Municipality of West Elgin

Policy HR-4.9
Electronic Monitoring Policy

Effective Date: **October 11, 2022**

Review Date:

Policy Statement

The Municipality of West (the Municipality) is committed to transparency with regard to electronic monitoring as required under the *Employment Standards Act, 2000 (ESA)*.

Policy

Electronic Monitoring refers to use of electronic means to observe, record, track or collect data on employees (including but not limited to employee performance, location and resource use) where such information may be accessed and/or reviewed by the employer or someone acting on the employers behalf.

This policy is intended to outline the Municipality's electronic monitoring practices and should be read in conjunction with other Municipal policies, guidelines or standards.

Application

This policy applies to all employees of the Municipality, as defined by the ESA, whether they are working remotely, in the workplace or are mobile.

Electronic Monitoring Practices

The following table outlines electronic monitoring technologies utilized by the Municipality:

Tool	Circumstances	How	Purpose
Endpoint Threat Detection and Response	Continuous	Endpoint Threat Detection and Response monitors the use of workstations (programs run, files read and written, etc.) and compares it against a baseline to detect abnormalities and potential unauthorized use	Network Security

Tool	Circumstances	How	Purpose
Email Tracking	Continuous	Software records copies of messages sent or received by address within the Municipality's domain	Network Security
Network/Performance Monitoring Tools/ Firewalls/VPN	Continuous	Tools that record network traffic occurring between workstations, servers, the internet, etc. Investigations may occur to troubleshoot incidents which may expose User Identifiable Information	Network Security
Event log Collection Tools	Continuous	Collection of event logs generated by electronic devices to a centralized or non-centralized system. Investigations may occur to troubleshoot incidents which may expose User Identifiable Information	Network Security
Electronic Key Fob/PIN	Each Scan or entering of PIN	An electronic sensor or PIN creates a record each time an authorized user scans or enters their number to enter certain Municipal Buildings	Facility Security
Vehicle Telematics/GPS	All fleet vehicles during use	On board sensors detect and report on vehicle location, driver behavior (hard breaking, rapid acceleration etc.) and engine diagnostics.	Fleet management, driver safety and security
Mobile Device location tracking and investigations	Continuous and with reasonable grounds	Enablement of location services on mobile devices. Investigations may occur to locate missing assets and/or	Asset Security

Tool	Circumstances	How	Purpose
		document unsanctioned employee activities	
Recording of Phone Calls	Continuous and with reasonable grounds	Voice recording of all telephone calls incoming and outgoing on the VOIP system. Investigations may occur to identify incidents of staff abuse and/or investigate complaints	To identify abuse of staff and to investigate complaints against staff
Laserfiche	On an as needed basis	Reporting tool built in that can identify slow downs or stoppages within workflows and processes that are automated. Investigations may occur to identify issues within an automated process	To identify slow downs in the human element of the automated business processes
Timecard – Fingerprint scan	At the start of every shift	Scan of each staff's finger print to clock in and out of work. States the time employee starts and ends their shifts as well as locations of workers at the beginning and end of shifts	Information used for payroll system and employee absenteeism

Nothing in this policy affects or limits the Municipality's ability to use information obtained through electronic monitoring. The Municipality reserves the right to monitor Information Technology assets and services belonging to the Municipality to ensure secure, effective and appropriate use. Employees should have no expectation of privacy as it relates to their use of Municipal Information Technology or the location of Municipal Assets.

Posting, Notice and Retention

The Municipality shall provide a copy of this Policy to each employee within thirty (30) calendar days of implementation.

Should any amendment(s) be made to this Policy after its implementation, the Municipality shall provide each employee a copy of the amended Policy within thirty (30) calendar days of the amendment(s) being made.

The Municipality shall provide a copy of this Policy to all new employees upon onboarding and within thirty (30) calendar days of the employee commencing employment with the Municipality.

The Municipality shall retain a copy of this and any revised version of this Policy for three (3) years after it ceases to be in effect.

Review

The Municipality reserves the right to review and evaluate this Policy annually and amend as necessary.