

=====

EMPLOYEE WORKPLACE & REMOTE MONITORING POLICY

Standard Operating Procedure, Privacy Framework & Employee Consent (2026 Edition)

=====

Company Name: [Company Legal Name] ("Company")

Effective Date: [Insert Date, e.g., October 1, 2026]

Policy Version: 3.0 (Comprehensive 19-Section Framework)

Review Cycle: Annual or Upon Substantive Tech/Legal Revisions

Applicable To: All Employees, Independent Contractors, and Third-Party Consultants

LEGAL DISCLAIMER:

This document is provided for informational and operational reference only and does not constitute formal legal advice. Labor, surveillance, and data privacy regulations vary across jurisdictions (e.g., the Digital Personal Data Protection Act in India, GDPR in the EU, and state-level electronic monitoring statutes in the United States). Employers must have internal counsel review this template before deployment.

1. PURPOSE

The purpose of this Employee Monitoring Policy is to establish transparent, lawful, and ethical standards under which [Company Name] observes workplace digital activities. Monitoring telemetry is collected exclusively to:

- a. Ensure accurate recording of billable hours and project velocity;
- b. Provide verifiable proof-of-work for client billing and audits;
- c. Safeguard corporate trade secrets, source code, and client confidential data;
- d. Maintain robust cybersecurity hygiene and prevent unauthorized data exfiltration;
- e. Prevent employee burnout by detecting overwork and optimizing workload balance.

2. SCOPE

This Policy applies to all computational hardware, local networks, cloud accounts, and digital communication channels owned, leased, or utilized on behalf of the Company. This encompasses corporate workstations, virtual desktop infrastructure (VDI), cloud file repositories, and approved Bring Your Own Device (BYOD) software sessions.

3. WHO IS COVERED

This Policy applies universally and without exception to:

- a. Regular full-time and part-time permanent employees;
- b. Independent contractors and freelance professionals;
- c. Fixed-term consultants, apprentices, and interns;
- d. Executive, managerial, and administrative staff.

Monitoring parameters are applied objectively across roles to prevent disparate impact.

4. DEVICES COVERED

4.1 Corporate-Owned Devices:

All laptops, desktops, tablets, and smartphones provisioned by the Company remain the exclusive property of [Company Name]. Employees acknowledge they possess no

reasonable expectation of personal privacy on corporate hardware.

4.2 Personal (BYOD) Hardware:

Personal laptops and home computers are subject to monitoring ONLY when the employee actively launches the designated tracking client (e.g., TrackLabs) or logs into a secure corporate VDI session. Personal partitions, off-duty activity, and personal hardware sensors remain completely private and unmonitored.

5. WORKING HOURS & TIMING

Monitoring is restricted strictly to designated, paid working hours:

- a. For fixed-shift personnel, monitoring coincides with scheduled shift windows;
- b. For flexible or asynchronous personnel, monitoring occurs only while the employee has explicitly toggled the timer to "Active Tracking";
- c. Zero monitoring occurs during meal breaks, personal pauses, or outside shifts.

6. TIME TRACKING PROTOCOL

6.1 Interactive vs. Automated Tracking:

Employees must record project hours through the authorized client. Interactive timers allow employees to start, pause, and categorize time by project and task.

6.2 Overtime Authorization:

All overtime beyond standard weekly limits (e.g., 40 hours/week or local statutory thresholds) requires advance written approval from the direct supervisor.

7. SCREENSHOT MONITORING & PRIVACY SAFEGUARDS

7.1 Frequency & Capture Modes:

Periodic screen captures are captured at randomized intervals (1 to 3 captures per 10-minute work block) solely while an active work timer is running.

7.2 Automated Privacy Masking (Blurring):

The Company enforces automated screenshot blurring to obscure sensitive personal information, passwords, banking portals, and private chat snippets.

7.3 Employee Inspection & Deletion Rights:

Employees may inspect all captures recorded on their account. If an accidental capture contains private or sensitive personal matter, the employee may delete it; the corresponding 10-minute block will be deducted from recorded billable hours.

8. WEBSITE AND APPLICATION TRACKING

Software tracks active window titles, application names, and browser URL domains to establish productivity benchmarks:

- Productive: Core business tools (e.g., IDEs, Jira, Figma, GitHub, Google Docs);
- Neutral: Search engines, reference portals, utility programs;
- Non-Productive: Social media, video gaming, and streaming entertainment.

Telemetry informs workload balance and training, not punitive micromanagement.

9. ACTIVE VS. IDLE TIME

Activity levels are measured through aggregate keyboard and mouse movement percentages. If no input activity is detected for ten (10) consecutive minutes, the tracking agent flags the session as idle and displays an inactivity prompt:

- a. Keep Offline Time: If engaged in work-related offline tasks (e.g., client call, manual document review), the employee may categorize the offline duration;
- b. Discard Idle Time: The inactive period is excised from the billable timesheet.

10. INFORMATION EXPLICITLY NOT MONITORED

To protect fundamental privacy rights, the Company and its software tools NEVER:

- a. Log individual keystrokes (no keylogging of characters, passwords, or PINs);
- b. Record audio via device microphones;
- c. Stream or capture video via device webcams;
- d. Monitor personal emails, personal WhatsApp, social media, or banking accounts;
- e. Track devices outside of billable shift hours or while the tracker is paused;
- f. Track physical location/GPS when off-duty.

11. WHO CAN ACCESS EMPLOYEE DATA (ROLE-BASED ACCESS)

Access to monitoring telemetry is strictly governed by Role-Based Access Control (RBAC):

- Direct Supervisors: View aggregate hours, task allocations, and blurred captures for direct reports only;
- HR & Payroll Officers: View timesheet summaries and attendance records for compensation and leave calculations;
- Executive Leadership: Access anonymized, department-level productivity metrics;
- System Administrators: Manage platform configurations, tenant access, and audit logs.

Data will never be shared, sold, or disclosed to unauthorized third parties.

12. DATA RETENTION & PURGING SCHEDULE

In compliance with data minimization mandates (e.g., Section 8(7) of India's DPDP Act and Article 5 of the EU GDPR):

- a. Screenshot Captures: Automatically purged after ninety (90) calendar days;
- b. Granular URL & App Logs: Retained for one hundred and eighty (180) calendar days;
- c. Summary Timesheets & Payroll Records: Retained for statutory periods (typically 3 to 7 years in accordance with tax and labor audit laws).

13. EMPLOYEE PRIVACY RIGHTS

Employees maintain explicit rights regarding their personal telemetry:

- a. Right to Transparency: Full disclosure of all metrics recorded;
- b. Right to Access: Unrestricted dashboard access to view personal historical logs;
- c. Right to Pause: Freedom to pause tracking instantly for personal errands;
- d. Right to Correction: Ability to request correction of inaccurate timesheet logs.

14. BRING YOUR OWN DEVICE (BYOD) RULES

For team members utilizing personal laptops or home computers:

- a. The tracking agent functions exclusively in manual, user-initiated mode;
- b. The application stops all telemetry collection the moment "Stop" is clicked;
- c. The Company possesses no technical capability to view personal files, photos, search history outside work hours, or home network traffic.

15. REMOTE & DISTRIBUTED WORKERS

Remote and hybrid team members are subject to identical standards as office staff:

- a. Monitoring verifies proof-of-work without requiring invasive surveillance;
- b. Employees are evaluated against agreed deliverables, sprint velocity, and milestones rather than continuous mouse movement;
- c. Time zone differences are respected, with flexible tracking intervals allowed upon supervisory agreement.

16. EMPLOYEE OBJECTIONS & DISPUTE RESOLUTION

If an employee disputes a recorded time entry, an idle flag, or a screenshot capture:

- a. Step 1: Raise the dispute informally with the direct manager within 5 business days;
- b. Step 2: If unresolved, escalate to the HR Department or designated Data Protection Officer (DPO) at [Insert Contact Email, e.g., privacy@company.com];
- c. Step 3: An objective review of audit logs will be conducted, with a written resolution provided within ten (10) business days.

No employee will face adverse retaliation for raising a good-faith privacy inquiry.

17. SECURITY & DATA PROTECTION

All monitoring telemetry is protected by enterprise-grade cryptographic standards:

- a. In-Transit Encryption: All data transmitted via TLS 1.3 cryptographic protocols;
- b. At-Rest Encryption: All screenshots and logs encrypted with AES-256;
- c. Infrastructure: Hosted in SOC-2 Type II and ISO/IEC 27001 certified data centers with multi-factor authentication (MFA) and automated vulnerability scanning.

18. POLICY UPDATES & AMENDMENTS

The Company reserves the right to amend this Policy to reflect technical advances or evolving statutory mandates (e.g., changes under the DPDP Act or labor codes).

Employees will receive at least thirty (30) calendar days of advance written notice prior to the effective date of any material amendments.

19. EMPLOYEE ACKNOWLEDGEMENT & CONSENT FORM

I hereby confirm that I have received, read, and understand the [Company Name] Employee Workplace & Remote Monitoring Policy (Version 3.0).

I understand that the Company utilizes workforce software (e.g., TrackLabs) to record billable time, verify proof of work, monitor application/URL usage during paid hours, and capture periodic blurred screenshots as set forth herein.

I consent to the collection, processing, and retention of my workplace telemetry in strict accordance with this Policy for the duration of my employment or contract.

Employee Full Name: _____

Job Title / Department: _____

Employee ID Number: _____

Corporate Email: _____

Office / Remote Location: _____

Date of Signature: _____

Employee Signature: _____

=====