[ON LETTERHEAD]

**ELECTRONIC MONITORING POLICY**

**This policy was originally prepared on:** **[**date**]**

**This policy was revised on:** **N/A** [**Note to Draft:** Insert future revision dates as applicable; note that employees must be provided a copy of any revised policy within 30 calendar days of revision]

**Overview**

**EMPLOYER** uses electronic monitoring to access, record, and review information in the circumstances described in this Policy.

In this Policy, “electronic monitoring” means **EMPLOYER’s** collection of information about an employee’s activities through **EMPLOYER**-owned electronic devices and employee-owned electronic devices that are used for work purposes, such as computers, computer networks, cell phones, GPS units and [**Note to Draft:** describe other electronic devices workplace/describe electronic devices used for work purposes; the **EMPLOYER** may substitute its own definition of electronic monitoring].

**Application**

The Policy applies to all of the **EMPLOYER’s** employees in Ontario, and includes management, executives, assignment employees and shareholders if they are employees under the applicable laws. [**Note to Draft:** An employer is not required to have the same policy applicable for all its employees, and may have a single policy that applies to all employees, or its policy can contain different policies (either in a single document or in multiple documents) for different groups of employees]

**Systems Subject to Electronic Monitoring**

**EMPLOYER** uses electronic monitoring systems that record activities, including traffic and logging data, on the following Systems:

**Communications and Computer Systems** including any e-mail, messaging, and other applications hosted by or on behalf of **EMPLOYER**; **EMPLOYER’s** internal communications and computing networks and associated servers; remote devices connected to **EMPLOYER** internal communications and computing networks and/or associated servers; electronic medical record systems; and all associated databases and removable storage media.

**Employee Systems and Resources** including employee schedules, payroll, benefits, and compensation data; support tickets; and travel and expense records.

**Physical Security and Recording Systems** including closed circuit television and audio footage; encrypted door locks; keycode panels; timecards; electronic keys (i.e., key fobs); and location-tracking installed in **EMPLOYER**-issued devices.

[**Note to Draft:** describe other electronic devices workplace/describe electronic devices used for work purposes].

**Responsibilities**

By using any of the Systems subject to electronic monitoring by **EMPLOYER**, each user thereby consents to the monitoring activities set out in this Policy and agrees to use the Systems at all times for the purposes for which these systems are intended, in accordance with all applicable legislation and **EMPLOYER** policies.

**Uses of Electronic Monitoring**

**EMPLOYER** may access, record, and review any information contained on the Systems, in accordance with applicable laws, for such time and to such extent as is reasonably necessary for the following purposes:

* To secure, maintain, manage, and repair any of the Systems.
* To improve 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.
* [**Note to Draft:** insert additional purposes based on the **EMPLOYER’s** business]

Information collected in the context of electronic monitoring as described in this Policy will be retained, used, and disclosed for the purposes described in this Policy, and will be subject to security, retention and access as described in **EMPLOYER’s** [Privacy Policy]. [**Note to Draft:** If no applicable privacy policy is currently in place, the sentence may be revised to state “[…] in accordance with all applicable laws.”]

**Administration of this Policy**

[Responsible Person/Department] is responsible for the administration of this Policy. If employees have any questions regarding this Policy, they may contact [Contact Person/Department].

**Breach of this Policy [*Optional*]**

Any reasonably suspected breach of this Policy and its associated procedures or guidance by **EMPLOYER’s** staff will be investigated in accordance with all applicable **EMPLOYER** processes and procedures. This includes any breach by any member of relevant staff responsible for implementing any system of monitoring covered by this Policy.

A breach of this Policy and its associated procedures and guidance by a member of **EMPLOYER’s** staff may result in corrective measures and discipline, up to and including dismissal for just cause.

A breach of this Policy and its associated procedures and guidance by non-staff will be investigated and may result in corrective measures being taken in accordance with the law and any relevant contract.

**Changes to this Policy**

**EMPLOYER** reserves the right to change, modify or delete portions of this Policy in accordance with applicable laws.

Employees will receive a copy of this Policy within 30 days of:

* This Policy’s implementation.
* Any changes made to this Policy.
* The employee’s hire date.

[**Note to Draft**: **A copy of the policy may be provided to employees as (i) a printed copy; (ii) an attachment to an email (if the employee can print a copy); or (iii) as a link to an online document (if the employee can access and print a copy)**]

**Acknowledgement of Receipt and Review [*Optional*]**

I, \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (employee name), acknowledge that on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (date), I received a copy of **EMPLOYER's** Electronic Monitoring Policy and that I read it and understood it.

|  |  |
| --- | --- |
|   | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Signature\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Printed Name\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Date |