

Non-Retaliation Policy Template

A standalone, adoptable policy giving effect to the non-retaliation commitments of Chapter 6: definitions, protections, reporting channels, consequences, and monitoring, with every point of adaptation in square brackets.

From *Grievance Mechanisms That Work: Designing and Operating Effective Non-Judicial Remedies* · Thomas Gaultier · thomasgaultier.com/resources/gmtw

This template provides the policy framework for the non-retaliation commitments described in Chapter 6. Adapt it to your organizational context, legal framework, and operating risks. It is a standalone policy that any organization operating a grievance mechanism can adopt: every point requiring adaptation, including references to the organization's own procedures, appears in square brackets.

STANDARDS REFERENCE

UNGP Principle 31 requires that mechanisms be “accessible,” with assistance for those facing barriers to access; its commentary names “fears of reprisal” among those barriers. IRMA Standard requirement 1.4.6.1 (2018) requires that grievance handling protect “the confidentiality and safety of those filing grievances.” IFC Performance Standard 1, para. 35 requires that mechanisms address concerns “without retribution.” This template operationalizes these requirements into an enforceable policy.

[Organization Name]

Non-Retaliation Policy for the Grievance Mechanism

[Effective Date] | Version [X.X]

— 1. Purpose

[Organization Name] is committed to ensuring that any person who files a grievance, provides information in support of a grievance, participates in an investigation, or cooperates with the grievance mechanism in any capacity can do so without fear of adverse consequences. This policy establishes the organization's non-retaliation commitment and defines the protections, reporting channels, and enforcement measures that give effect to that commitment.

— 2. Scope

This policy applies to:

- All employees, officers, and directors of [Organization Name] and its subsidiaries.
- All contractors, subcontractors, and their employees working on [Project Name] or related activities.
- All community members, stakeholders, and other individuals who interact with the grievance mechanism.
- All security personnel, whether employed directly or through third-party providers.

This policy covers the grievance mechanism operated at [site/project/corporate level] and all intake channels, investigation processes, and resolution procedures associated with it.

— 3. Definition of Retaliation

Retaliation is any adverse action taken against an individual because that individual filed a grievance, participated in a grievance process, provided testimony or evidence, or supported another person in doing so. Retaliation includes, but is not limited to:

- Termination, suspension, demotion, or reduction in wages or benefits.
- Transfer, reassignment, or change in work duties intended as punishment.
- Threats, intimidation, harassment, or coercion, whether verbal, written, or physical.
- Denial of access to project benefits, services, or employment opportunities.
- Damage to property, restriction of movement, or interference with livelihood activities.
- Exclusion from community meetings, consultation processes, or benefit-sharing arrangements.
- Adverse action against family members, associates, or community representatives of the complainant.
- Any action by security personnel, public or private, connected to the filing or pursuit of a grievance.

Retaliation may be committed by employees, contractors, community leaders, government officials, security personnel, or any other person acting in connection with the project. [Organization Name] will investigate all credible reports of retaliation regardless of who is alleged to have committed the act.

— 4. Protections

[Organization Name] provides the following protections to all persons who engage with the grievance mechanism:

- **Confidentiality.** The identity of complainants and witnesses is protected under the confidentiality protocols of [reference the organization's grievance procedure]. Access to identifying information is restricted to authorized personnel on a need-to-know basis.
- **Anonymity.** The mechanism accepts anonymous grievances through designated channels. No effort will be made to identify anonymous complainants.
- **Safe reporting of retaliation.** A dedicated confidential channel for reporting retaliation is maintained separately from the general grievance intake. Reports of retaliation may be made to [designated role, e.g., the Compliance Officer, the site General Manager, or the corporate Ethics Hotline]. This channel operates independently of the personnel involved in the original grievance.
- **Interim protective measures.** Where a credible risk of retaliation is identified, [Organization Name] will implement interim measures to protect the individual while the retaliation allegation is investigated. Measures may include temporary reassignment of the alleged retaliator, enhanced security monitoring, or alternative access arrangements for community members.
- **Access to external remedies preserved.** Using the grievance mechanism does not require the complainant to waive any legal rights or access to external mechanisms, including courts, national human rights institutions, regulatory bodies, or OECD National Contact Points.

— 5. Reporting and Investigation

Any person who believes they have experienced or witnessed retaliation should report it through one of the following channels:

- [Designated role/person] at [contact details].

- [Confidential hotline or email] operated by [independent third party, if applicable].
- [Any intake channel of the grievance mechanism], with the grievance flagged as a retaliation report.

All retaliation reports are treated as grievances of the highest severity class and investigated within the timelines and procedures defined for such cases in [reference the organization's grievance procedure]. The investigation is conducted by a person independent of the original grievance and the alleged retaliator. The Grievance Officer monitors all open cases for indicators of retaliation as part of ongoing case management.

— 6. Consequences

Confirmed retaliation by any employee or contractor of [Organization Name] will result in disciplinary action proportionate to the severity of the retaliation, up to and including termination of employment or contract. Confirmed retaliation by a third party (e.g., a community leader, government official, or security provider) will result in [Organization Name] taking all reasonable steps within its influence to address the retaliation, including engagement with local authorities, modification of security arrangements, or other appropriate measures.

— 7. Communication

[Organization Name] will:

- Include a summary of this policy in all grievance mechanism awareness materials distributed to communities and workers.
- Communicate the non-retaliation commitment verbally at every intake and acknowledgment interaction [reference the corresponding steps of the organization's grievance procedure].
- Display this policy in accessible formats and local languages at all intake points, community notice boards, and worker information areas.
- Include non-retaliation training in the onboarding of all staff, contractors, and security personnel who interact with affected communities or workers.
- Report annually, in aggregate, on the number of retaliation reports received and investigated and on their outcomes, as part of the mechanism's performance reporting [reference the organization's reporting procedure].

— 8. Monitoring

The Grievance Officer monitors for retaliation indicators using [reference the organization's retaliation monitoring framework]. Indicators include: complainant withdrawal after initial filing, reports from community focal points, changes in grievance filing patterns from specific communities or worker groups, and direct reports from complainants or witnesses. Monitoring findings are reported in [reference the organization's periodic grievance review].

— 9. Review

This policy is reviewed annually and updated as necessary to reflect changes in the operating context, applicable legal requirements, or lessons learned from retaliation monitoring. The review is conducted by [designated role] and approved by [senior management role].

Approved by: [Name, Title]

Date: [Date]

Next review date: [Date]



No one should pay a price for using the mechanism.

Free to download and to use in your work. Please keep the attribution. These are working templates, not legal advice: adapt them to your operating context and applicable law, with qualified counsel where the stakes require it.