TRANSPARENCY INTERNATIONAL
the global coalition against corruption

# INTEGRITY VIOLATIONS REPORTING POLICY

Issued by: Chief Executive Officer
Applicable to: Chair, Vice-Chair, Chief Executive Officer, National Chapters, Individual Members, Board of Directors, International Council, employees, third parties
Last updated: 2021
Date of next review: 2022

# INTEGRITY VIOLATIONS REPORTING POLICY

## 1. INTRODUCTION

The Transparency International Secretariat (TI-S) is committed to advancing accountability, integrity and transparency. As an organisation, we aim to be an example of good management, ethical practice and openness to greater transparency and accountability. Through the preventative components of its Integrity System, TI-S aims to reduce the likelihood and impact of incidents in which those who work for and represent the organisation fail to exhibit the standards of behaviour that TI-S expects, or act in accordance with TI's Mission, Vision, Values and Guiding Principles ('integrity violations'). However, TI-S recognises that this risk can never be entirely eliminated through preventative measures alone.

When they occur, TI-S's ability to effectively and efficiently manage incidents of (suspected) integrity violations and protect our staff, organisation and other stakeholders from risk, is contingent on it having a trusted system through which violations, suspected violations, or related integrity concerns can be safely and confidentially reported to an appropriate person.

TI has long recognised the important role of whistleblowers in preventing and detecting wrongdoing. TI-S has developed this Integrity Violation Reporting Policy to ensure that those who report do not suffer any repercussions for their efforts.

This document outlines the procedures for reporting a (suspected) integrity violation or related integrity concerns and details the support and protections available for those that raise reports. The procedures are designed in line with the international standards and best practices that TI advocates for.

## 2. PURPOSE

The purpose of this policy is to:

- encourage individuals working for and with TI-S and other stakeholders to report suspected integrity violations committed by or within TI-S, through its reporting channels
- establish the circumstances in which such reporting shall be considered a requirement of TI-S employees
- provide guidance on how to report a suspected integrity violation, or related integrity concern, safely and confidentially
- explain what measures TI-S will take to protect the identity of those that report integrity violations/raise integrity concerns
- explain how TI-S protects those that raise reports from potential unfair treatment and retaliation

## 3. SCOPE

### 3.1 Who Can Use This Policy to Report Concerns?

Anyone can report under this policy. This includes all those working for or with TI-S (e.g., staff, consultants, volunteers, suppliers, donors, partners and affiliates, including staff members of TI EU, the TI US office and TI National Chapters, etc.), Members of the TI Movement, as well as members of the public.

Reports and/or concerns can be raised by those who have been subjected to, affected by, witnessed, received information about, or otherwise suspect the commission, or attempted commission, of any

(active, previous, attempted or potential) integrity violation.

In relation to interpersonal integrity violations, violations might be directed towards, or suffered or experienced by, specific individuals. These are referred to in this policy as **Affected Persons**. Whilst reporting is encouraged, Affected Persons are under no explicit or implied obligation to report violations directed towards, or suffered or experienced by them.

For the purposes of this policy, 'TI-S staff' includes all contracted employees (including volunteers and interns) of the Transparency International Secretariat, including TI-US.

## 3.2 What is Reporting?

The terms "reporting" and "whistleblowing" are often used interchangeably. In this policy, the term *reporting* is used to describe the process of communicating information of any (suspected) integrity violation within, by, or on behalf of TI-S to a relevant point of contact either internally or externally.

### 3.2.1 Internal and External Reporting

*Internal reporting* refers to the use of the functions within TI-S's Integrity System to communicate information of any (suspected) integrity violation within, by, or on behalf of TI-S. These are detailed below and include the **management line**, **Integrity Manager** or **External Whistleblowing Reporting Point**.

*External reporting* refers to situations in which a report of (suspected) integrity violations is raised directly with entities that are external to TI-S, such as competent authorities, the media, civil society organisations, legal associations, trade unions or business/professional organisations or the public. External reporting is often deemed necessary when an organisation's internal reporting channels have failed, or are not trusted.

### 3.2.2 Integrity Violations

Integrity violations to which this policy applies include:

- violations of the TI-S Code of Conduct and related TI-S policies,
- criminal offences and breaches of law,
- damage or risk of harm to human rights, the environment, public health or safety
- acts to cover up any of these

when committed by anyone working for and under any form of contract or agreement with TI-S, including prospective and current employees, executive staff, interns, contractors, volunteers or consultants, in the context of their work within, or on behalf of TI-S. In case of doubt about whether a concern falls within the scope of this policy, the Integrity Manager can be contacted for advice.

# 4. REPORTING OBLIGATIONS

## 4.1 Interpersonal Integrity Violations

Interpersonal integrity violations include breaches of the Code of Conduct relating to **discrimination**, **bullying and harassment**, **sexual harassment** and **sexual exploitation and abuse**. Such breaches are more specifically defined in the Code of Conduct (Note: reporting obligations with regard to child abuse concerns are specified below, see Child Protection).

Whilst reporting is encouraged from those that have suffered, been subjected to, or personally affected by, interpersonal integrity violations (**Affected Persons**), Affected Persons are under no explicit or implied obligation to report violations directed towards, or suffered or experienced by them.

In order to maintain a safe, respectful and inclusive working environment, TI-S staff members who witness, or are aware of the occurrence of interpersonal integrity violations are expected to take action to challenge, prevent or report them, where possible after consulting the Affected Person. Where safe and appropriate to do so, required action might include: offering or providing support to those impacted by the violations (or associated risks); intervening or challenging inappropriate conduct directly, or; offering/providing support or guidance to an Affected Person during their reporting of the issue. If appropriate, staff are strongly encouraged to report such violations in accordance with the procedures established in this policy. If in doubt, staff should discuss the issue with their manager, the Integrity Manager, the Works Council, or others as detailed in this policy.

## 4.2 Non-Interpersonal Integrity Violations

TI-S staff members that know or suspect the commission, attempted commission, or planned/intended future commission, of a *non*-interpersonal integrity violation (as defined in the Code of Conduct and above) *must* report it in accordance with the (internal or external) reporting procedures established in this policy.This obligation to report shall apply unless the Reporting Person reasonably believes that the submission of a report would put them at risk of physical or psychological harm, unfair treatment or retaliation. In this event, staff members are *strongly encouraged* to consider the additional safeguards available through channels of anonymous (including via the External Whistleblowing Reporting Point) and external reporting, as detailed in this policy. Staff in such circumstances are strongly encouraged to seek confidential guidance from the Integrity Manager or to consult the policies that comprise the Integrity System regarding options available for safe reporting (including opting to remain anonymous in the submission of their report) and the support and protections available for those that report integrity violations and concerns.

## 4.3 Child Protection

Any suspected or alleged incidents of child exploitation or abuse or non-compliance with the standards of behaviour defined in the Child Protection Policy *must* be reported through one of the designated reporting channels detailed in this policy. Such incidents must also be reported to the relevant authorities (usually the police) via the Chief Executive Officer (CEO) representing the organisation. This is a legal obligation.

# 5. INTERNAL REPORTING

## 5.1 How to Make a Report Internally

Reports of suspected integrity violations can be made verbally or in writing to any of the following three channels. Reporters are free to choose whichever channel they feel is most appropriate. Reports can be made verbally or in writing to a (1) TI-S Line Manager, (2) the TI-S Integrity Manager, or (3) the External Whistleblowing Reporting Point, as follows:

### 5.1.1 TI-S Line Manager

TI-S staff may opt to report their concern to their line manager (where applicable) or, if necessary or preferred, more senior managers in the management line.

Any manager receiving a report shall transmit it to the Integrity Manager (IM) after collecting the consent of the reporting person (in consideration of the Reporting Obligations). They should not investigate or dismiss the report themself. The manager should not share information about the report, including the identity of the reporting person, to anyone other than the IM. In some circumstances the manager may feel it is necessary not to reveal the identity of the reporter to the IM when communicating the report. In these circumstances the manager may be asked to support the IM as an intermediary for any necessary ongoing communication with the original reporter.

If the IM is implicated in the report or has a potential conflict of interest, then the manager will communicate the report to the CEO. If both the IM and the CEO are implicated or have a potential conflict of interest, then they will communicate the report to the Board of Directors. These specific scenarios are detailed below (5.4).

### 5.1.2 TI-S Integrity Manager (IM)

Reports can be submitted directly to the IM by anyone, in any circumstances. Their contact details are available online in TI's public website and TI intranet.

### 5.1.3 External Whistleblowing Reporting Point

Anyone can report suspected integrity violations to the External Whistleblowing Reporting Point. The External Whistleblowing Reporting Point can, upon request of the reporting person, remove information that might identify the source of their report before sharing it with the IM and serve as an intermediary to facilitate communication between the reporting person and the IM and/or any other relevant parties.

If the IM is implicated in the report or has a potential conflict of interest, the External Whistleblowing Reporting Point will communicate the report to the CEO. If both the IM and the CEO are implicated or have a potential conflict of interest, then they will communicate the report to

the Board of Directors. These specific scenarios are explained below (5.4).

Contact details for the External Whistleblowing Reporting Point can be found online on TI's public website and TI intranet.

## 5.2 Suggested Information to Include in an Internal Report

When submitting a report via the integrity system, it is recommended that a reporter should include as much of the following information as they have available:

1. Broad description of the suspected violation
2. Detailed information, where available:
    - What happened? Detailed description of what the reporting person knows about the issue or incident(s) and how they came to know about it
    - Who is involved? Who is responsible? Was anyone else involved? Who is/are the potential victims or affected persons? Who else knows about the issue? Were there any witnesses?
    - When did the incident(s) occur? Information about dates and times.
    - Where did the incident(s) occur?
    - Anything else?
3. Date of report
4. Preferred contact details

If the reporter has legitimate access to documents or other items in support of their report (e.g., photos, screenshots, documents, messages, emails), then these should also be provided. However, reporters should not attempt to obtain items or information that are not already in their possession, or legitimately available to them. The reporter should not seek to investigate the matter themselves prior to submitting their report.

## 5.3 TI-S Response to a Reported Integrity Violation

### 5.3.1 Initial Acknowledgment and Escalation of a Report

Following the receipt of a report through any of the internal reporting channels listed above reports shall be acknowledged/escalated within the following timeframes:

**Reports Received via Management Line or External Whistleblowing Reporting Point (EWRP)**

- The manager or EWRP receiving the report will acknowledge receipt to the reporting person and request consent[1] to transmit the report to the Integrity Manager (or alternative reporting point, as per the Alternative Reporting Options, below – 5.4) within 3 working days.[2]
- The manager or EWRP will share the report with the Integrity Manager (IM) within 2 working days of receiving consent to share.[2]
- The IM will acknowledge receipt of the the report to the reporting person (if known to the IM, or otherwise via the manager or EWRP[3] where possible) – within 2 working days of receipt.

**Reports Received via Integrity Manager**

- The IM will acknowledge receipt of the report to the reporting person within 2 working days.

### 5.3.2 TI-S Response Process Following Receipt of a Report

TI-S's response to a reported integrity violation will ordinarily follow a 5-step process. This process is broadly outlined at Annex 1.

The Integrity Manager (IM) is responsible for assessing the report. They will document the report and determine whether or not it relates to a potential integrity violation.

[1] Received reports relating to child protection concerns, or in which there is a reasonable belief that any person may be at risk of serious physical harm or death, must be reported to the Integrity Manager or relevant authorities in all cases. In such circumstances and if necessary, the person receiving the report must make all reasonable efforts to remove any information from it that might identify its source.

[2] Wherever possible, it is advised that consent to share a report be obtained in writing either at the time, or via retrospective written confirmation of a verbal agreement.

[3] Intermediaries shall be expected to pass on communications with a reporting person within a reasonable timeframe. In most circumstances this shall be within 2 working days, unless extenuating circumstances prevent them from doing so.

If the report does not relate to a potential integrity violation, the IM will direct the reporting person (if known) to the appropriate channel where applicable (e.g., HR, Works Council). If the identity of the reporting person is not known to the IM, then they should themselves refer the report (unless the content of the report is such that onward sharing would be inappropriate).

If the report refers to a potential integrity violation, the IM will conduct a preliminary assessment and advise to the CEO as to the next step(s) to be taken (e.g., formal investigation, management action, HR grievance procedures, policy review, staff training, etc.). In most cases these steps shall be led by the IM with support from/in collobaration with relevant stakeholders as necessary (e.g., HR, the Legal Team, the WoCo, etc.).

TI-S's response to integrity violations (including investigation and, where necessary, disciplinary measures) shall follow due process in accordance with relevant legal and procedural requirements (i.e., applicable codes of labour law). In the case of interpersonal integrity violations (particularly those relating to sexual exploitation, harassment and abuse) the response shall observe 'victim/survivor focused' principles when appropriate[4]. This means that the response process will be conducted in a way that avoids re-traumatisation, and prioritises the well-being, needs and wishes of Affected Persons.

If, at any stage in the response process, a Reporting or Affected Person wishes to appeal against or challenge an action or decision made in the management of that process, they may opt to escalate the matter to the CEO or Chair/Vice Chair[5] as appropriate. Additionally, the legal rights and protections of all parties involved in a reported integrity violation (including those accused of misconduct) must be duly observed at all times. Any party that feels such rights and protections have been breached may also consider seeking independent legal advice in relation to possible external legal recourse.

### 5.3.3 Response Process Timeframe

TI-S strives to resolve cases in a timely manner. In standard cases, TI-S will complete the response process within 6 weeks. However, extensions of this timeframe are possible when duly justified (e.g., in the case of particularly complex or serious incidents, unavoidable absences of key witnesses or stakeholders, etc.). Where possible, the IM shall inform reporting and/or affected persons of undue delays in the response process (see Progress Updates below).

### 5.3.4 Progress Updates

Throughout the response process, the Integrity Manager will provide regular progress updates to the reporting and/or affected person(s)**,** including the following:

- next steps in the process
- timeframe for next steps and when they can expect further feedback
- where relevant, reasons for limited details of feedback
- information on available support and measures taken for their protection where required
- information on responsibilities of the organisation
- information on responsibilities of the reporting person
- the final outcome of the case, subject to relevant legal and data protection standards, and with due regard to the confidentiality of any disciplinary process. Where outcome information cannot be provided, the reasons for this will be duly explained

In considering the level of information that can be shared with a reporting/affected person, the Integrity Manager must balance necessary considerations of privacy, confidentiality, as well as any sensitivies as to the issues raised or otherwise encountered during the response process, against the legitimate interests and concerns of a reporting/affected person. Information that might undermine the integrity or confidentiality of an investigation process would not ordinarily be

[4] See https://www.unhcr.org/5fdb345e7.pdf. Further explanation of the application of victim/survivor focused principles shall be detailed in the TI-S Investigations Protocol (pending).

[5] The function of the Chair and Vice Chair is as determined in the Transparency International Charter.

shared. For example, where decisions and/or conclusions have been informed by otherwise confidential information that was accessed or obtained during an investigation, it may not be possible to provide detailed explanations of such decisions/outcomes to a reporting person. In cases of interpersonal integrity violations *not* reported by the affected person(s), consent of the affected person(s) must be obtained by the IM before progress updates can be shared with a reporting person.

### 5.3.5 Onward Reporting of Criminal Conduct to Relevant Authorities

If a report and/or investigation reasonably indicate the commission of a criminal offence, TI-S's organisational stance shall be to proactively report externally to the relevant policing authorities. In some limited circumstances however, the CEO (in consultation with the IM, Legal Team, or affected person(s)), may opt not to report an incident. These circumstances shall be limited to cases in which:

- consent from an affected person is not provided or cannot be obtained,
- the conduct in question is so minor in nature that police involvement would be disproportionate or unduly onerous,
- relevant policing authorities are already aware of the issue,
- it is reasonably believed that the involvement of policing authorities would create an unacceptable risk of serious harm to any individual, or
- TI deem that the conduct in question has been criminalised contrary to human rights standards and/or TI's values, or that its criminalisation is otherwise unethical in nature.

Concerns over the reputational impact on Transparency International of reporting the conduct shall not be considered reasonable grounds for non-reporting.

In some circumstances, it may be a legal requirement to report criminal offences to the authorities. In Germany, examples would include offences that fall within S.138 p.1 of the German Penal Code, or certain breaches of the Child Protection Policy. Mandatory reporting requirements will differ according to the jurisdiction in which the relevant conduct occurred, and so in each case legal advice shall be obtained by the IM.

## 5.4 Alternative Internal Reporting Options

In some cases, reporters may feel that the internal reporting options are inappropriate. The below table summarises potential scenarios in which a reporter might wish to consider alternative internal reporting options and guidance on how reports should be raised and managed in such circumstances.

In all cases, the protections detailed in this policy apply and must be taken into consideration by those responsible for managing the response to a report (including IM, CEO, TI Board and TI Chair/Vice Chair).

| # | Situation | Applicable Procedure |
|---|---|---|
| **1** | IM is implicated in misconduct by the report. | Reporter may:<br>▪ report directly to the CEO<br>▪ eeport to line manager or EWRP and request they transfer report to the CEO instead of the IM<br>The CEO will take the role that would normally be fulfilled by the IM. This means that the CEO will assess the report and manage the response/investigation.<br>In no circumstances shall the IM be permitted to investigate a report in which they are implicated in misconduct. |

| | | |
|---|---|---|
| **2** | IM has a conflict of interest in the issues reported. | Reporter may:<br>▪ report directly to the CEO, explaining the details of the conflict of interest<br>▪ report to line manager or EWRP – explaining the conflict of interest – and request they transfer the report and details of the apparent CoI to the CEO instead of the IM<br>The CEO will assess the report and determine if there is actually a conflict of interest and, if so, whether the conflict can be effectively mitigated. If a conflict cannot be mitigated, the CEO will themselves assess the report and manage the response/investigation process without involvement of the IM.<br>If the CEO determines that there is no conflict of interest or is able to apply measures to effectively mitigate a conflict, then the report shall be passed to the IM to manage (in accordance with necessary mitigation measures).[6]<br>In no circumstances shall the IM be permitted to investigate a report in which they have a conflict of interest, or risk of conflict of interest that has not been effectively mitigated. |
| **3** | CEO is implicated in misconduct by the report. | The reporter may:<br>▪ report directly to the IM<br>▪ report to line manager or EWRP and request the report be transferred to the IM without the involvement of the CEO<br>The IM will then bypass the CEO in their management of the issue; reporting directly to the Board of Directors.<br>The Board of Directors will manage the response/investigation process, with support from the IM if appropriate. In no circumstances shall the CEO be permitted to oversee or directly manage the response to a report in which they are implicated in misconduct. |
| **4** | CEO has a conflict of interest in the issues reported. | The reporter may:<br>• report directly to the IM, explaining the CEO's apparent conflict of interest<br>• report to line manager or EWRP and request they explain the CEO's apparent conflict of interest in their onward reporting to the IM.<br>The IM will assess the concern and determine if there is actually a conflict of interest and, if so, whether the conflict can be effectively mitigated.<br>If a conflict cannot be mitigated the IM will bypass the CEO in their management of the issue; reporting directly to the Board of Directors. The Board of Directors will manage the response/investigation process, with support from the IM if appropriate.<br>If the IM determines that there is no conflict of interest, or is able to apply measures to effectively mitigate a conflict, then the CEO shall be permitted to retain their ordinary oversight/decision-making role during the response/investigation process (in accordance with necessary mitigation measures).[6]<br>In no circumstances shall the CEO be permitted to have a decision-making role in a response/investigation process in which they have a conflict of interest, or risk of conflict of interest that has not been effectively mitigated. |

[6] If the case relates to an interpersonal integrity violation, the CEO or IM shall communicate this decision to the reporting/affected person, at which point they may opt to withdraw their report, or otherwise utilise alternative reporting options as detailed in this policy.

| | | |
|---|---|---|
| **5** | Both the CEO and IM are implicated in misconduct and/or have a conflict of interest in the issues reported. | The reporter may:<br>▪ report directly to the Board of Directors, explaining the IM/CEO's apparent conflict of interest or implication in misconducted<br>▪ report to line manager or EWRP and request the report be transferred to the Board of Directors without the involvement of the IM and CEO.<br>The Board of Directors will manage the response/investigation process. |

# 6. EXTERNAL REPORTING[7]

## 6.1 External Reporting to the Competent Public Authorities

TI-S has developed its internal reporting system so as to make it safe and accessible for those who wish to report a suspected violation of integrity. However, Transparency International recognises the right of staff members to report suspected wrongdoing directly to the competent authorities either instead of, or in addition to, a report made internally. In Germany, competent authorities would include, for example:

- Anti-Diskriminierungsstelle des Bundes (Federal Anti-Discrimination Agency)
- Landesamt für Arbeitsschutz, Gesundheitsschutz und technische Sicherheit Berlin (Berlin State Office for Occupational Health and Safety Protection)
- the police/law enforcement agencies
- Berlin Financial Supervisory Authority (BaFin)

In some specific instances, this is a legal obligation.[8]

TI-S employees may opt, therefore, to report their concern directly to competent public authorities and fully bypass the internal reporting mechanisms.

## 6.2 Public Reporting

TI-S recognises that public reporting is part of the right of freedom of expression. TI-S commits to ensuring that its internal integrity system is sufficient to effectively address suspected integrity violations but – where this is considered unsafe, compromised, or has otherwise proved ineffectual – TI-S acknowledges that some people might feel it necessary to report information about suspected integrity violations to external public parties (such as the media, civil society organisations, or the general public), particularly where they feel that this is the only effective means of addressing them.

With the exception of Affected Persons reporting interpersonal integrity violations, TI-S employees are ordinarily required to first use either TI-S's internal reporting mechanism or report via external competent public authorities before disclosing concerns publicly. In accordance with the standards set by the EU Directive on Whistleblowing, the protections detailed in this policy shall apply to reporters that report concerns directly to the public in the following circumstances:

- No appropriate action was taken in response to a report previously made through TI-S Integrity System and then to the competent authorities, or directly to the competent authorities, within a reasonable timeframe. In most cases, a 'reasonable timeframe' shall be considered 3 months from receipt of a report, however this may be extended to 6 months where duly justified.[9]
- The reporting person has reasonable grounds to believe that there is an imminent or manifest danger to the public interest (e.g., emergency situation, risk of irreversible damage).
- The reporting person has reasonable grounds to believe that, in reporting through the internal channels, there is a risk of retaliation, or a low prospect of the wrongdoing being effectively addressed due to the particular circumstances

[7] For the purposes of this policy, external reporting refers to any report made outside of TI-S's internal reporting channels.

[8] Sec. 138 para. 1 German Penal Code: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1396

[9] Explanations for delays in a response outcome shall be provided to the reporting/affected person in accordance with the considerations detailed above (see Progress Updates).

of the case (e.g., where evidence may be concealed or destroyed, or those involved in the management of the response may be in collusion with the perpetrator or themselves involved in the issue of concern).

# 7. SUPPORT AND PROTECTION FOR REPORTING PERSONS

## 7.1 Individuals Protected

The protections listed in this section shall be extended to persons as follows:

1. reporting persons – defined as persons reporting suspected integrity violations under this policy with the reasonable belief that the information reported is true at the time of reporting. Protection is extended to reporting persons regardless of the outcome of the response process, including those who made inaccurate reports in honest error;[10]
2. persons associated with the reporting person:
    i. family members and close personal associates of the reporting person
    ii. legal entities that the reporting person owns, works for, or is otherwise connected to
    iii. any person who has assisted or attempted to assist a reporting person
3. any person who is believed to be a reporting person;
4. any person participating in the handling of a report;
5. any person who refuses to carry out or take part in any suspected integrity violation.

## 7. 2 Protection of the Identity

### 7.2.1 Confidentiality & Data Protection

All those involved in the receipt, management and oversight of reports must ensure that they maintain confidentiality in all cases. They must treat all reports and related information in confidence and manage any related records or data securely. Information related to a case will be shared on a strictly 'need-to-know' basis, with protection to the maximum extent possible of the identity of the parties involved, as well as any information that may reveal their identity.

Reporting persons who feel they require additional guarantees for the protection of their identity can make a report via the External Whistleblowing Reporting Point and ask them to remove information that might reveal their identity from their report.

In some circumstances, it may be a legal requirement that the identity of the reporting person is disclosed to additional parties. This might be the case in situations in which a reported concern results in criminal investigation or prosecution, civil litigation, or other judicial process, and TI-S are legally compelled by the authorities to disclose all files or information pertinent to the case. Disclosures might need to be made either to the relevant authority/court, a legal adviser/representative, or other involved parties such as defendants, plaintiffs, respondents, etc. The reporting person should be notified via the Integrity Manager (or other senior manager, as appropriate) as soon as possible. The IM should follow all reasonable measures to communicate this notification, however in some circumstances (e.g. where the identity of the reporting person is unknown or cannot be established, there are no means to contact the reporting person, such contact is legally prohibited, etc.), this may not be possible. Potential additional measures to protect a reporting person from unfair treatment or other potential repercussions should be considered by a senior stakeholder panel, comprising the CEO, Integrity Manager and either Head of HR or Head of Governance and Legal in consultation with the reporting person. Where legal action has been instigated by TI-S, this senior stakeholder panel must ensure that the risk of such disclosure is duly considered in the decision to pursue the action. The reporting person must be consulted and their views taken into account.

In all other cases, the identity of the reporting person can only be revealed by those involved in the

[10] In the handling of reports, it shall be presumed that the person making the report did so in the honest belief that the information was true at the time of reporting, even if ultimately it was found to be inaccurate. This shall be the case unless, through the investigation process, clear and convincing evidence is identified that a false, misleading or otherwise inaccurate report was made knowingly by the reporter.

receipt, management and oversight of reports with the express consent of the reporting person. When collecting that consent, an explanation should be provided in writing about why the disclosure of their identity is deemed necessary and to whom it will be disclosed, as well as any information about potential additional measures that will be taken to protect them from unfair treatment or retaliation.

The identity of a reporting person will not ordinarily be revealed to any person(s) implicated in potential wrongdoing (the 'Accused Party'), unless in circumstances in which this was legally obligated, as above. In the event of disciplinary action, an Accused Party would have a right to respond to evidence against them (as compiled during the investigation process), but this would not include the identity of the original source of the complaint. In relation to an interpersonal integrity violation, the identity of an affected or reporting person might be implicit by the facts and nature of the incident(s) in question. This might also be the case with a non-interpersonal integrity violation in which the reporting person is the only person that could have known about or witnessed the conduct in question. Options regarding confidentiality in such cases shall be discussed between the IM and affected/reporting person prior to the commencement of an investigation process.

### 7.2.2 Anonymous Reports

TI-S fully recognises the right of reporting persons to remain anonymous. Reports made anonymously through the internal channels provided by TI-S under this policy (e.g., unsigned letter or anonymous email to the IM) will be treated as seriously as non-anonymous reports and in accordance with this policy.

Anonymity, however, has its limitations:

- It will be practically difficult for TI-S to provide comprehensive protection to a person whose identity is unknown.
- Assessments of reports may be limited in scope or focus where it is not possible to communicate or seek further information/clarification from the reporting person.
- The reporting person will not be informed of the progress and outcome of the investigation.

Therefore, while TI-S accepts anonymous reports and respects the wishes of those who want to remain anonymous, TI-S encourages the use of the External Whistleblowing Reporting Point. This reporting channel provides an extra layer of protection of the identity – by not disclosing the identity of the reporting person to the person handling the case – while enabling communication via an independent intermediary.

Alternatively, reporting persons that wish to remain anonymous are advised to consider utilising/providing alternative means of nameless contact when making their report, such as through anonymous email accounts.

## 7.3 Protection Against Unfair Treatment

TI-S will take necessary measures to prevent and remedy unfair treatment resulting from internal and external reporting.

### 7.3.1 What is Unfair Treatment Resulting from Reporting?

Unfair treatment or retaliation resulting from reporting is any threatened, recommended or actual, direct or indirect act or omission, which occurs in a work-related context linked to reporting. This includes, for example:

- suspension, dismissal or equivalent measures
- demotion or withholding of promotion
- transfer of duties, reduction or limitation of work assignments, change in working hours
- unfair selection for tasks or attendance at events
- restrictions on or removal of available resources, such as budgets or human resources
- withholding of training
- a negative performance assessment or employment reference
- unwarranted inspection or investigation of duties, or disclosure of the result thereof
- imposition or administering of any disciplinary measure, reprimand or other penalty
- coercion, intimidation, harassment or ostracism
- discrimination, disadvantageous or unfair treatment
- failure to convert a temporary employment contract into a permanent one, where the

worker had legitimate expectations that they would be offered permanent employment

- failure to renew, or early termination of, a temporary employment contract
- harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income
- blacklisting
- early termination or cancellation of a contract for goods or services.

## 7.4 Protection Against Lawsuit

TI-S will not enter into agreements that might waive or obstruct a reporting person's rights and protections. TI-S will not pursue legal action against a reporting person for a report made in accordance with this policy (internally or externally). TI-S will not pursue legal action against individuals who disclose relevant restricted information in a report made internally or externally in accordance with this policy.

These protections do not extend to those who disclose or report information that they know to be false, inaccurate or misleading.[10]

## 7.5 Complaint of Unfair Treatment Resulting from Reporting and/or Breach of Confidentiality

A complaint of unfair treatment resulting from reporting or a complaint of breach of confidentiality under this policy can be made through the TI-S Integrity System, in accordance with this policy. The same measures and process as detailed in this policy shall be applied.

Those found to have been responsible for unfair treatment resulting from reporting may face disciplinary action, including dismissal, as well as reporting to authorities if their actions constitute a violation of the law. Where the unfair treatment relates to the conduct of a TI associate outside the secretariat (such as at a TI National Chapter, for example), this shall be escalated by the Integrity Manager to the Board of Directors for action.

Where unfair treatment/retaliation resulting from a report is committed by an external party (e.g. a TI-S supplier), TI-S may consider pursuing civil, criminal, or administrative, legal action through the relevant authorities. Where identified, such conduct may result in the termination or non-completion of an existing contractual relationship.

## 7.6 Remedies and Compensation for Unfair Treatment

If it is established that unfair treatment is occurring/has occurred, TI-S will take necessary action to stop that unfair treatment and protect the physical, financial and psychological wellbeing of the person and to remedy any loss, including indirect and future losses and financial and non-financial losses. To the greatest extent possible, the reporting person and other protected individuals listed in this policy should be restored to a situation they were in – or would have been in – had they not suffered unfair treatment. Examples of restorative actions that might be considered include, but are not limited to:

- reinstatement of the person either to the position they occupied before retaliation or to a similar position with equal salary, status, duties and working conditions
- fair access to any promotion and training that may have been withheld
- restoration of duties, if possible
- recognition of lost time and impact on performance
- withdrawal of litigation against a reporting person
- deletion of any records that could constitute a dossier for blacklisting or later retaliation
- relaunching a procurement process
- restoration of a cancelled contract
- apologies for failures
- financial compensation for past, present and future lost earnings
- financial compensation for pain and suffering (including medical expenses)

## 8. FOLLOW UP AND AVAILABLE SUPPORT RESOURCES

TI-S provides staff with support resources, where needed, before, during and after any reporting process. Several resources, listed below, are available to assist individuals who are experiencing or have experienced unfair treatment for information, referral, emotional support and physical/mental health assistance. Information about the available services that are available is accessible to all staff via the Integrity Manager and HR. Such information shall be proactively provided by the IM to all (identifiable) reporting/affected persons following the receipt of a report. These include:

**Internal support resources offered to TI-S staff**

- Team Managers
- Integrity Manager
- Human Resources Team: for support, guidance and referral to appropriate psychosocial support services and for operational arrangements in the workplace aimed at reducing mental/psychosocial stress
- Works Council: for assistance or mediation if you submit a complaint of discrimination or unfair treatment through the available reporting channels as per Sec. 84 of the Works Constitution Act
- External Whistleblowing Reporting Point

**External support resources offered to TI-S staff**

HR and/or the Integrity Manager can provide detailed information on external support resources,[11]which include:

- Confidential counselling on conflicts and mental health issues or in crisis situations (individual support and/or group sessions)
- Assistance with physical and psychological health issues

[11] Many of these services can be provided free of charge for TI-S employees. Further guidance on support coverage availability and costs should be sought from HR.

## 9. COMMUNICATION AND TRAINING

This policy shall be made available to all TI-S staff and the public. Additionally, the Integrity Manager is responsible for providing training on this policy to all staff on a regular basis (at least once per year) and as appropriate to their roles and functions in the TI-S Integrity System. This policy should therefore be:

- Published on the TI website, the TI intranet and signposted in TI-S offices
- Included in the induction programme and mandatory annual refresher training sessions
- Mentioned in agreements with chapters, suppliers, consultants, service providers, etc.

Individuals who have a specific role in the integrity system will receive training in the operation of the policy and in how to handle reports of wrongdoing and prevent/address retaliation.

## 10. CONTINUOUS MONITORING AND REVIEW

Following its implementation, the effectiveness and suitability of this policy must be continually reviewed by the Integrity Manager. On a quarterly basis, the IM will compile the data and analyse trends related to the number of informal contacts and formal reports of wrongdoing received, the nature of the issues reported and resolution processes carried out and the reporting person's feedback including satisfaction with the reporting system. Statistical data relating to the functioning of this policy shall be reported to all staff by the Integrity Manager annually. This policy will be reviewed annually and improved as necessary. The review will be led by the Integrity Manager, in cooperation with relevant stakeholders.

# ANNEX 1

The table below summarises the general response process that TI-S shall apply following the submission of a report through its internal reporting mechanisms. For the purposes of the Integrity Violations Reporting Policy, the 5 steps of the response have been broadly summarised to provide clarity to Reporting/Affected Persons as to the process through which a report shall be managed. A more comprehensive explanation of TI-S case management and investigation processes shall be available in the Investigations Protocol (pending).

In all circumstances, the response process must be in accordance with the guiding principles of TI-S's Integrity System: accessibility, confidentiality, data protection, fairness and due process, safety and security, independence, mutual responsibility, clarity and proportionality. Guidance on the interpretation and application of these principles is available in TI-S Integrity System – Strategic Framework.

| Step | Actions |
|---|---|
| **Step 1: Receiving a Report** | Following the receipt of a report through any of the internal reporting channels, reports shall be acknowledged/escalated as follows:<br><br>**Reports Received via Management Line or External Whistleblowing Reporting Point (EWRP)**<br><br>• The manager or EWRP acknowledges receipt and requests consent to transmit the report to the Integrity Manager (IM) **within 3 working days**.<br><br>• The manager or EWRP shares the report with the IM **within 2 working days** of receiving consent to share.<br><br>• The IM acknowledges receipt of the the report to the reporting person (if known to the IM, or otherwise via the manager or EWRP where possible) – **within 2 working days** of receipt.<br><br>**Reports Received via Integrity Manager**<br><br>The IM acknowledges receipt of the report to the reporting person **within 2 working days**. |
| **Step 2: Assessing a Report** | The Integrity Manager (IM) documents and assesses the report, determining whether or not it relates to a potential integrity violation.<br><br>If the report does not relate to a potential integrity violation, the IM directs the reporting person (if known) to the appropriate channel where applicable (e.g., HR, Works Council). If the identity of the reporting person is not known to the IM and the IM has no reasonable means of contacting them to obtain consent, then they refer the report themselves (unless the content of the report is such that onward sharing would be inappropriate).<br><br>If the report does relate to a potential integrity violation, the IM conducts a preliminary investigation and provides advice to the CEO[12] as to the next step(s) to be taken.<br><br>The possible outcomes of the **preliminary investigation** are:<br><br>▪ **That an investigation is warranted**<br><br>• There is objective evidence or compelling indicators that an integrity violation has, or might have, occurred, requiring formal investigation beyond the scope of a preliminary investigation.<br><br>• Note: the issue identified for investigation might differ in focus from the suspicion as it was initially reported. Additionally, if the preliminary investigation |

[12] In the event that the IM believes that the CEO unreasonably declines to follow their advice appropriately, or that such a disagreement between the IM and CEO cannot be appropriately resolved, the IM may escalate the matter to the Chair or Vice Chair.

indicates that a criminal act may have taken place, the matter might need to be reported externally to the police or relevant authorities.

- Cases requiring investigation shall progress to *Step 3*.

- **That non-investigative response actions are required**
  - Further investigation is not justified, necessary, proportionate, or possible, however other response actions are required. This might include referrals to other functions (such as HR), TI chapters, or external entities, or other follow-up actions such as risk analyses, training or mediation.
  - Cases requiring actions other than referrals (i.e., mediation, informal resolutions, policy review, further training, etc.) shall progress to *Step 4*.
- **That no further action is necessary**
  - There is insufficient information available to justify the need for formal investigation or to continue a formal response to the report. This would apply where the information reported cannot be corroborated, or where the review has not identified any indicators of an integrity violation, or other risks or concerns requiring action.
  - Cases requiring no further action shall progress to *Step 5*.

The IM communicates the outcome of the preliminary investigation to the reporting person and/or affected person, as appropriate. Appeals against the outcome of a preliminary investigation may be raised to the CEO in the first instance, or alternatively to the Chair/Vice Chair.

**Step 3: Investigating a Report**

The procedure for a preliminary investigation and any subsequent investigation procedures is detailed in the Investigation Protocol (pending).

If an investigation is instigated, it must follow due process, relevant legal codes and (where appropriate) victim/survivor centred principles.

Investigations will ordinarily be ordered by the CEO and conducted either by the IM, or by an external party overseen by the IM.

**Step 4: Taking Action**

Once the investigation is concluded, the Integrity Manager advises the CEO as to appropriate measures to be taken. This could include mediation, training, changes in policy, support actions/redress for an affected person, etc.

If the investigation finds that an integrity violation has taken place, the Integrity Manager advises the CEO as to any appropriate, proportionate sanction(s) against any identified culpable party (in consideration legal advice and applicable employment law standards).

The CEO (in consultation with relevant parties, e.g., HR and the Legal Team) determines what (if any) follow up measures should be undertaken, including the commencement of disciplinary action when necessary.

**Step 5: Concluding the Response**

The IM ensures that the case and outcomes are appropriately documented and retained. Including the retention of relevant process records and items of evidence.

Records relating to disciplinary hearings and outcomes are retained in the relevant employee's HR file

The IM communicates case outcomes to the reporting person and/or affected persons, as appropriate.

Transparency International
International Secretariat
Alt-Moabit 96, 10559 Berlin, Germany

Phone: +49 30 34 38 200
Fax: +49 30 34 70 39 12

ti@transparency.org
www.transparency.org

Blog: transparency.org/en/blog
Facebook: /transparencyinternational
Twitter: @anticorruption