ELECTRONIC MONITORING POLICY

[Organization Name] is committed to abiding by all of its obligations under Ontario’s Employment Standards Act, 2000 (ESA), specifically those which apply to electronic monitoring.  As such, [Organization Name] is committed to informing its employees about the presence (if any) of electronic monitoring software or equipment either in the workplace or contained on any of the organization’s servers or programs.

This policy is based on [*Bill 88: Working for Workers Act, 2022*](https://www.ola.org/en/legislative-business/bills/parliament-42/session-2/bill-88#BK7) and is subject to change as per any new information provided by the Government of Ontario.

This policy is intended to specify:

* A description of how and in what circumstances, [Organization Name] may electronically monitor employees,
* The purposes for which [Organization Name] may use the information obtained through electronic monitoring, and
* The date the policy was prepared and the date any changes were made to the policy.

This policy offers standards to ensure the following:

* Employee safety and security;
* That the company operates efficiently; and
* That appropriate data is collected to make informed business decisions, as needed.

SCOPE

As an organization of more than 25 employees as of January 1 (note: part time and casual employees, as well as employees at different company locations are counted in this total), [Organization Name] is required to have this policy in place regarding electronic monitoring.

This policy applies to all employees of [Organization Name] who are covered by the *Employment Standards Act*, whether their primary location of work is in the workplace, at home, on the road, or a combination of any or all of the above.

EFFECTIVE DATE

This policy is effective as of its creation date. It must be in place by March 1 of any year when an organization employs 25 or more employees as of January 1 of that calendar year.

CHANGES TO THIS POLICY

Any changes to this policy will be noted in this section, along with the date(s) that changes were made.

EMPLOYEE COUNT

Employees to be counted include “anyone who meets the definition of "employee", including: “homeworkers, probationary employees, some trainees, officers of a corporation who perform work or supply services for wages, employees on definite term or specific task contracts of any length, employees who are on lay-off, so long as the employment relationship has not been terminated and/or severed, employees who are on a leave of absence, employees who are on strike or who are locked-out, and employees who are exempt from the application of part(s) of the ESA.”

Note: in the event that [Organization Name] does not have 25 employees as of January 1, but grows to 25 employees during the year, the organization will put this policy in place by March 1 of the following year.

Should [Organization Name]’s total employee count decrease to fewer than 25 employees, the policy will remain in place until the following January 1, at which point (if the employee count is still below 25), a written policy is no longer required.

POLICY

ESA Requirements

The ESA requirements do not:

* establish a right for employees not to be electronically monitored by their employer; or
* create any new privacy rights for employees.

However the ESA requires transparency about whether employees are electronically monitored. Nothing in the ESA limits the use of information obtained through electronic monitoring.

Providing Copies of this Policy to Employees

* [Organization Name] will provide this written policy to all employees within 30 days of its effective date.
* If any changes are made to this policy, employees will be provided with the updated policy within 30 days of any changes.
* In the case of newly hired employees, [Organization Name] will provide a copy of this policy to them within 30 days of their date of hire.

The policy may be provided either:

* As a printed copy, or
* An attachment to an email, or
* A link to a document online

If an employee is not able to access the document online or cannot print the document, they may request a printed copy from their supervisor/manager.

Electronic Monitoring Equipment in Place

[Organization Name] has the following electronic monitoring equipment in place in the workplace (remove what is not applicable):

* Email monitoring software
  + All email communications sent using company-owned networks, equipment, or user accounts are monitored, and this may include personal email accounts accessed through company-owned IT assets.
* Video cameras and recording equipment for public areas
  + Video surveillance technology is used on company premises to deter theft, vandalism, and ensure employee safety. Should illegal conduct be uncovered, video surveillance footage may be disclosed to approved third parties. Bathrooms, changing rooms, and other private spaces do not have video surveillance. Video surveillance equipment will be clearly visible and marked with notices and does not include audio.
* Internet and app activity monitoring, including downloaded documents and accessed websites, etc.
  + [Organization Name] monitors employee network and computer activities to verify that company-owned IT resources are used only for work-related or professional activities. Computer activity data can evaluate employee performance, detect malicious or high-risk behaviours, monitor network performance, and avoid security incidents.
* Keystroke trackers for keyboards
  + [Organization Name] uses keystroke trackers to monitor employee activity while they are working remotely.
* Recording equipment on all phones for external calls
  + [Organization Name] records all external calls to ensure that customer service and satisfaction are at optimal levels. These records also help to improve internal processes.
* GPS monitoring is in place in company vehicles which tracks both geography, time, speed, etc.
  + [Organization Name] has GPS monitors in place in company vehicles to ensure employee safety and security and to send help if an employee is ever in danger. These records may also be accessed in the event of an accident.
* Biometric technology
  + Biometric technology is in use for access to the building and to specific work areas for employees.
* Key card monitoring for access to the building and/or restricted areas
  + Keycard access is monitored in any areas, including parking garages, etc.

Reasons for Accessing the Electronic Records for Monitoring Equipment

[Organization Name] will access the records for this equipment in the following circumstances:

* In the event of an investigation into a client complaint
* In the event into a complaint of non=payment for time worked
* In the event the authorities request the electronic records
* In the event of a complaint of harassment or violence

Data Retention

All data obtained by workplace monitoring will be retained digitally on an encrypted drive with the password protection and will be retained for no longer than is required per privacy law, unless it is the subject of an investigation. Personal information will only be held longer in extraordinary circumstances or by law.

Retention of this Policy

[Organization Name] will ensure that copies of this policy, including any subsequent revisions, are retained for a period of three years after the policy ceases to be in effect.

Questions or Complaints

Any questions or complaints regarding this policy should be directed to the employee’s supervisor.