Electronic Monitoring Policy

Category: Legislated Policy
Department: Human Resources
Effective Date: TBD 2024

Table of Contents

Purpose

Electronic monitoring can be used by the City of Cornwall (the "City") to collect information about employee activities while in the workplace or while working remotely. This Electronic Monitoring Policy (the "Policy") describes the Employer's approach to electronic monitoring in compliance with the relevant provisions of the Ontario *Employment Standards Act, 2000*, S.O. 2000, c.41 as amended from time to time (the "ESA").

The City of Cornwall is committed to transparency with regard to electronic monitoring. The purpose of this Policy is to provide transparency about the City's use of electronic monitoring tools for employee activities, including:

- how and in what circumstances the City electronically monitors employees, and,
- the purposes for which information obtained through electronic monitoring may be used by the City.

Scope

This Policy applies to all employees of the City whether the employee is working at an Employer work site, working remotely or a hybrid work model.

Application

This electronic monitoring policy aims to fulfill the City's legal obligations to address the circumstances where the City may electronically monitor employees and purposes for which such recorded information may be used. This Policy does not provide employees any new rights or right to not be electronically monitored. The contents of this Policy do not affect or limit the City's ability to conduct electronic monitoring, or use information obtained through electronic monitoring. This policy is not intended to amend or supersede any grievance procedure or other aspect of any applicable collective agreement.

Legislation and Applicable Regulations

This Policy is subject to:

- Digital Platform Workers' Rights Act, 2022
- Ontario Employment Standards Act, 2000
- Municipal Freedom of Information and Protection of Privacy Act (MFIPPA).

Definitions

- **Electronic Monitoring** – the collection and/or use of information about an employee by an employer, for the benefit of an employer, by means of electronic equipment, software (including those managed or hosted by a third-party, e.g. cloud software) or electronic network.
- **Employer** – The Corporation of City of Cornwall.
- **Employee** – an individual who performs work, in any capacity, for an employer as defined by the Employment Standards Act of Ontario which includes paid and unpaid employees, contractors, temporary employees, employees who work on site, remotely or in a hybrid capacity.

- **Active Monitoring** – the intentional tracking of activities and events, usually in real time, including without limitation: audit logs, audio and video files, camera footage, physical entry logs and location information, that may be actively reviewed on a regular basis.
- **Passive Monitoring** – The collection of data, activities, and events, as a result of automated systems to maintain business operations.
- **Record** – means any record of information, however recorded, that contains identifiable information about an individual in relation to an activity or event.

Roles and Responsibilities

The City, its management and employees must adhere to their responsibilities in accordance with this Policy.

Directors and Senior Management

- Ensure directing compliance and resolving any conflicts with this Policy;
- Ensure that procedural guidelines are established for this Policy;
- Upholding transparency of electronic monitoring that occurs in the workplace.
- Take all reasonable steps to ensure that management and employees rights are maintained, and procedures are followed as detailed in this Policy.
- Refrain from penalising or taking any other reprisal action against employees who have questions regarding this Policy or request compliance with it. Legitimate employer direction and/or corrective action towards employees is not considered “reprisal action.”

General Manager of Human Resources

- Develop and maintain this Policy and ensure annual reviews of the policy to align with applicable legislative changes.
- Provide new employees with a copy of this Policy within 30 days of the employee’s start date.
- Provide existing employees with a copy of any amended versions of the Policy within 30 days of the amendment.
- Provide advice and guidance to management and employees to support this Policy.
- Receive and manage employee inquiries related to the application of this Policy.
- Ensure privacy of all employees is respected and maintained in any electronic monitoring activities.

Supervisors and Managers

- Ensure that the privacy of employees is respected while maintaining a standard of appropriate use of City issued devices, vehicles, and accesses.
- Advise employees of the instances where they may be electronically monitored through means not mentioned in this policy;
- Respond to employees’ inquiries and resolve issues raised in collaboration with Human Resources.
- Responsible for contacting Human Resources to seek guidance in the application of this Policy.

Employees

- Responsible for familiarizing themselves with this Policy and adhering to its guidelines.

- Notify management if they have any concerns relating to this policy or if they are otherwise unable to comply with this Policy.
- Responsible for contacting Human Resources to seek guidance in the application of this Policy.

Information Technology

- Understand implications around electronic monitoring of employees prior to making any changes to new software and programs, work equipment, practices or protocols which may impact this Policy.
- Informing HR of any changes to the software, practices or protocols that may impact this Policy.

Policy Statement

In this Policy, “electronic monitoring” includes all forms of monitoring of employees using technological, electronic, or digital means to track, observe or monitor employees’ actions, including but not limited to, electronic equipment, mobile devices or software installed on computers or mobile devices (where data is used in compliance with the privacy policy and Acceptable use of IT equipment policy), video cameras, GPS tracking software installed on vehicles, electronic key cards and keypads.

The City will ensure that it uses the recorded events and activities for the purpose for which it was obtained and communicated and where its purpose remains consistent. The City will make every effort to inform the employee, using explicit statements and warnings, where technology permits, or using awareness and training, that an employee is being actively monitored prior to the employer engaging in monitoring activities.

This policy does not supersede any rights an employee may have under a collective agreement or employment contract with the employer. However, this policy does not provide new rights or privileges to employees to not be electronically monitored.

Active Electronic Monitoring of Employees

As a regular course of business, the City does not actively electronically monitor employees for performance management. However, the City reserves the right to monitor employees for the purpose of their performance management when there are reasonable grounds, with oversight from appropriate authorities, and in compliance with relevant legislation, the City’s policies, and collective agreements. Employee performance management may include tracking employee attendance, location, and activities to ensure fulfillment of their job duties and/or compliance with organizational policies. Examples of active electronic monitoring of employees may include, but are not limited to:

- Monitoring the date and time of access to physical locations and digital resources.
- Monitoring physical location using global positioning system (GPS) technology.
- Active electronic monitoring of employees may also include direct access to the contents of assigned account(s) and/or the device(s) used by an identified employee. City accounts include, and are not limited to, email, voicemail, Teams, SharePoint, OneDrive, and other storage space assigned for use by an individual employee.

Passive Monitoring of Employees

The City conducts passive electronic monitoring of physical spaces and digital identities, assets, and resources for the following purposes:

- **Physical security** – To assure the safety of community members and the physical security of premises; to monitor for violations of organizational policy; and, to monitor for violations of municipal, provincial, or federal laws.

- **Environment management** - To assess and manage the physical environment, including but not limited to heating, cooling, lighting, and other facilities services that contribute to a comfortable living and workspace.

- **Information technology service assurance** – To identify indicators of service degradation, and to assure ongoing availability and integrity of digital assets and resources connected to the network.

- **Cybersecurity** - To detect, prevent, and respond to cybersecurity events and incidents, and to assure the security and safety of digital identities, assets, and resources.

- **Audit and compliance** - To monitor and assure confidentiality and compliance with organizational policies, contractual obligations, relevant legislation, and regulations.

Data collected during passive electronic monitoring may include data about identifiable employees. Such data may be used to review the activities of an identifiable employee or may be used in correlation with other data sets to review the activities of an identifiable employee in the event of a complaint or investigation in alignment with applicable City policies and procedures.

The use of data collected during passive electronic monitoring at the City is done with oversight from appropriate authorities and in compliance with relevant legislation and City policies. The City's use of any electronic monitoring tools for employment-related purposes is subject to any rights an employee may otherwise have per their employment contract, collective agreement or otherwise at law.

Use of Information

The information obtained by the Employer through electronic monitoring may be used for the following purposes if there a reasonable cause to do so. The use of monitored data includes but not limited to:

- tracking employee working time through systems such as punch cards or time tracking to ensure accurate compensation and/or adherence to working time or attendance policies;
- improving work efficiency by tracking time spent on specific task types, tracking employee use of specific tools or software, or tracking employee location and travel time;
- protecting employee health and safety by tracking employee location or keeping a record of employee access to the workplace;

- ensuring employee adherence to workplace policies, especially those related to use of IT systems. For example, the Employer may review an employee's internet browsing history or instant messaging history following a complaint of inappropriate behaviour;
- To evaluate employee performance, to assess productivity and to ensure appropriate use of Employer equipment if necessary;
- For the purpose of investigations, to resolve any complaints or in case of suspicious activities such as theft, vandalism, break-in etc.

Appendix A of this policy address the various systems, software and tools through which employee activities could be monitored.

Privacy

Access to recorded activities, logs, and information, under the custody and control of the City of Cornwall, is limited to mangers and general managers who are responsible to manage and maintain the data. The City is committed to maintain the privacy of its employees and other identifiable individuals to the extent possible.

Data Retention

In order to comply with the Freedom of Information and Protection of Privacy Act, 1990 and other statutory requirements, all records, activities, and events recorded using electronic monitoring within the scope of this policy, will be kept in accordance with the City’s Record Retention Policy. Any data not covered under the City’s record retention policy may be kept for at least one (1) calendar month from the date that the data was first captured.

Policy Communication and Awareness

The City will provide all current employees with access to or a copy of this Policy within 30 calendar days of implementation. The City will provide all employees hired after this Policy is implemented with access to or a copy of this Policy (or the applicable revised version) within 30 calendar days of the employee’s start date.

Violations and Consequences

Any violations of this policy will be addressed in accordance with the City disciplinary procedures. The severity of the violation will be taken into consideration when determining appropriate consequences.

Review and Revision

This policy will be reviewed annually to ensure its effectiveness and relevance. Any necessary revisions will be made to align with changes in legislation, technology, and work practices. If the policy is changed, employees will receive a copy of the written policy within 30 calendar days of the policy change.

Related Policies

This Policy is intended to outline the City’s electronic monitoring practices and should be read in conjunction with the City’s other applicable policies, guidelines, or standards, including but not limited to:

- Acceptable Use Policy for Information Technology
- Access to Information and Privacy Policy
- Video Surveillance Policy
- Records Retention Policy

X ______________________________

Manon L. Levesque
City Clerk

X ______________________________

Matthew Stephenson
Interim General Manager, Human Services

X ______________________________

Tracey Bailey
General Manager, Financial Services

X ______________________________

Mathieu Fleury
Chief Administrative Officer

Appendix A - Sources for Electronic Monitoring

Currently, the City is engaged in following monitoring activities:

Monitoring of Video Surveillance

The City collects data and information about activities in physical spaces on the City's premises. This data includes video surveillance of employee or public activities. Security cameras are installed at various facilities and locations across the City of Cornwall. Cameras record videos, collect and retain video of physical spaces including indoors and outdoors. The Security Cameras are used for passive monitoring of employee activities. The data and logs can be used for the purpose of investigations or in the case of any suspicious activities.

Monitoring of Key Fobs/Smart Cards/Digital Badging

Entry, exits, and other doorways are locked using electronic locks which are accessible through use of an access card, key fobs, smart card, or other digital badging technologies. The access data is recorded by the card access system(s) which collects and retains logs of physical attempts to access City's buildings and/or areas with restricted access.

Data collected may include, and is not limited to:

- the date and time of the request,
- the unique identifier of the card being used to attempt access.
- Door location

The data and logs could be used for the purpose of investigations or in case of any suspicious activities.

Passive Electronic Monitoring of digital identities, assets, and resources

Any employee utilizing devices (PC, laptop, tablet) connected to the corporate network either directly through a wired or wireless connection, or via remote access (VPN) for their day-to-day activities, can expect data to be collected. This data may include, and is not limited to, the date and time of the request, the name and internet protocol address ("IP address") of the requesting device, and the name and IP address of the digital asset or resource being requested, and the physical location of the requesting device. Additional data is collected in relation to cybersecurity threats. This data may include, and is not limited to, the results of malware scans, and the behaviour of executables, files, software, code, and processes when opened or accessed, and other data about cybersecurity threats. The data and logs could be used for the purpose of investigations or in case of any suspicious activities.

Remote Access (VPN)

This VPN solution is used for users with remote access from laptops. The systems maintain logs including the Date and time of access, username, laptop name, Windows version, Secure Access version, remote IP, VPN tunnel data usage, authentication type (single, 2FA), Wi-Fi name, cellular or other network usage, and more.

Domain Name System (DNS) Servers

DNS servers collect and retain logs of internet resource requests. Automated analysis of internet resource requests is performed to prevent exposure to known cybersecurity threats. Data collected and retained may include, and is not limited to:

- the date and time of the request,
- the name and IP address and the requesting device,
- the name and IP address of the resource being requested (e.g., websites and other resources that are accessed by devices on the City network),
- details about cybersecurity threats prevented and/or detected.

Data collected by DNS Servers may be correlated with other data sets to monitor activities of an identifiable person or persons.

Firewalls

Firewalls collect and retain logs of network connections, including connections from the internet to digital assets and resources on the network, connections from devices on the network to websites and other resources on the internet, and connections between devices on the network. Automated analysis of network connections and the content thereof is performed to prevent exposure to known cybersecurity threats. Data collected may include, and is not limited to:

- the date and time of the request,
- the name and IP address and the requesting device,
- the name and IP address of the resource being requested (e.g., websites and other resources that are accessed by devices on the City network).
- details about cybersecurity threats prevented and/or detected.

Data collected by Firewalls may be correlated with other data sets to monitor activities of an identifiable person or persons. Firewall VPN

PC Management and Inventory Systems

The City collects data for PC Management and inventory including data for various device tools and access. The logs include user access per device with date and time. The PC Management and Inventory System also catalogues and inventories installed software.

Network Servers

The City's Network Policy Servers collects data/logs and provide authentication services for Wi-Fi access on corporate devices. The logs are recorded at each connection attempt which includes include Username (valid or invalid), log in attempts - success or failure, date and time of access, device name.

Authentication and Authorization

The City collects data about authentication attempts to digital assets and resources. This data may include, and is not limited to, the date and time of the authentication attempt, the authentication identifier (e.g., network ID) and IP address of the requestor.

Active Directory

Digital assets and resources collect data about successful and unsuccessful authentication attempts.

Microsoft 365

All content directly provided to Microsoft 365 applications, including all text, sound, video, image files, and software, is retained and associated with the City's Microsoft tenant subject to both Microsoft's Data Handling Standard and the City's internal data retention policies.

Email

Email servers, including Outlook, Microsoft Exchange Online, retain logs of email communications. Email servers, including Outlook, retain logs of the results of cybersecurity threat analysis on the content of messages. Content may be retained if a cybersecurity threat is detected or suspected.

Microsoft SharePoint

Applications and sites on the Microsoft SharePoint platform may be configured to retain activity and audit logs.

Anti-Virus Software

The City collects data about cybersecurity threats on City owned and issued devices, and personally owned devices that are protected by Anti-Virus software managed by the City. This data includes, but is not limited to, the results of malware scans, internet resources to which the device has connected, and the behaviour of executables, files, software, code, and processes when opened or accessed, and other data about cybersecurity threats.

Endpoint Protection

The City uses endpoint protection software which collects logs of cybersecurity threat analysis on the content of files and network connections. Content may be retained if a cybersecurity threat is detected or suspected. The logs are maintained for:

- Endpoint: logs activities like process executions, network communications, and file modifications;
- Network: Logs network activities related to potential threats, such as unusual data transfers or communications with known malicious IP addresses;
- UBA: monitors and logs user sign-in activities and attempts to access resources. It can detect anomalies in user behavior, such as sign-ins from unusual locations or multiple failed login attempts, which could indicate compromised credentials;
- Email / Teams: This includes logging of email activities, including the tracking of phishing attempts, malware distribution via email, and abnormal email sending patterns. It also monitors collaboration tools like Microsoft Teams for potentially harmful or suspicious activities;
- Cloud: extends its logging capabilities to cloud applications, monitoring for unusual user activities, and risky configurations. It can log data about file downloads, data sharing activities, and access to sensitive information in cloud applications.

Access Software

The City uses a software system which includes a suite of identity and access management products that has capabilities for securing and managing identities and access across environments. The following logs are maintained:

- Sign-in logs: The sign-in logs can track user sign-in activities, including information like the IP address, device information, and information on successful and unsuccessful sign-in attempts.
- Audit logs: Audit logs record changes made in the directory, such as adding or removing users, changing group memberships, and modifying application settings.
- Risk detection logs: Records potentially risky sign-in behaviors based on a variety of signals (location, time of access, baseline deviation, etc.)

GPS System - Acetek

Acetek System in installed in the City’s EMS vehicles which may record and maintain records of location of the vehicles, speed of the vehicles, use of emergency warning systems, idling time, seat belt use by the Driver. The system also records and maintain video surveillance footage recorded from cameras from inside the EMS vehicles. This data is used for passive monitoring for purposes of providing emergency services with location of the vehicle, performance management, investigations, monitor vehicles performance and in case of suspicious activities.

GPS System – Geo-Data Systems

Geo-Data Systems is installed in all company vehicles except EMS vehicles. This system records and maintains records and logs for data including location of the vehicle, hard use of brakes or acceleration, idling time. This data is used for passive monitoring for purposes including performance management, investigations, monitor vehicles performance and in case of suspicious activities.

Work Phones

Call logs on work phone be monitored for call duration, source, destination, costs etc. may be recorded for usage & license management and for reconciliation of long-distance charges with the service provider(s).

Time and Attendance Stations

The electronic time and attendance stations installed at various locations records the time of entry and exit for each employee when the smart card is tapped on the system. The purpose of the stations to record time entry and prepare timesheets for employees. The data reports are used for time keeping, investigations, or in case of suspicious activities

Maintenance Systems

The maintenance system is used to record data involving documentation of preventative maintenance of EMS vehicles. The recorded data includes – data of maintenance, name of the employee performing maintenance. The data is for investigations, performance management, or in case of suspicious activities.

MediSystems Portal

The MediSystems Software records and maintain data/logs once an employee requests for medication from Pharmacy. The data or logs are used for investigations, performance management, or in case of suspicious activities.

Call Bells

The Nursing call system records and maintains data/logs of the call requests from the patients/visitors and response time to the call requests. The data or logs is used to evaluation of employee performance, for investigations or in case of suspicious activities.