Electronic Surveillance

Name of Requestor:	Date:
Organization:	
Reason for Request: ATIPP Warrant Other	
Police File Number:	Investigator:
Location of Occurrence:	
Dates and times of requested search:	
Results of Data Search:	
Description of Data provided:	
Authorized by:	Date:
Received by:	Date:

Appendix B
Risk Assessment Template

Risk Assessment

Department:		Date:
Location:		

This assessment template is provided as a tool to identify, evaluate and mitigate security risks in the workplace.

High and Medium activities must be eliminated or mitigated and documented through an action plan. Low risk activities are not required to be documented.

Frequency	Severity of Consequences			
	Nil	Low	Medium	High
High	No risk	Medium	High	High
Medium	No risk	Low	Medium	High
Low	No risk	Low	Low	Medium
Unlikely	No risk	Low	Low	Low

1. Personal/Physical Security Risk Factors

a) What is the Security Risk

_____

_____

_____

Identify the Consequence(s)

_____

_____

_____

Rating ---------- NR L M H

b) Can the risk be mitigated or eliminated through conventional methods. Refer to Appendix "B

Yes No

c) **Is the threat level acceptable?** Yes No

d) **Is an Action Plan required?** Yes No

e) Describe Action to be taken:

Completed by:

Appendix C
Risk Factors and Mitigation Options

Personal Security:	Risk Factors:	Mitigation Options:
	1) Working Alone a) Injury b) Assault c) Nuisance clients d) Awareness e) Remoteness **2) Structures** a) Desk/Work Station Size and Height b) Office Configuration c) Location of Exits and Entrances (Visibility and Access) **3) Active Intruder** a) Disgruntled Employee b) Member of Public **4) Work Place Conflict** a) Unresolved conflict with co-worker **5) Location** a) Rural b) Secluded c) Remoteness **6) Handling Cash** a) Target for Theft/Robbery	**1) Barriers** a) Desk/Counter Height Increased b) Protective Glass Installed **2) Work Area** a) Positioning desk/work station i) Barrier ii) Facing Public Entrance iii) No backing onto public washrooms iv) Uncluttered **3) Safe Locations/Escape** a) Secure Office b) Fire Exit c) Lower level window **4) Emergency Numbers** a) Police b) Ambulance c) Security d) Supervisor e) Call Center **5) Communication** a) Phones b) Radios c) Code or Safe Words d) Panic buttons/Alarms e) Unit/Group Meetings f) Written bulletins, policies, directives g) Communication skills training **6) Knowledge** a) Layout of work location b) Contact persons c) Emergency Plans **7) Cameras** a) Entrances and exits b) High Risk areas c) Signage to notify of video recording **8) Identification Tags**

		a) Full Time Employees b) Part time or casual employees c) Visitors to specific areas d) Contractors **9) Security Patrols** a) Stationary Sites b) Foot Patrols c) Mobile/Vehicular Patrols d) CCTV Monitoring **10) Parking Lot** a) Adequate lighting b) Clear/Open route c) Travel in groups d) Check in for depart and arrival e) Vehicle locked/Items stored **11) Situational Awareness** a) Observe what is happening around you. b) Make decisions based on observations and actions
Physical Security	**Risk Factors**	**Mitigation Options**
	1) Access a) Uncontrolled i) Unlocked ii) No/Inadequate video surveillance iii) Lack of electronic access control iv) No or limited security personnel **2) Fire Exits** a) Not all are alarmed b) Batteries not maintained in those battery operated c) Obstructed/Debris **3) Elevators** a) Communication i) Emergency phones not working ii) No direction on Emergency process iii) No lockout for restricted areas **4) Parking** a) Location b) Distance from work location	**1) Locks** a) Building Entrances b) Offices and Storage Rooms c) Desk and Lockers **2) Window Coverings** a) Blinds or Curtains b) Locks/Barriers c) Safety Glass **3) Identification Tags** b) Building Entry c) Restricted Interior Access **4) Electronic Access** a) Building b) Internal working areas c) Entry and Exit tracked by computer **5) Sign in to building/facilities** a) General public b) Contractors **6) Cameras** a) Public Entrances b) High Risk areas i) Interaction with Public ii) Money Transactions **7) Signs**

	c) Inadequate lighting d) Open access to general public e) Poor or no video coverage **5) Windows** a) No coverings i) Blinds ii) Bars/Screen b) Easy Access c) Not safety glass **6) Thefts** a) External b) Internal	a) Direction to Services b) Notification of CCTV recording **8) Security Patrols** a) Frequency b) Thorough c) Competent d) Communication e) Decision making ability f) Documentation/Reporting **9) Lighting** a) Strategic Locations b) Quality c) Hours of Operations **10) Music** a) Audio Deterrence i) Loitering ii) Vandalism **11) Awareness** a) Internal Communication i) Security conscious workplace b) Emergency Plans **12) Site Assessments** a) Regular site assessment by managers

Appendix D
Request for Electronic Surveillance

Requestor:							Date:			
Department:							Phone:			
Job Position:										
Has City of St. John's Electronic Surveillance Policy been reviewed:		yes		No						
Has Risk Assessment been Completed?	yes		No		Copy Attached	yes		No		
Number of Cameras requested:		Number of Monitors Requested:			Number of signs to advertise Video Surveillance					
Site address and proposed location(s) of installation:				Anticipated cost:						
Rationale supporting Request: (attach risk assessment)										
Signature of Requestor:										
Name and Signature of Funding Approval Authority:							Date:			
Reviewed and Recommended by Line City Manager:							Date:			
Comments:										
Reviewed and Supported by Manager Information Technology:							Date:			
Comments:										
Reviewed and Supported by Manager of Corporate Security							Date:			
Comments:										
Approved by City Manager/Designate:							Date:			
Comments:										