<...Company Name Here...>
Employee Monitoring Policies

Company's Devices

All computers, telephones, other electronic devices and electronic communications services provided by <...Company Name...> (company) to employees are the property of the company. All data transmitted and/or received via company devices belong to the company.

Using Your Own Devices

Employees have permission to use their own devices to conduct work-related duties. Working hours are to be used for job-related purposes only. It is strictly prohibited to spend working time on personal grounds during working hours. All work-related data is the property of the company.

Job-Related Use

Employees are permitted to use the company's property such as computers, other electronic devices, the internet, e-mail, phone, and printing devices' which are to be used for work-related purposes only during working hours. It is strictly forbidden to use the property of the company for personal purposes during working hours.
Working hours are to be used for work purposes only.

Personal Use

Company property is to be used reasonably and responsibly by employees before/after working hours and during lunch hours. Inappropriate use, such as excessive personal use; sending, accessing or storing discriminatory, harassing, defamatory, or pornographic content; duplicating or distributing copyrighted material without permission; and transmitting confidential, proprietary, or trade secret information; - is prohibited on the company's property.

Purpose of Monitoring

The purpose of this Employee Monitoring Policy is to ensure transparency in how the organization monitors employees' activities using WorkTime non-invasive employee monitoring software. This policy is designed to protect sensitive business data, maintain productivity, and comply with legal and ethical standards. WorkTime is used solely for productivity analysis and does not involve invasive tracking methods such as keystroke logging or screen recording.

Scope of Monitoring

This policy applies to all employees, contractors, and interns using company resources, including but not limited to:

- Computers, laptops, and other devices (both company-issued and personal if used for work-related purposes).
- Internet and network systems.
- Email and communication platforms (e.g., chat tools, messaging systems).
- WorkTime software used for productivity tracking.

Monitoring Objectives

The organization may use WorkTime monitoring software for the following reasons:

- **Productivity Optimization**: To measure workload distribution and ensure efficiency.
- **Workforce Management**: To analyze work patterns and improve employee performance without invasive methods.

Activities Monitored

The organization uses WorkTime to collect the following non-invasive data:

- Time spent on applications and websites relevant to work tasks.
- Work hours, attendance, and idle times.
- Productivity trends based on active/inactive periods.

WorkTime does not track keystrokes, take screenshots, or access personal/private data. Personal devices will only be monitored if they are used for work purposes and with the employee's consent.

Data Collection and Retention

Monitoring data will be:

- Stored securely in compliance with data protection laws.
- Retained for a period of [X months/years], after which it will be permanently deleted unless required for legal purposes.
- Accessed only by authorized personnel for productivity assessment and compliance purposes.

Employee Rights

Employees have the right to:

- Be informed about what is being monitored and why.
- Review data collected about them upon request.
- Report concerns about potential misuse of monitoring data.

Monitoring will not interfere with legally protected activities such as breaks, labor organizing, or personal communications outside work hours.

Legal and Ethical Compliance

The organization commits to conducting all monitoring activities in compliance with applicable laws, such as [insert applicable laws, e.g., CCPA], and ethical standards. WorkTime monitoring is designed to be non-invasive and will not extend to areas or activities where employees have a reasonable expectation of privacy.

Implementation and Communication

This policy will be communicated to all employees through [e.g., employee handbooks, onboarding materials, dedicated training sessions]. Employees will be required to acknowledge this policy in writing. Any updates to this policy will be communicated promptly.

Non-Compliance

Employees who violate this policy by bypassing or tampering with monitoring systems may face disciplinary action, up to and including termination of employment. Similarly, misuse of monitoring data by the organization or its representatives will result in disciplinary action against responsible parties.

Review and Updates

This policy will be reviewed periodically to ensure alignment with evolving workplace practices, technological advancements, and regulatory changes.

Acknowledgment Form

By signing below, I acknowledge that I have read, understood, and agree to comply with the Employee Monitoring Policy.

Employee Name: _____

Employee Signature: _____

Date: _____