United Nations
Office on Drugs and Crime

Model Speak Up Policy

Approved by the Board of Directors or any other relevant body
XX/XX/202X

Disclaimer

The designations employed and the presentation of material in this information product do not imply the expression of any opinion whatsoever on the part of the United Nations concerning the legal or development status of any country, territory, city or area or of its authorities, or concerning the delimitation of its frontiers or boundaries. The contents of this work do not necessarily reflect the views of the United Nations or its officials, or Member States, or contributory organizations, nor do they imply any endorsement.

This document was produced in a collaborative manner with representatives from the private sector and civil society, under the UNODC project "Strengthening the Integrity and Anti-Corruption Efforts of the Private Sector in Myanmar". It is intended to serve as a model that companies may tailor to their specific contexts and needs. It is designed to be a living document that users are encouraged to review and adapt over time.

For an adaptable version of this document, please contact us at uncac@un.org.

For further information, please visit:

- UNODC Business Integrity Portal (available at: https://businessintegrity.unodc.org/)
- www.businessintegritymyanmar.org

Contents

How to read and tailor this document	
XXX	Baseline
XXX	Parameters to be changed
XXX	Suggestions to consider

Glossary

External stakeholders: customers, clients, suppliers, and communities.

Initial recipient of report: a person in charge of receiving a disclosure made by a reporting person and, in most cases, of handling the initial assessment of a report.

Internal stakeholders: [Company name]'s board of directors, executive leadership, supervisory board members, permanent and temporary employees, contractors, subcontractors, interns, facility management workers, volunteers, and any other relevant persons inside the company. Current and former members of the company, as well as job applicants who may observe wrongdoing or malpractice in the recruitment process, are also included here.

Reportable wrongdoing: an instance of actual or potential work-related violation of the Code of Conduct of [Company name], as detailed in section 3 of the policy.

Reporting channel: a system established to disclose alleged misconduct or wrongdoings in a safe and inclusive manner and designed to minimize the risk of retaliation.

Abuse of scheme: Any stakeholder who intentionally reports false or misleading information with a motive to obtain personal advantage or to cause intentional harm to someone commits an abuse of the scheme and will be subjected to disciplinary sanctions.

Whistle-blower: A person, entering in the personal scope of this policy, who discloses a reportable wrongdoing in the context of his/her professional activity or work-related context, based on reasonable grounds to believe that the information is true at the moment of reporting, and using the established reporting channels.

Retaliation: any direct or indirect detrimental action that adversely affects the employment or working conditions of a whistle-blower, where such action has been recommended, threatened, or taken as a result of a report made in the framework of the policy.

Executive summary

[Company name] commits to the highest levels of integrity, honesty, accountability, and responsibility. The Speak Up Policy encourages internal (and external stakeholders) to raise concerns or speak up confidently about reportable wrongdoings by any internal stakeholders of [Company name]. The policy details processes and procedures for raising concerns through different reporting channels, the protection of reporting persons, and the company's investigation process.

[Companies need to determine if they choose to cover external stakeholders under this policy. If so, this should be reflected across the policy.]

1. Purpose

The objectives of the Speak Up Policy are to:

- Encourage stakeholders of [Company name] to comply with ethical conduct and promote a culture of integrity.
- Inform stakeholders of what is considered reportable wrongdoing in the company.
- Provide clear guidance to stakeholders on how to report wrongdoing.
- Inform stakeholders about their reporting rights and obligations.
- Provide whistle-blowers with protection against retaliation.
- Guide the internal investigation and documentation process.
- Identify and take appropriate measures against ethical and legal risks that may cause harm to the company and its reputation, as well as to its internal and external stakeholders.

[Companies should develop the purpose of the policy according to their own corporate values and what they aim to achieve with the policy. Companies should also consider whether they want to cover different internal and external stakeholders in addition to what is mentioned in this template.]

2. Speaking Up

Speaking Up means reporting one's concern or knowledge about reportable wrongdoings of [Company name]'s internal stakeholders to the responsible units or individuals of the company.

At [Company name], we encourage you to report promptly any knowledge of or concerns you may have about reportable wrongdoings. This must be done on reasonable grounds, meaning to:

- Make a report with the belief that the alleged wrongdoing has occurred, is occurring, or is likely to occur.

- **NOT** to report intentionally false or misleading information with a motive to obtain personal advantage or to cause intentional harm to someone.

3. What should you speak up about?

At [Company name], we consider that any violation of our Code of Conduct or policies is a wrongdoing. You may speak up about potential or actual work-related wrongdoing, including an omission, which has occurred, is occurring, or will likely occur.

Examples of reportable wrongdoings may include, but are not limited to, the following:

- Non-compliance with the company's Code of Conduct, values, or rules.
- Misconduct, which in this case is defined as conduct relating to financial, human resources and sexual concerns that breach the Code of Conduct.
- Breaching of various national or international laws and regulations, as well as industry standards,
- Fraudulent activities that may include misappropriation of funds and misrepresentation of financial information.
- Asking for, giving or receiving bribes to influence decisions that have a bearing on the business.
- Discrimination or harassment based on factors such as gender, sexual orientation and race.
- Creating of a hostile workplace environment through intimidation or harassment.
- Non-disclosure of a conflict of interest that could compromise decision-making.
- Unauthorized usage of the company's assets and resources for personal gain.
- Unauthorized usage or disclosure of the company's confidential and sensitive information for personal gain or business advantage.
- Threatening to retaliate against a reporting person, their family members or the facilitators of the whistle-blowing or investigation process.
- Any other conduct that can cause harm to the health, safety, and security of the [Company name]'s employees, the community or environment in which the business is operating or to its customers.

Although the Speak Up Policy does not cover the following, you are encouraged to raise a concern through the [Grievance Policy/Procedure] regarding:

- Grievances or concerns relating to HR matters, for instance, terms of employment or performance-related issues or treatment at work.
- Personal or legal disputes.
- Customer complaints.

4. Who is protected against retaliation?

The following company's internal (and external) stakeholders are protected by the Speak Up Policy when raising their concerns or speaking up about misconduct or wrongdoings:

- Member of the Board of Directors.

- Executive leadership.
- Permanent and temporary employees.
- Interns.
- Facility management workers, volunteers, etc.
- Contractors/Subcontractors.
- Family members of reporting persons.
- Personnel handling reports and participating in an investigation.
- Facilitators of the whistle-blower process or investigation process as well as persons wrongly identified as the whistle-blower.

[Companies need to determine if they choose to cover external stakeholders under the whistle-blowing policy, and reflect this across the policy to include customers, clients, suppliers and communities.]

5. How to raise a concern

At [Company name], we encourage concerns about wrongdoings to be raised internally whenever possible. This can be done through your direct supervisor, or a senior manager above your immediate supervisor. You can also contact the compliance department as the need may arise. At [Company name], we provide different reporting interfaces, such as email, WhatsApp/SMS, physical letter, in-person reporting, and an online reporting platform. Each reporting channel ensures the confidentiality of the reporting person throughout the process. Any concerns, reports, and information received through these channels will be treated confidentially.

If you are comfortable raising your concern through an email, you may directly make a report to compliance.team@xxx.xyz using the template provided in the annex section. When raising a concern or speaking up about wrongdoings, we encourage you to provide as much information as possible for the [Compliance Department] to evaluate the report and, if necessary, conduct an investigation afterwards.

Anonymous reporting is possible as long as the evaluation of the reports shows that the person raised a concern based on reasonable grounds and provides as much detailed information as possible for the report to be effectively processed (see 5.1).

Any stakeholders covered by the present policy seeking guidance on reporting possibilities can reach out to their [line managers] or [Compliance Officer] through the different reporting channels.

5.1 Anonymous reporting

Information from anonymous sources will be assessed and may lead to an investigation. However, anonymous allegations are often more difficult to pursue as there may be no way for the [investigation team] to clarify the information provided or to ask follow-up questions. If you choose to remain anonymous, please provide as much detail as possible and consider providing some means to contact you if further information or clarification is needed. For instance, consider providing us with a free web-based email address with an assumed name or alias that will allow you to retain your anonymity.

You can also make use of our anonymous online reporting platform that is accessible through [this link]. The platform provides an anonymous, two-way communication channel that ensures your safety and anonymity, while enabling the exchange of information, in the event that more details are required to support an enquiry based on the report filed. The system does not track any sensitive information, such as location data and IP addresses.

[Companies need to determine the reporting channels and to provide detailed information about them also in the SOPs and in other related documents. In these documents, it should be clear under what conditions the reporting is confidential and can be anonymous.]

6. Protecting whistle-blowers

6.1 Responsibility of the organization

At [Company name], we protect the identity of whistle-blowers (name, gender, rank, department, telephone number and telephone extension, email address, IP address, etc. of the reporting person, as well as to the extent possible any information that can lead to a determination of these elements and eventual identification of the whistle-blower.).

Additionally, we seek to protect whistle-blowers from any form of retaliation. Retaliation means any direct or indirect detrimental action that adversely affects the employment or working conditions of an individual, where such action has been recommended, threatened, or taken for the purpose of punishing, intimidating, or injuring that individual because of the reporting action they engaged in according to the present policy. This includes, inter alia:

- Harassment, coercion, intimidation, discrimination, or bullying, including based on gender.
- Unsubstantiated negative performance appraisals or feedback that is not reflective of actual performance.
- Unjustified contractual changes, such as non-extension or termination of appointment, demotion, reassignment, transfer, dismissal, reductions in (or deductions of) work hours and wages; suspension, loss of promotion opportunities, isolation, reduction of work responsibilities, etc.
- Unjustified modification of duties; unjustified non-authorization of holidays and other types of leave, or a change of location of work.
- Unreasonable delays in authorizing travel, or the provision of entitlements.
- Threats of retaliation.
- The imposition or administration of any disciplinary measure, reprimand, or other penalty, including those of a financial nature.
- The threat of violence, damage to property, or any other action that would result in injury or other crime.
- Violence, damage to property or any other action that would result in injury or other crime.
- Counter-allegations that are unfounded or untrue.

- Blacklisting (a sector- or industry-wide agreement, whether formal or informal, which prevents an individual from finding alternative employment).
- The provision of inaccurate or untrue information in an employment reference to prevent an individual from obtaining future employment, or the refusal to provide a reference when requested to do so.
- Prosecution under civil or criminal law for breach of secrecy, libel, or defamation.
- Any other unfair treatment or reprisal (threatened or actual) not otherwise covered by this list.

[Companies should contextualize this list according to their operations and modify the retaliation list to fit their needs and context.]

This protection is also applicable to:

- Witnesses of the wrongdoing.
- Colleagues of the whistle-blower, including those identified as the whistle-blowers.
- Facilitators (including initial report recipients, investigators, managers, and others tasked with handling whistle-blower reports).

6.2 Responsibility of the whistle-blower

The whistle-blower is also responsible for safeguarding the confidentiality of the information reported, such as the name of the alleged personnel. The reporting person must not be involved in investigating the reported issue and should not engage with the alleged party to obtain more information.

6.3 No retaliation

We have a zero-tolerance approach to any form of retaliation against reporting persons who report on reasonable grounds. If you witness or face retaliation, we encourage you to file a complaint against retaliation. Any person filing a complaint against retaliation is encouraged to make the complaint in a written form to document it. For such cases of retaliation, we also provide an alternative reporting mechanism in order to keep the issues separate. To ensure proper management of the case, a different officer from that in charge of investigating the alleged wrongdoing will be charged with investigating the alleged retaliation.

Any person found to have abused the scheme or retaliated against another for reporting, handling reports or participating in an investigation, will face disciplinary action. This may include termination of employment for [Company name]'s employees and termination of the engagement or contractual arrangements or other appropriate action in case of third parties.

7. Investigation or fact-finding

The company investigates reports according to the [Management Procedures]. Generally, the following procedure applies to each report: initial assessment, investigation, or fact-finding, making decisions,

closing the case, reporting and following up. Throughout the process, we ensure the confidentiality of the reporting person.

7.1 Initial assessment

Upon receiving a report, the [Compliance Department] will send an automatic acknowledgment message to the reporting person provided the reporting person has indicated a way to contact them. The [Compliance Department] then evaluates the report based on the information provided if it is made on reasonable grounds and will contact the reporting person if the report has not been made anonymously. [This may take up to 7 working days.]

7.2 Investigation or fact-finding

The [Compliance Department] assigns a trained [investigator] or [an investigation team] to assess if the allegations in the report meet the relevant criteria established in the present policy. The [investigator] or [an investigation team] may ask for more information from the reporting person, if necessary and possible. The [investigator] or [an investigation team] conducts the investigation confidentially, objectively, and fairly. [This may take up to 30 working days.]

[Criteria should be set by the organization that implements this policy.]

7.3 Making a decision

If the investigation or fact-finding shows that the allegation of wrongdoing is determined to be true or is very likely to be true, the [investigator] or [an investigation team] reports the findings to the [Compliance Committee]. Based on the findings, the [Compliance Committee] makes a decision and recommendation to the [management] and [HR department].

7.4 Closing the case and reporting

The [investigator] or [an investigation team] produces a report, including all relevant violations, facts, and evidence, to approve or disapprove the allegations. The report is then secured, and the [Compliance Department] ensures that no one has access to it except authorized personnel. The [Compliance Department] informs the reporting person about the closure of the case. [This may take 1 to 7 working days.]

[Companies should contextualize the content to fit their needs and processes.]

8. Documentation and confidentiality

The [Compliance Department] records, documents, and keeps all reports confidential, and the company ensures that no one has access to them except authorized persons. The reports and information will not be disclosed without the reporting person's' consent. However, the company may reveal the reporting

information on a need-to-know basis, such as the reporting persons' identity, under certain circumstances, such as when:

- The Board of Directors considers that it is in the best interest of the company to reveal the information.
- Government authorities demand the information.
- The company concluded that the allegations were malicious and intentionally falsified or misleading.

Before disclosing such information, the reporting person must be consulted.

9. Contact

For any questions concerning the policy, you can contact [Company name]'s [Compliance Department] at compliance.team@xxx.xyz.

Annex

Speak Up Report Form

REPORTING FORM (CONFIDENTIAL)
Complainant's Information
I prefer to remain anonymous, understanding that the investigating team may not be able to obtain additional details from me or pursue appropriate action on the matter due to my anonymity (if so, please do not provide any identifying information that could compromise your anonymity): Yes No
Complainant Name:
Email Address:
Physical Address:
City, State, Zip:
Mobile Phone Number:
Work Address:
City, State, Zip:
Work Phone Number:
Are you a current (company name) stakeholder: Yes No
Are you a former (company name) stakeholder: Yes No
What is your exact current status/position within the company:
Are you a citizen (member of the general public): Yes No
Has this issue been reported to any other party: Yes No
If yes, to whom:
Information of Alleged Person(s)
Alleged Person(s) Name:
Address:
City, State, Zip:
Phone Number:
Department:
Location:
What is the exact current position of the alleged individual(s):
Information/Details of the report
What would you like to report?
Describe the incident(s) as clearly as possible. Include a complete description of the conduct and the place – with as many facts and data as possible. Please remember to include the Who (Subject of report), What (issue), When (date of incident), and Where (location of incident). Attach additional documents as necessary:

Is there any specific evidence (e.g. documentation, witnesses) that you are aware of, and how can they be located or contacted?
Date: