

Employee Monitoring Policy

Template — replace every bracketed field and delete any section describing monitoring you do not conduct.

This is a template, not legal advice. It does not account for your industry, your states of operation, your collective bargaining agreements or employees located outside the United States. Four US states require notice before monitoring — New York, Delaware, Connecticut and Maine — and their duties differ. Have counsel review this before you issue it. Statutes checked 22 October 2026.

1. Introduction

1.1 Purpose

[COMPANY NAME] (“the Company”) uses certain monitoring tools on Company-provided systems and devices. This policy explains what is monitored, why, what data is collected, how long it is retained, who may access it and what rights employees have. It applies from [EFFECTIVE DATE].

1.2 Scope

This policy applies to all employees, and to [CONTRACTORS / TEMPORARY STAFF / INTERNS — delete as applicable], who use Company-provided devices, accounts, networks or software. It applies to [LIST: Company laptops and desktops, Company email accounts, Company network, Company-issued mobile devices].

This policy does not apply to personal devices operating on personal networks, except where an employee voluntarily enrolls a personal device in a Company programme under section 5.

1.3 Definitions

Monitoring means the automated or manual collection of data about the use of Company systems, as described in section 2.

Company systems means [DEVICES, ACCOUNTS, NETWORKS AND APPLICATIONS provided or paid for by the Company].

Working hours means [THE EMPLOYEE'S SCHEDULED HOURS as recorded in [SYSTEM]].

2. Monitoring we conduct

2.1 Types of monitoring

The Company conducts the following types of monitoring:

WHAT	DATA COLLECTED	BUSINESS PURPOSE
[Time tracking]	[Start and stop times, hours by project]	[Payroll, client billing, project costing]
[Application and website activity]	[Names of applications and sites used during working hours]	[Security, productivity measurement]
[Screenshots]	[Periodic screen captures at [INTERVAL] during working hours]	[Verification of billable work]
[Email and network security scanning]	[Metadata, attachment scanning for malware]	[Information security]
[Physical premises]	[CCTV in the locations listed in 2.2]	[Security of premises and staff]

2.2 Locations

On-premises monitoring takes place in the following locations: [LIST SPECIFIC LOCATIONS].

Connecticut requires the notice to identify these locations and to be posted in them. List rooms and areas, not “all premises”.

2.3 What we do not monitor

The Company does not:

- Monitor personal devices on personal networks;
- Activate webcams or microphones remotely or covertly;

- Record the content of keystrokes;
- Read the content of communications identified as personal;
- Collect the location of employees outside working hours;
- Monitor for the purpose of identifying union activity or other legally protected activity;
- Collect health, financial or other special-category personal data through monitoring tools;
- Monitor [ADD ANY FURTHER EXCLUSIONS].

Every line above is a commitment. Delete any the Company's tools do not actually enforce.

3. Purpose of monitoring

Monitoring is conducted only for the purposes stated in section 2.1. Data collected for one purpose is not used for another without a documented review by [ROLE] and, where required, notice to affected employees.

4. Personal use and expectation of privacy

Limited personal use of Company systems is [PERMITTED / NOT PERMITTED]. Where personal use is permitted, employees should be aware that activity on Company systems is subject to the monitoring described in section 2.

Employees who send personal communications through Company systems may mark them [PERSONAL] in the subject line or equivalent field. The Company will not read the content of communications so marked, except where section 8 applies.

5. Personal devices and personal spaces

5.1 Personal devices

[OPTION A: The Company does not monitor personal devices and does not permit Company data on them.]

[OPTION B: Employees may access Company [EMAIL / APPLICATIONS] from personal devices. In that case the Company collects [SPECIFY] and can [SPECIFY: remotely remove Company data]. The Company does not access personal files, photographs, messages or location data on personal devices.]

An employee may decline to install any Company monitoring or data collection application on a personal device. An employee who declines will be offered a Company-provided device for the work concerned, and declining will not affect their employment in any way. Requests and refusals are recorded by [ROLE].

Required in Maine by 26 M.R.S. § 620-A(4). Sound practice everywhere, because a mandatory install on a personal device is the single most contested line in a monitoring policy.

5.2 Homes, personal vehicles and personal property

The Company does not use audiovisual monitoring — camera or microphone — in an employee's home, in an employee's personal vehicle or on an employee's property.

[WHERE A ROLE GENUINELY REQUIRES IT: The sole exception is [ROLE / TASK], where audiovisual monitoring is required for the duties of the job. The requirement, and the reason for it, are recorded in the role description and reviewed at each policy review.]

Maine bans this outright at 26 M.R.S. § 620-A(3) unless the monitoring is required for the duties of the job. Notice does not cure it and neither does consent, so a camera-on rule for remote staff has to meet the job-duty test or be dropped.

6. Data collected, access and retention

Access. Monitoring data is accessible to [ROLES ONLY, e.g. the employee's direct manager, HR, the IT security team].

Employee access. Employees may request a copy of monitoring data relating to them by contacting [CONTACT]. [WHERE THE TOOLING SUPPORTS IT: employees can view their own activity data at any time in [SYSTEM].]

Retention. Monitoring data is retained for [RETENTION PERIOD] and then deleted, except where a longer period is required by law or by an active investigation or legal hold.

Third parties. Monitoring data is processed by [NAME SOFTWARE VENDORS]. It is not sold, and is not shared with any other third party except [AS REQUIRED BY LAW / SPECIFY].

7. Data security and breach notification

Monitoring data is stored [SPECIFY: encrypted at rest, access-logged] and is protected by the controls set out in [INFORMATION SECURITY POLICY]. If monitoring data is subject to a personal data breach, the Company will notify affected employees and any required authority in accordance with [APPLICABLE LAW] and [BREACH RESPONSE POLICY].

8. Monitoring without prior notice

In narrowly defined circumstances, the Company may monitor without the prior notice described in this policy — specifically, where the Company has reasonable grounds to believe that an employee is engaged in conduct that violates the law, violates the legal rights of the Company or of its employees, or creates a hostile work environment, and where monitoring may produce evidence of that conduct. Such monitoring requires the prior written approval of [ROLE], is limited to what is necessary, and is documented.

This section also does not limit the Company's obligations in connection with a criminal investigation.

[FOR EMPLOYEES HIRED IN CONNECTICUT ON OR AFTER 1 OCTOBER 2026: the Company provides a separate plain-language written statement before the start of work, describing the prohibited activities that may be monitored without prior notice.]

9. Employee rights, questions and concerns

Employees may:

- Ask what data is collected about them and request a copy;
- Ask for inaccurate data to be corrected;
- Raise a concern or object to a specific monitoring practice;
- [EXERCISE ANY FURTHER RIGHTS available under applicable law, including under Regulation (EU) 2016/679 where applicable].

Questions and concerns go to [CONTACT — NAME, ROLE, EMAIL]. The Company will respond within [NUMBER] working days. Raising a concern under this policy will not result in retaliation.

10. Policy review and re-notice

This policy is reviewed every [SIX / TWELVE] months and whenever the Company changes its monitoring tools or a relevant law changes. Last reviewed: [DATE]. Next review: [DATE].

Annual notice. The Company gives written notice to every current employee, at least once each calendar year, that it conducts the monitoring described in this policy. The notice for [CALENDAR YEAR] is sent in [MONTH] by [ROLE], and the dispatch is recorded.

Required in Maine by 26 M.R.S. § 620-A(5), which is owed to all current employees rather than only to those being monitored. It runs on the calendar year, so a notice sent in December and the next in January of the year after next misses a year entirely.

At interview. Candidates are told during the interview process that the Company conducts monitoring. [ROLE] includes the statement in the interview script and in the job posting.

Required in Maine by 26 M.R.S. § 620-A(5). The statute asks only that the candidate be informed and does not require a written record — keep one anyway, because the employer carries the compliance burden.

11. Acknowledgement

I confirm that I have received and read the [COMPANY NAME] Employee Monitoring Policy dated [DATE], and that I have had the opportunity to ask questions about it.

Employee name

Signature

Date

This acknowledgement records receipt of the policy. It is not a consent to any processing for which separate consent is required.

Template only — not legal advice. Have counsel review before issuing. monitask.com/forms/employee-monitoring-policy-template/