

Whistleblower Policy Template

A free, adaptable template covering protected reports, reporting channels, confidentiality and anonymity, anti-retaliation, investigation, and the evidence auditors sample. Mapped to SOC 2, ISO 27001, SOX, and HIPAA.

HOW TO USE THIS TEMPLATE

Replace every [bracketed value] with your own. Delete any section that does not apply, keep the numbering, and route the final version through your normal approval process, including review by employment or securities counsel. The values are recommended defaults, not framework requirements: no framework names a whistleblower policy for a private startup. Write rules you can show evidence for every quarter.

Company: [Company name]

Policy owner: [Role, e.g. Compliance Lead]

Version: [1.0]

Effective date: [Date]

Approved by: [Name, title]

Next review: [Date, at least annually]

1. Purpose and scope

Purpose. [Company] is committed to honest, lawful conduct. This policy gives anyone who works for or with [Company] a safe way to raise concerns about suspected wrongdoing, and commits [Company] to investigate those concerns fairly and to protect the people who raise them.

Scope. This policy applies to employees, contractors, interns, board members, advisors, vendors, and former personnel who have information about [Company]'s business.

Related policies. Code of Conduct Policy, HR Security Policy, Incident Management Policy, Security Awareness Training Policy.

2. Protected reports

You may report a concern about any of the following, whether it has happened, is happening, or is likely to happen:

- Fraud, theft, or misstatement of financial information
- Bribery, corruption, or conflicts of interest
- Security misconduct, including attempts to hide or delay reporting of an incident
- Misuse of customer, employee, or other personal data

- Violations of law, regulation, or [Company] policy
- Retaliation against someone who raised a concern

The standard is good faith. You do not need proof. A reasonable, good-faith belief is enough, and you are protected even if the concern turns out to be mistaken. Knowingly making a false report is a violation of this policy. Harassment and discrimination concerns may also be raised through [HR process].

3. Reporting channels

Every concern can be raised through either route. Use the second route if the concern involves the first route's owner or senior leadership.

Route	Contact	Use when
Route 1: Compliance Lead	[Name], [email address or form link]	Default route for any concern
Route 2: Independent contact	[Board member, advisor, or outside counsel], [email address]	The concern names Route 1, a founder, or senior leadership
Anonymous form (optional)	[Form link]	You prefer not to give your name

You may report in writing or ask for a conversation. If you prefer, you may also report to a regulator or government agency at any time, and nothing in this policy requires you to report internally first.

Channel options at a glance

Option	Anonymity	Evidence quality	Fits when
Shared inbox	Weak (sender visible)	Good (email trail)	A starting point, never the only route
Web form to two named people	Moderate	Good (structured fields)	Most teams under 50 people
Third-party hotline	Strong	Good (case records)	Larger teams, EU staff, low trust in internal routes

4. Confidentiality and anonymity

Your identity will be shared only with those who need it to investigate or as the law requires. You may report anonymously through [form link]. Anonymous reports are reviewed with the same care, but [Company] may be less able to investigate or give you feedback, and the facts of a report can sometimes reveal who made it. [Company] will not try to find out who made an anonymous report.

TEST YOUR CHANNEL

An email address that shows the sender's identity is not anonymous. If this policy offers anonymity, file a test report and check what the receiver can see.

5. Anti-retaliation

[Company] prohibits retaliation against anyone who reports a concern in good faith or who takes part in an investigation. Retaliation includes dismissal, demotion, reduced pay or hours, changes to access or responsibilities, exclusion from meetings, an unwarranted negative review, threats, and harassment.

- **Managers** who receive a concern must pass it to a reporting route within [1 business day] and must not investigate it themselves.
- **Nobody** may try to identify an anonymous reporter.
- **Retaliation is a violation** of this policy and is subject to discipline up to and including termination.
- **If you believe you have faced retaliation**, report it through any route in this policy.

6. Investigation procedure

1. **Acknowledge** the report within [5 business days] and say what happens next.
2. **Log it** with a case ID in the case log.
3. **Check for conflicts.** A person named in a report, or whose team is involved, takes no part in handling it.
4. **Triage** by severity. Fraud, legal exposure, and safety come first.
5. **Assign** an investigator who is independent of the matter.
6. **Interview and collect evidence.** Share the reporter's identity only on a need-to-know basis.
7. **Decide** whether the concern is substantiated.
8. **Remediate** the issue and any harm to the reporter.
9. **Close** the case with a written summary.
10. **Give feedback** to the reporter within [90 days] where confidentiality allows.

EU STAFF

If you employ 50 or more people in the EU, the EU Whistleblower Directive (2019/1937) sets acknowledgment within seven days and feedback within three months. National laws differ, so check each country where you have staff.

Case log fields

Field	What it records
Case ID	Unique number, never the reporter's name
Date received and channel	When and how the report arrived

Category and severity	Fraud, security, data misuse, other, with a priority
Owner and conflict check	Who investigates, and confirmation they are independent
Status and outcome	Open, substantiated, not substantiated, or referred
Retention date	When the record may be destroyed, set with counsel

7. Roles and independence

Role	Responsibility
Policy owner [Compliance Lead]	Owns this policy, receives Route 1 reports, keeps the case log, reports case counts to [leadership or board] each [quarter]
Independent contact [Board member or counsel]	Receives Route 2 reports and any report naming the policy owner or senior leadership
Investigators	Independent of the matter, trained in confidentiality
Managers	Pass concerns on within [1 business day] and never retaliate

8. Records and review

- Keep this policy with its version, approval date, and acknowledgments from every person in scope
- Keep the case log, case summaries, and test reports for [retention period set with counsel]
- File a test report through every channel [annually] and keep the record
- Review this policy at least [annually] and after any case that exposed a gap

Confidentiality agreements: carve-out clause

Add language like this to NDAs, separation agreements, and employment agreements. SEC Rule 21F-17 bars impeding communication with SEC staff, and 18 U.S.C. 1833(b) requires notice of whistleblower immunity in agreements that govern confidential information, or a cross-reference to this policy.

SAMPLE CLAUSE

Nothing in this agreement or any [Company] policy prevents you from reporting possible violations of law to a government agency, including the Securities and Exchange Commission, or from cooperating in an investigation, and you do not need [Company]'s permission or notice to do so. Under 18 U.S.C. 1833(b), you will not be held liable under any trade secret law for disclosing a trade secret in confidence to a government official or an attorney solely to report or investigate a suspected violation of law, or in a sealed court filing. See the [Company] Whistleblower Policy for how to raise concerns internally.

Which laws apply at which stage

Your situation	What applies
Private startup, US-only	No federal statute requires a written policy. SOC 2 auditors and customers still ask for one
50 or more employees in the EU	EU Directive 2019/1937: internal channel, acknowledgment within 7 days, feedback within 3 months
Preparing an IPO	SOX Section 301 (audit committee complaint procedures, Rule 10A-3) and Section 806 (anti-retaliation) become live once listed
Handling protected health information	HIPAA 45 CFR 164.502(j)(1) protects workforce whistleblower disclosures; 164.530(g) bars retaliation
Any employer	SEC Rule 21F-17 and the DTSA notice rule (18 U.S.C. 1833(b)) limit what your agreements may say

Framework notes

Framework	Where it lives	What an auditor looks for
SOC 2	CC2.2 (point of focus on separate communication lines), CC1.1, CC2.3	A reachable channel that people know about, and records that it works. A hotline is not mandatory
ISO 27001:2022	Annex A 6.8, 5.24 to 5.26, 6.4, 5.34	Event reporting, incident handling, discipline, and privacy of personal data in reports
SOX	Sections 301 and 806	Public companies: audit committee complaint procedures and anti-retaliation controls
HIPAA	164.502(j), 164.530(g)	Workforce disclosure protections and no retaliation for complaints

Evidence checklist

- Approved policy with version number and date
- Signed acknowledgments from everyone in scope
- Channel screenshot or dated test report for every route
- Case log export, even if it has no entries
- Closed-case summaries with retention dates
- Manager training record

This template is general information, not legal advice. Have employment or securities counsel review the final policy before you publish it. Free to use and adapt. Published by ComplyJet: complyjet.com/blog/whistleblower-policy-template