Workplace Device Tracking Policy

Effective Date: [Date] | Version: [1.0] | Last Revised: [Date]

1. Purpose

[COMPANY] provides company-issued devices to support the work of its employees. This policy defines how activity on those devices is monitored, what data is collected, and how that data is used and stored. It exists to give employees a clear and honest account of what automatic tracking on company-owned devices means in practice, and to establish the boundaries within which monitoring operates.

2. Devices Covered

This policy applies to all computing devices owned and issued by [COMPANY], including laptops, desktop computers, and mobile devices enrolled in the company's device management system. It does not apply to personal devices employees own and use independently, even when those devices are used for work-related tasks. Employees participating in a bring-your-own-device program are subject to a separate policy.

3. Data Collected

During tracked work sessions, [COMPANY] may collect the following categories of data:

- **Time tracking.** The start and end times of active work sessions, and how time is distributed across projects or tasks.
- **Application and URL activity.** Which applications and websites are used during tracked hours.
- **Activity levels.** Indicators of keyboard and mouse usage used to determine active versus idle time. [COMPANY] does not record the content of keystrokes or user input, but rather the frequency of said device usage.
- **[Optional] Screenshots.** Periodic screenshots taken at defined intervals during tracked hours. [Remove if not applicable.]
- **[Optional] GPS location.** Location data for devices used in the field. [Remove if not applicable.]

4. Tracking Conditions

Tracking on company-issued devices runs automatically according to the schedule defined below. It does not require manual input from employees to start or stop.

- Tracking is active during the following hours: [Days of week], [Start time] to [End time],

[Timezone].

- Tracking is based on active computer use. Sessions begin when keyboard or mouse activity is detected and pause during periods of inactivity.
- No tracking occurs outside of the scheduled hours defined above.
- Tracking schedules are configured and managed by [COMPANY] administrators.

5. Access

Access to tracking data is limited to the following roles:

- **Administrators.** [COMPANY] system administrators who configure and maintain the tracking system.
- **Managers.** Team managers and supervisors with direct oversight of the employees whose data is collected.
- **Employees.** Each employee may view their own activity data through [PLATFORM]. This access is read-only. Employees do not control when tracking runs or how it is configured.

Data is not shared with third parties except as required by law or as necessary to operate the tracking system through [COMPANY]'s software provider.

6. Retention

- Tracking data is retained for [X days / months / years] from the date it is collected.
- Data is stored on servers operated by [COMPANY's software provider], located in [Region / Country].
- Upon expiration of the retention period, data will be permanently deleted. Deletion may occur sooner when required by law, upon verified employee request (where applicable), or in response to broader operational requirements.

7. Boundaries

The following are explicitly outside the scope of this policy and are not monitored:

- Personal files stored on company devices are not intentionally accessed or reviewed as part of routine monitoring. However, limited incidental capture of on-screen content may occur through automated tracking (e.g., screenshots or application activity).
    - When sensitive data is uncovered, [COMPANY] will take reasonable steps to limit access, avoid use of the content for evaluative purposes, and

delete/redact it where appropriate.

- Activity that occurs outside of scheduled tracking hours is not actively monitored. Tracking systems are configured to disable data collection outside those hours.
- No monitoring will occur on personal devices not enrolled in [COMPANY]'s device management system.
- The content of personal communications is not intentionally monitored. However, such content may be incidentally captured if it appears within tracked applications or screenshots during work sessions.

8. Employee Visibility

Employees subject to this policy are entitled to the following:

- Advance notice before tracking begins on any device they use.
- Access to their own activity data through [PLATFORM] at any time.
- A copy of this policy upon request, available at [location — e.g., employee handbook, internal wiki].
- Notification of any material changes to this policy before those changes take effect.

By continuing to use company-issued devices following the effective date of this policy, employees acknowledge that they have read and understood its contents.

Acknowledgment

Employee Name: _____

Signature: _____

Date: _____