

conscious SCALING

A prompt-based template for Seed to Series B companies

What is a Whistleblowing policy?

A Whistleblowing policy sets out how an employee or other stakeholder can confidentially raise concerns about wrongdoing inside the company, and how those concerns will be handled. It protects people who raise concerns in good faith from retaliation or detriment.

The policy serves the business as well as the individual. Early signals of problems give the company a chance to fix them before they escalate. A clear, well-known process reduces the risk that issues are reported externally first, or not at all. It reinforces ethical behaviour and signals that the company takes integrity seriously.

Companies of any size and ownership type benefit from having a Whistleblowing policy. In the EU, the Whistleblower Directive (2019/1937) requires companies above 50 employees in scope member states to have internal reporting channels (verify current state in your jurisdiction). The Whistleblowing policy can sit as a standalone document or inside the Code of Conduct or employee handbook.

Example Template

Commitment / statement:

Define your commitment to lawful and ethical conduct and link it back to your values. State clearly that you encourage people to raise concerns and that you protect those who do.

Purpose / Scope of policy:

Describe the objective of the policy and who it applies to.

1. Who can raise a concern

State who can raise a concern under the policy. Typically: all employees, contractors, board members, suppliers, customers and other stakeholders. Cover former employees and job applicants where relevant.

2. What concerns can be raised

State what types of concern the policy covers. Examples include: criminal offences, breaches of law or regulation, serious wrongdoing, financial impropriety, safety risks, environmental damage, bullying or harassment, and behaviour that falls below your established standards. Make clear the policy is for genuine concerns, not personal grievances (which have a separate process).

3. Protection and support for whistleblowers

Set out the protections in place. State that retaliation, harassment, or detriment against anyone raising a concern in good faith will not be tolerated. Confirm your commitment to confidentiality and, where preferred and possible, anonymity. Reference the legal protections that apply in your jurisdiction. Explain what support is available (HR contact, employee assistance programme, external advice line where you have one).

4. How to raise a concern

Make this concrete. Set out the channels available:

- Direct line manager
- An alternative manager or senior leader if the line manager is involved
- HR or People team
- A named board member or non-executive director
- A dedicated email address or web form
- An independent third-party reporting platform (examples: Whispli, NavexGlobal, Vault Platform, Speak Up). These allow anonymous reporting and are increasingly used by growth-stage companies
- External regulators where appropriate (the policy should not deter people from reporting externally where they have a right to do so)

Explain what information to provide and reassure people that they do not need to have proof or know all the facts before raising a concern.

5. What the company will do after a concern is raised

Set out the process clearly:

- Acknowledgement of the report within a defined period (the EU Whistleblower Directive specifies acknowledgement within 7 days; verify current numbers in your jurisdiction)
- Initial assessment and triage
- Investigation, including who conducts it and how independence is maintained
- Communication back to the whistleblower on outcome and next steps within a defined period (the EU Directive specifies feedback within 3 months)
- Action taken, where wrongdoing is found
- What happens if a concern raised in good faith turns out to be unfounded (no detriment); and what happens in cases of malicious or knowingly false allegations

6. Records, oversight and continuous improvement

How are reports logged and tracked? Who has access? How long are records retained (in line with data protection law)? How are themes reviewed by senior management or the board? How are managers trained to receive concerns?

Policy adherence:

All employees should be required to read the policy and confirm they have understood it.

Policy approval:

Who is accountable for this policy day to day? Who is the senior sponsor? How often will it be reviewed and updated (annually as a minimum)?

How to embed this policy

Drafting this policy is the start, not the finish. Use these prompts to make it real:

- Where will the policy live so employees can find it (handbook, intranet, shared drive)?
- How will it be introduced (onboarding, all-hands, training)?
- Who owns it day to day, and who is the escalation point?
- How often will it be reviewed and refreshed (annually as a minimum)?
- How will employees confirm they have read and understood it?
- How will it be communicated to suppliers, customers, and other relevant third parties?

How this policy connects

This policy works alongside others. Cross-reference where helpful:

- Code of Conduct (overarching behaviour and ethics)
- DEI policy (recruitment, fair treatment, inclusion)
- Anti-Harassment & Discrimination policy (protecting against unwanted behaviours)
- Sustainability policy (environment, social and governance)