Whistleblower Policy

Policy · US · Updated 2026-07-23 · Square brackets are placeholders to replace with your own details.

A whistleblower policy is the written commitment that people who report suspected wrongdoing — safety hazards, fraud, financial irregularities, legal violations, or serious breaches of company policy — have defined channels to report through and will not suffer retaliation for using them. It tells employees what to report, where to take it, and what happens after they do.

The policy earns its keep long before anyone blows a whistle. Problems that reach management early are cheap to fix; the same problems reported first to a regulator, a plaintiff's attorney, or a journalist are not. Employees choose the internal channel only when they believe two things: that the report will be acted on, and that reporting will not cost them their job. This document is where your organization puts both commitments in writing.

This template gives you the reporting channels, the anti-retaliation commitment, the investigation approach, and the confidentiality rules — with the federal protections framed accurately, so the policy promises nothing less than the law already requires.

Purpose and scope

This policy sets out how anyone working for [Your company] — employees, officers, and [contractors and temporary workers, if included] — can report suspected wrongdoing, and what protections they have when they do. It applies to reports about the company, its people, and anyone acting on its behalf.

Nothing in this policy creates a contract of employment or changes the at-will nature of employment at [Your company], and nothing in it restricts anyone's right to report suspected violations of law to a government agency at any time.

What to report

Report anything you reasonably believe involves illegal activity, a serious safety risk, or a serious breach of [Your company] policy. When in doubt, report — deciding whether something qualifies is the investigator's job, not the reporter's. Examples include:

- Safety and health hazards, unreported injuries, or pressure to work unsafely.
- Theft, fraud, or falsification of records, timesheets, or financial statements.
- Bribery, kickbacks, or undisclosed conflicts of interest — see [the anti-bribery policy].
- Violations of laws or regulations that apply to our work: [environmental, licensing, consumer protection — list the areas relevant to your industry].
- Retaliation against anyone for reporting any of the above.
- Harassment and discrimination complaints have their own route under [the anti-harassment policy]; a report made here is routed there, never turned away.

How to report

- To your manager, for anything you are comfortable raising directly — most concerns resolve fastest closest to the work.
- To [HR contact / compliance officer] by [phone, email, or in person], when the concern involves your manager or you would rather not raise it locally.
- Through [the reporting hotline / web form at location], which [does / does not] accept anonymous reports. Anonymous reports are investigated as far as the information allows — the more specific the report, the more we can do with it.
- To [senior leader / the audit committee] for concerns about senior management or financial reporting.
- To a government agency, at any time — before, after, or instead of reporting internally — including OSHA for safety matters and the SEC for securities matters. Internal reporting is encouraged; it is never a precondition.

No retaliation

Retaliation against anyone for making a good-faith report, or for participating in an investigation, is prohibited and is itself grounds for discipline up to and including termination. Retaliation means any adverse action taken because of a report: termination, demotion, discipline, cut hours or shifts, denied promotion or training, exclusion, threats, or harassment.

This protection covers reports that turn out to be unsubstantiated — what matters is that the reporter honestly believed the concern at the time. If you believe you have experienced retaliation, report it immediately through any channel in this policy. Federal anti-retaliation rights, including the right to file a complaint with OSHA, exist independently of this policy and are not affected by it.

How reports are handled

1. Every report is acknowledged within [timeframe] where the reporter is known, with the name of the person handling it.
2. [Name/role] assigns an investigator with no stake in the outcome — never someone the report implicates, and never someone who reports to them.
3. The investigator gathers documents, speaks to the people involved, and records findings. Serious matters — [suspected legal violations, financial reporting concerns, anything involving senior management] — are escalated to [senior leader / counsel / the audit committee] at the outset.
4. The reporter is told when the matter is closed and, where confidentiality allows, what happened in outline.
5. Findings, actions taken, and dates are recorded at [system/location].

Confidentiality and good faith

Reports are handled confidentially: shared only with the people needed to investigate and act, which is a small circle, not the rumor mill. Complete secrecy cannot be promised — a fair investigation sometimes reveals its source — but the duty not to retaliate binds everyone regardless.

Good faith is the only standard a reporter has to meet. An honest report that proves wrong carries no consequences. Knowingly false reports — using this policy as a weapon — are misconduct, handled under [the progressive discipline policy].

Records and review

Reports, investigation records, and outcomes are kept at [system/location], access-restricted to [roles], and retained for [period]. [Name/role] reviews the log [frequency] for trends — repeat subjects, repeat locations, channels nobody uses.

This policy is reviewed [frequency, e.g. annually], after any substantiated retaliation complaint, and when the law changes. Owner: [name/role]. Next review due: [date].

How to use this template

1. Name the real channels first: who answers the [hotline/inbox], who investigates, and who hears reports about senior management — a policy that routes everything to one person fails the day that person is the problem.
2. Decide the anonymity question deliberately: an anonymous channel surfaces more reports; a named-only channel gets more usable ones. Whichever you choose, say so plainly in the policy.
3. If [Your company] is publicly traded or preparing to be, take advice on the Sarbanes-Oxley requirements before adopting this — the audit-committee procedures for accounting complaints are specific.
4. Check your state's whistleblower statute for protections broader than the federal baseline and align the policy to the stronger standard.
5. Train managers on receiving a report: thank, record, escalate, and change nothing about how the reporter is treated — most retaliation claims begin with a manager's first reaction.
6. Publicize the channels where people actually work — posters, onboarding, the handbook. A reporting channel nobody remembers exists only on paper.

Official guidance

- OSHA — Workers' rights and protections
- OSHA — How to file a safety and health complaint
- SEC — Office of the Whistleblower
- EEOC — Retaliation