

Employee Monitoring Policy Template

Template version date: October 2, 2026

This template provides general policy guidance and should be adapted to the laws and working arrangements that apply to your organization. Complete every bracketed field, remove unused options, and obtain appropriate legal/privacy review before adoption.

1. Document control and responsibility

Organization: *[Company name]*. Policy version: *[Version]*. Effective date: *[Date]*. Policy owner: *[Role / department]*. Approved by: *[Approver]*. Next review: *[Date]*.

This policy applies to *[employees / contractors / other covered workers]*, working in *[locations]*, using *[approved devices and systems]*. The organization responsible for the monitoring information is *[Entity and contact details]*. Related documents are *[privacy notice, acceptable-use policy, retention schedule, and any location-specific notices]*.

2. Purpose and justification

[Company name] uses the monitoring described here for *[specific approved purposes, such as reviewed time allocation, investigating a defined operational issue, or protecting named systems]*. The purpose, necessity, less intrusive alternatives, and applicable legal basis are documented in *[assessment / review reference]*.

Monitoring must remain connected to those purposes. A new purpose, a more intrusive collection method, or an expansion of the people covered requires *[approval and review process]* before use. The applicable legal basis and any additional conditions for sensitive information are *[complete after legal/privacy review]*.

3. Information collected and excluded

Only the enabled and approved categories listed below are collected. Replace each bracket with the actual configuration, collection method, and purpose; delete unused categories.

- Time and attendance: *[timestamps, reviewed work periods, breaks, idle signals, and relevant allocation fields]*.
- Application usage: *[application names / window titles / duration / other exact fields; distinguish metadata from content]*.
- Website usage: *[domains / full URLs / page titles / duration; state whether query strings and page content are excluded]*.
- Screenshots: *[enabled or disabled; permitted devices, displays, capture frequency or triggers, and safeguards]*.
- Other monitoring: *[video, audio, keystrokes, email, messages, location, or other methods]*. Methods not expressly listed and approved are disabled. Any proposed use needs a separate assessment and the required notice or authorization.
- Excluded information: *[personal accounts, private files, passwords, health information, confidential communications, or other excluded content]*, with *[technical exclusions and handling procedure for incidental capture]*.

4. Work periods, schedules, and pauses

Routine monitoring operates only during *[approved working periods]*, using *[schedule or employee-started session rule]* in *[reporting time zone]*. Fixed, flexible, overnight, and cross-midnight work are handled by *[specific rules]*. Scheduled absence, leave, breaks, and work away from the device are handled by *[pause / correction / review process]*.

Routine screenshot and work-activity collection are off outside the approved work period. Employees can see the monitoring state and use *[verified start, stop, pause, or private-time controls]*. Where these controls are unavailable, *[alternative arrangement]* applies before rollout.

Any separately approved security logging or exceptional collection outside those periods is described in *[separate notice: purpose, exact fields, authorization, access, and duration]*. It does not silently expand routine productivity monitoring.

5. Screenshot boundaries and safeguards

Screenshots are *[disabled / enabled only for the following purpose]*. Where enabled, capture is limited to *[approved work applications, devices, displays, and working periods]* at *[frequency / trigger]*. The process for excluded applications, screens, and sensitive content is *[verified configuration and procedure]*.

Image blurring or redaction is *[describe whether applied before upload or only to a displayed copy, and whether originals remain]*. Original and protected versions are governed by *[access rules, export permissions, retention, and deletion]*. Do not describe an image as protected without checking each retained version.

An employee who notices inappropriate capture should contact *[privacy contact]* through *[channel]*. The reviewer will restrict access while checking *[incidental-capture procedure]*, document the action, and remove or otherwise handle the information in accordance with *[approved process and applicable obligations]*.

6. Personal devices and remote work

Monitoring on personally owned devices is *[not permitted / limited to the following approved work environment and periods]*. Installation, permitted scope, visibility, separation from personal use, and removal are governed by *[bring-your-own-device arrangement]*. A company-managed alternative is *[describe availability and process]*.

For home and remote work, collection is limited to the approved work activity. Household activity, family members, private surroundings, and personal communications are out of scope. *[Describe safeguards and employee controls.]* Video or audio collection is not enabled merely because an employee works remotely.

7. Access, security, and service providers

The following roles can access the following information for the stated purposes: *[role → fields / report → purpose → approval owner]*. Access is limited to the approved need, reviewed *[frequency]*, and removed when the role or employment arrangement changes. View, download, export, and administrator permissions are *[define separately]*.

[Service provider and hosting locations] process the data under *[contract and responsibility arrangements]*. Safeguards for accounts, transfers, storage, access records, incident response, and international transfers where relevant are *[verified measures and contact]*. Records must remain in approved systems; private copies and unauthorized sharing are prohibited.

8. Client and third-party reports

Clients receive *[no employee monitoring information / only these approved account-specific fields]*. *[Authorized reviewer]* checks the account, permitted fields, purpose, recipient, and sharing method before release. Unrelated accounts, private employee information, and raw screenshots are excluded unless expressly justified, reviewed, and disclosed in the applicable notice.

Client access, report exports, onward sharing, and revocation are governed by *[account-specific rules]*. Client service or SLA measures come from *[operational system]*, rather than being inferred from a computer-activity percentage. Other disclosures are handled through *[review and authorization process]*.

9. Retention, deletion, and exceptions

The approved retention schedule is: time records *[period and trigger]*; app/site records *[period and trigger]*; screenshots and originals *[period and trigger]*; exports *[period and trigger]*; access and review records *[period and trigger]*. Each period has a documented purpose and review owner in *[schedule reference]*.

Deletion covers *[active systems, originals, protected copies, exports, and backup lifecycle]*. *[Responsible role]* verifies expiry and deletion *[frequency]*. A documented legal hold or other approved exception identifies the records, reason, owner, review date, and restricted access. Retention does not extend indefinitely because data is available.

Employee departure, provider changes, and contract termination are handled by *[access revocation, export if needed, return/deletion, and evidence procedure]*.

10. How information is used in reviews

Monitoring information supports *[defined review or investigation]*. Computer activity, idle signals, or screenshots alone do not establish the quality of work or explain why a gap occurred. Reviews consider relevant output, quality, delivery, workload, work away from the device, and the employee's explanation.

Before information is used in a material employment decision, *[human reviewer]* checks the source, accuracy, comparable work, relevant context, and employee response. The process for correction, challenge, and escalation is *[describe]*. Any automated scoring, profiling, or decision process is *[not used / separately described and reviewed, with safeguards and the applicable notice]*.

11. Notice and local requirements

The organization provides this policy and the applicable privacy and statutory notices through *[delivery methods]* at *[required time before monitoring / hiring, as applicable]*. Required workplace postings, receipt records, and language or accessibility arrangements are *[complete for each location]*.

Location-specific notices and additional requirements are recorded in *[reviewed annex]*. This general template does not replace statutory wording, posting, consultation, or other obligations. Material changes to collection, purpose, access, or retention require *[review, configuration update, and renewed information / notice process]* before implementation.

12. Questions, corrections, and individual requests

Questions about monitoring, inappropriate capture, missing work context, or inaccurate records can be sent to *[role and contact]*. Requests to access, correct, object to, restrict, or otherwise exercise applicable rights are handled through *[request procedure and privacy notice]*, subject to the law and applicable exceptions.

[Responsible role] records the request, verifies identity as needed, protects other people's information, and responds within the applicable timeframe. The escalation route is *[HR / privacy lead / relevant external route]*. Raising a concern in good faith will be handled under *[non-retaliation and grievance arrangements]*.

13. Review and approval record

Legal/privacy review: *[Name / role, scope of review, locations covered, date, outstanding actions]*.

Operational configuration tested by: *[Name / role, date, evidence reference]*. Policy approved by: *[Approver, date]*.

Review this policy at *[interval]* and when law, working arrangements, vendors, purposes, capture methods, retention, or access materially change. The policy owner maintains the current version and closes documented actions before the affected monitoring begins.

14. Employee acknowledgment of receipt

I acknowledge that I received the employee monitoring policy, version *[Version]*, and the applicable notices on *[Date]*. I have been told where to find the current policy and how to ask questions or raise a concern.

This acknowledgment records receipt. It is not a blanket consent to monitoring, a waiver of rights, or a substitute for an appropriate legal basis and any separate authorization required by applicable law.

Employee name: *[Name]*. Signature or electronic acknowledgment: *[Field]*. Date: *[Date]*. Organization representative / receipt record: *[Field]*.

Implementation checklist

- ☐ Complete bracketed fields and remove every unused monitoring category.
- ☐ Document purpose, necessity, alternatives, legal basis, and any required assessment or consultation.
- ☐ Complete the location-specific notice, acknowledgment, posting, and privacy review.
- ☐ Match the policy to tested work periods, personal-device rules, and screenshot settings.
- ☐ Check sensitive-content exclusions, blur/original handling, and incidental-capture procedures with dummy data.
- ☐ Test reviewer/client access, exports, employee moves, and access revocation.
- ☐ Approve retention for each record type and test deletion, backups, exports, and exit handling.
- ☐ Explain the policy, record the required notice/receipt evidence, and provide a working questions route.
- ☐ Resolve outstanding review actions, obtain approval, and schedule a meaningful review.

Neebix Editorial Team · <https://neebix.com/blog/employee-monitoring-policy-template>