

INTEGRITY STANDARD OPERATING PROCEDURES

REPORTING AND HANDLING SUSPECTED BREACHES

SEPTEMBER, 2023

CONTENTS

- 1. INTRO 4
- 2. SCOPE 4
- 3. REPORTING INTEGRITY CONCERNS..... 4
 - What To Report? 4
 - Why Report? 4
 - Who Can Report? 5
 - How To Report? 5
 - False And Malicious Reporting 5
 - The Role Of Confidential Advisors 6
 - Protection Of Complainants And Whistle-Blowers From Retaliation 6
 - Data Safety..... 6
- 4. SUPPORT TO THOSE AFFECTED 7
- 5. HANDLING OF INTEGRITY CONCERNS OR ALLEGATIONS..... 7
 - Step 1: Receipt Of The Complaint *24 Hrs* 7
 - Step 2: Pre-Assessment And Registration Of The Complaint *48 Hrs*..... 8
 - Step 3: Identification Of Decision Maker/Committee And Case Committee *48 Hrs* 8
 - Step 4: Case Management *Ongoing* 10
 - Step 5: Investigation *1 Month (Ideally)*..... 10
 - Step 6: Follow-Up *1 Week* 11
 - Special Cases: 12
- 6. DISCIPLINARY MEASURES..... 12
- 7. GRIEVANCE PROCEDURE 13

8. GLOSSARY 13

ANNEX 1 REPORTING FORM 15

ANNEX 2 FLOWCHART..... 17

ANNEX 3 CASE MANAGEMENT RACI-TABLE 18

ANNEX 4 CONFIDENTIALITY AGREEMENT TEMPLATE 19

ANNEX 5 INVESTIGATION TERMS OF REFERENCE TEMPLATE 20

1. INTRO

These Integrity SOPs describe the Standard Operating Procedures for reporting and handling suspected integrity breaches. It consolidates the *Whistle-blower Regulations*, the Case Handling procedure laid out in the *Policy regarding (Un)desirable Behaviour*, and the *Handling Irregularities and/or Integrity Violations* document.

These Standard Operating Procedures should be read in conjunction with:

- Integrity Framework
- Cordaid's Code of conduct
- Safeguarding policy
- Fraud policy
- Conflict of Interest policy
- Anti-terrorism & Anti-money laundering policy
- Data protection policy
- Information Security policy

2. SCOPE

These procedures apply when the alleged perpetrator of misconduct is a representative of Cordaid and Cordaid subsidiaries, including members of the Supervisory Board, directors, staff, consultants, volunteers and interns. Further, it applies to implementing partners and suppliers who are contracted for the purpose of reaching Cordaid's objectives. It also applies to the beneficiaries and any other persons or parties who come into contact with Cordaid programs.

3. REPORTING INTEGRITY CONCERNS

Representatives of Cordaid and persons outside Cordaid who come into contact with (contracted partners of) Cordaid are mandated to report suspicions or concerns of integrity breaches.

What to Report?

Any concerns, suspicions, or allegations of integrity breaches, as outlined in the policies related to Safeguarding, Fraud, Conflict of Interest, Anti-Terrorism and Anti-Money Laundering can be reported.¹

Why Report?

Allegations of integrity issues should be reported to the organisation for two key reasons:

1. For any person affected to receive support and to put a stop to the misconduct,
2. To hold Cordaid accountable and to help Cordaid identify and manage risks and trends, which can be used to strengthen the culture of integrity within the organization, e.g. by dismissing staff that doesn't respect Cordaid's integrity standards.

¹ Where complaints relate *exclusively* to disagreements or conflicts regarding labour rights, such as contracting, benefits or performance appraisal, the complaint procedure laid out in the [Legal Status Regulations](#) or local HR Manuals applies. Where complaints or incidents relate *exclusively* to security, the [security incident reporting procedure](#) applies.

Who can Report?

Anyone including Cordaid representatives or any external parties who come into contact with Cordaid can report concerns or allegations about integrity breaches. This means that not only staff, consultants, volunteers, or interns can report, but also third parties like beneficiaries, suppliers or staff of partner organizations.

Anonymous reports can be made via the online reporting form called 'EthicsPoint'. Cordaid will treat anonymous reports as any other report as long as sufficient information is available to process the complaint. Please also see Cordaid's commitment to Confidentiality, Protection of complainants and others involved (*under nr. 4*), and Support to those affected (*under nr. 5*).

How to Report?

To make a report about an integrity issue, both allegations of fraud and corruption and other allegations of integrity concerns relating to interpersonal misconduct, you have different options:

Channels for reporting are as follows:

Online via www.cordaid.org/en/reporting-integrity-concerns-and-security-incidents/.

Directly to the Anti-Corruption and Anti-Fraud Officer and the Integrity and Safeguarding Officer via integrity@cordaid.org,

To the immediate or higher supervisor who will then submit the report to the Anti-Corruption and Anti-fraud Officer or Integrity and Safeguarding Officer. In case of a partner, consultant or supplier - to the manager in charge of their contract. Persons who have formed suspicions may also report to higher supervisors where the immediate supervisors are implicated or they feel the immediate supervisor will not take the report seriously,

Staff who are unable to report to their line manager or directly to the Integrity Officer or to the Anti-Corruption and Anti-Fraud Officer (Fraud and corruption allegations) may also use the external whistle-blowing channels to report. These external channels are:

An external Whistle-blower Service via +31 (0)88 1331 030, via email to advies@huisvoorklokkenluiders.nl, or directly [online](#) (Dutch). To report (suspected) misconduct via the House of Whistle-blowers, the wrongdoing must be of public interest and as well as based on reasonable suspicions.

Make use of Cordaid's international networks: ACT Alliance by sending an email via complaintsbox@actalliance.org or Caritas Internationalis directly to Caritas Internationalis Secretary General (If the complaint is against the Secretary General, then the Complaint Handling Officer will report to the President.)

Cordaid representatives and any other external parties who intend to make reports of allegations of integrity breaches are encouraged to exhaust the internal reporting channels first unless in the instances where they believe the allegations raised will not be taken seriously.

Note: If you have suspicions or concerns of an integrity breach, do not try to investigate the issue yourself. Your only responsibility is to report the concern or the allegation, from there it is the responsibility of the Case Committee to deal appropriately with the concern.

False and malicious reporting

Reports of allegations of integrity breaches must be made in good faith. Intentionally submitting false report(s) shall constitute a misconduct for which disciplinary measures will be imposed. Disciplinary measures will not be taken against an individual who reports a misconduct in good faith even if the allegations are not substantiated after an investigation or review is conducted.

The Role of Confidential Advisors

Country/Cluster Offices and the Global Office of Cordaid in The Hague all have Confidential Advisors, a 'person of trust'. Cordaid also has an external Confidential Advisor who is not an employee of Cordaid. Cordaid representatives can find names and contact details of all Confidential Advisors on the [Integrity page](#) on SharePoint (internal).

Confidential Advisors are there to listen and support Cordaid representatives. Together you can explore whether and what action you can take when you experience or witness misconduct – the decision remains with you. Conversations will be treated confidentially. For more details on the role of Confidential Advisors, check [SharePoint](#) (internal).

Protection of complainants and whistle-blowers from Retaliation

Cordaid considers complaints as vital signals that help the organization fulfil its *Duty of Care* and ensure that we *Do No Harm*. A report of (suspected or alleged) misconduct must never have negative effect on the person reporting the allegation. The staff reporting the allegations or suspicions of integrity breaches must be protected by the management team and direct supervisor against any reprisal.

Cordaid will not tolerate any type of retaliation against complainants, people affected, witnesses, those tasked with handling a case or those supporting the person affected. This includes but is not limited to dismissal or other unilateral contractual changes, transfers of location or duties, inhibiting professional chances, not granting or imposing benefits (e.g., sick leave, leave days), aggression and violence, bullying, ignoring, excluding, making unfounded or disproportionate criticism about the complainant and their performance, intimidating or threatening the complainant, or equivalent, *because* of the complaint.

When you fear or experience retaliation or breaches of confidentiality, please include this in the initial complaint or reach out to the Case Committee, the Integrity Officer, or a Security Advisor (if you fear for your safety). On a case-by-case basis, suitable measures will be put in place to ensure your protection.

Any form of retaliation or deterring anyone from reporting will be treated as a misconduct and will be subject to disciplinary measures.

Data Safety

Cordaid respects confidentiality and has a responsibility to protect sensitive personal data in line with Cordaid Data protection policy and Cordaid Information Security policy. To help protect the confidentiality of integrity issues and the privacy of those involved, the following will apply for emails and documents containing sensitive information:

- Wherever identifying details (e.g., names, job title, etc.) are included: mark subject of the email/name of the document as 'Confidential' or 'Strictly Confidential'. In documents, add 'Confidential' or 'Strictly Confidential' in the header and add a Watermark 'Confidential'.
- Wherever sensitive, but not directly identifying details are included (e.g., Gender & Integrity Assessments): mark subject of the email/name of the document as 'Restricted'.
- Do not mention identifying details in the subject/title of emails/documents.
- Do not share any data with people who are not involved in the response to a case ('need-to-know rule'), e.g., do not share the original complaint with the Subject of Complaint.
- Ensure that emails, folders, documents, and notes can only be accessed by those authorized, and password-restrict the access wherever possible.
- Cordaid's data and information will be encrypted to ensure it remains secure and all Cordaid laptops will have Bit locker (encryption) capabilities.

Breach of confidentiality and data protection protocols will be treated as a misconduct and will be subject to disciplinary measures.

4. SUPPORT TO THOSE AFFECTED

People affected by misconduct or retaliation might need access to different psychosocial, medical, legal, or security-related services. The Confidential Advisors are responsible for overseeing and facilitating the required services for those people who report incidences of misconduct to them. The Integrity and Safeguarding Officer will be responsible for facilitating the required services (if necessary) to those who make reports of misconduct allegations through the Cordaid internal reporting channels. The services can be offered either internally or externally, depending on capacity and taking into account the preference of the person affected. Support services are to be paid by the integrity budget of the respective country/cluster office. In exceptional cases, financial support by GO can be requested. Requests will be assessed on a case-by-case basis. A Mapping of available support services per Country Office is available on [SharePoint](#).

5. HANDLING OF INTEGRITY CONCERNS OR ALLEGATIONS

Any person who receives a concern or allegation of misconduct of a Cordaid representative is responsible to provide 'First Aid' and to ensure that the complaint is followed up appropriately. In case of *acute* security risks, please follow the security incident reporting.

A flowchart and RACI-Table illustrating the Case Handling process can be found in Annexes 2 and 3. Please note that the time indications for each step are indicative.

Step 1: Receipt of the complaint 24 hrs

- If in a conversation: ask key questions (what, when, where, who witnessed, etc.), but do *not* investigate or judge the situation. In case of potentially traumatic incidents (e.g. following sexualised violence), do not ask for details.
- In case of *acute* psychosocial, medical, legal, or security needs that cannot wait, make sure that these needs are met (e.g., going to hospital, police, safe place, etc.). Note that in case of serious sexualized violence, such as rape, those affected need to be able to access medical emergency care within 72hrs of the incident. See also Cordaid [Safety First Policy](#) for guidance on acute incidents. Only involve people who *need* to know to help with the response.
- In case of serious incidents (e.g., child abuse), make a first verbal report to the Integrity and Safeguarding Officer as soon as possible.
- Fill in the reporting form [online](#) or use the form in Annex 1 and send it to integrity@cordaid.org within 24 hours of receiving the complaint.

In the instance where a Confidential Advisor is made aware of an allegation of an integrity breach, the Confidential Advisor will provide information about the reporting procedures which can be followed i.e., both the internal reporting procedures or criminal or civil proceedings, and their consequences. The Confidential Advisor is only mandated to report the complaint to the competent authority when he/she is of the opinion that the content of the complaint warrants this (e.g., in case of mandatory reporting in child abuse cases). The Confidential Advisors make analysis of the reported integrity incidents and use this analysis to advise the Management Board on the policies and measures to be taken, without disclosing identifying details of particular cases.

- If the report was done in writing: acknowledge receipt of the complaint and state that the complaint will be followed up in line with Cordaids policies and procedures.

Step 2: Pre-assessment and registration of the complaint 48 hrs

This will be conducted by:

- Ethics Point and Integrity@Cordaid.org email account are monitored by both the Integrity and safeguarding Officer and Anti-Corruption and Anti-Fraud Officer
- Both Assess the nature of the complaints received and assign them accordingly as follows:

In case of interpersonal misconduct: The Integrity & safeguarding Officer, in consultation with the Anti-corruption and Anti-fraud officer and the CEO assesses the admissibility and severity of the complaint.

In case of financial misconduct: The Anti-corruption and Anti-fraud officer in consultation with the Integrity and safeguarding Officer and the CFO assesses the admissibility and severity of the complaint.

Sources of information: HR director GO, HR manager CO, Integrity Focal Point, Country director (if not implicated in the complaint)

Admissibility

- Is the complaint about the behaviour of a Cordaid representative or someone linked to Cordaid
- Is the complaint about an Integrity issue that falls under the authority of Cordaid's integrity system?
- Is there enough information to deal with the complaint?
- Is there already an inquiry or investigation taking place by another organisation/body?

Severity

- Does the complaint involve actual or potential harm to people, resources, or funds?
- Is the alleged Subject of Complaint a person in a position of power (director, manager)?
- Is there a possible abuse of a child or a beneficiary?
- Is the reputation of Cordaid at risk? Where the position or status of the organisation is at risk with Local Government, Stakeholders and Local Authority or in the Netherlands including possible media focus.

If the criteria for admissibility and severity are not sufficiently met, the Anti-Corruption and Anti-Fraud Officer or the Integrity and safeguarding Officer will either seek for additional information from the complainant, forward the complaint to those responsible (e.g. Police, Security Advisor or Integrity and Safeguarding Officer of partner organization, or line manager of the accused in cases of management concerns), or refer the issue back to the complainant with an explanation.

Registration

The Integrity and Safeguarding Officer or the Anti-Corruption and Anti-Fraud Officer supported by the Integrity Support Officer registers the case in Ethics Point, opens a case file including the Report Form.

Step 3: Identification of Decision Maker/Committee and Case Committee 48 hrs

Based on the pre-assessment of the case, a Decision Maker/Committee is assigned/formed. The Decision Maker/Committee subsequently appoints a Case Committee. The Case Committee consists of internal experts depending on the nature of the case.

- Non-high-sensitive cases and on country level (and the Country/Cluster Director is not involved): a case committee will be appointed by the **Country/Cluster Director** together with another staff member (Decision Maker/Committee) in consultation with the Anti-Corruption and Anti-Fraud Officer and/or the Integrity and safeguarding Officer.
- Global Office cases and/or high sensitive cases: Case Committee will be appointed by the BoD as the Decision Maker or committee in consultation with the Integrity and safeguarding Officer or the Anti-corruption and Fraud Officer. See Annex 6 Case Management Matrix.

Definitions:

Depending on the Nature of the Case a Decision Maker or Decision Committee of a Min of two persons could be recommended.

Decision Maker:

This is a person who in the end of the process has to decide upon the investigation report and follow-up actions including disciplinary actions/proceedings in consultation with other management staff.

Decision Committee:

This is a minimum of two persons who in the end of the process has to decide upon the investigation report and follow-up actions including disciplinary actions/proceedings in consultation with other management staff.

Exception only in non-sensitive cases on country level. The Decision Maker/Committee is who-in the end of the process has to decide upon the investigation report and follow-up actions including disciplinary actions/proceedings. The Decision Maker/Committee is accountable for the quality of the investigation and writes the ToR for the case committee as assignment. The Chair of the Decision Committee is the case owner.

Decision Maker/Committee Role

The role of the Decision Maker/Committee is to oversee any inquiries or investigations. The Decision Maker/Committee prepares the ToR of the investigation and gives the assignment to the Case Committee and is ultimately accountable for the quality of the investigation.

To preserve the independence and integrity of the inquiries, investigations, and disciplinary process (if any), a Decision Maker/Committee will be appointed from either the BoD, Supervisory Board (if the BoD is implicated or Conflicted), Cluster or Country Director, provided that he or she is:

- competent to perform the role of a Decision Maker.
- can be the line manager/supervisor of the alleged perpetrator, and
- considered as part of the managerial/leadership team in either global, regional or Country offices but cannot be in any way directly or indirectly – implicated in the allegation.

The Decision Maker/Committee should also not be appointed from persons who would be expected to be part of disciplinary proceedings (if any) e.g., Country Offices HR teams.

Case Management will often be taken up by the Integrity Focal Point or the Integrity and Safeguarding Officer or Anti-Corruption and Anti-Fraud Officer either of the following situations:

- a) The case involves sexual abuse or exploitation.
- b) The case involves minors (below 18 years of age),
- c) The alleged perpetrator is the Country/Cluster Director,
- d) Otherwise, exceptional case.

Other members of the Case Committee

- Other members of the Case Committee are appointed depending on the nature of the case: for instance: the integrity focal point, an (internal) expert like a business controller and the HR advisor GO or CO.
- To be involved for specific input or assignments: HR advisor (CO or GO) and/or legal advisor and/or Safety & security advisor and/or gender expert and/or IT specialist, communication expertise, donor expertise and quality management expertise.

The Case Committee consists of a minimum of two persons but can be more. All decisions in the case management are made by the Case Committee. The Case Committee gives regular updates on the case to the Decision Maker/Committee and if needed steering moments (depending on the size and severity of the case).

Step 4: Case Management *ongoing*

- **Risk assessment:** The Case Committee conducts a risk assessment (at various levels: safety of the survivor and anyone involved; legal, security, donor and media risks; risks for the project management and implementation) and the Decision Committee decides/implements measures to mitigate those risks.
- **Activities:** If required, the Case Committee conducts or facilitates a fact-finding preliminary investigation, as long as it does not jeopardise any future investigations. This could include a conversation with the complainant or desk research, without raising profile or informing the alleged perpetrator of the complaint. The Decision Maker/Committee assesses whether a full-fledged investigation is necessary and appropriate.
- **Investigation:** If an investigation is launched, the Decision Maker/Committee, in consultation with the Case Committee, drafts the ToR (see Annex 5 Investigation Terms of Reference Template) and the Investigation Plan, and appoints the investigation team, usually comprised of two investigators. This can be an internal investigation team or external agency. In case of internal investigation team they are part of the Case Committee.
- The lead investigator *must* be trained and experienced in conducting integrity investigations in the given domain (i.e., safeguarding, fraud), given the particular complexity and sensitivity of integrity issues.
- The Support investigator is assigned based on their skill set of knowledge to compliment the Lead Investigator.
- An investigation interview cannot be done by a single person.
- **Investigators' standard**
An investigation is a process requiring the highest personal integrity, respect for all involved and accountability. Investigators should demonstrate competence and must comply with the highest ethical standards.
- Investigators shall maintain objectivity, impartiality, and fairness throughout the investigation process. Investigators shall perform their duties independently. They shall also be free from improper influence and retaliation for carrying out their duties.
- **Reporting:** The Decision Maker/Committee is responsible for notifying relevant stakeholders, like local authorities or Project Leads who will then inform the donors. No identifying details will be shared (unless required by law, for instance in the case of child abuse).
- **Documentation:** The Investigators are as part of the Case Committee responsible for logging all key steps taken, including calls, emails, meetings, investigations, etc. The Decision Maker/Committee checks if the Case Registry is updated by the Case Committee.

Step 5: Investigation *1 month (ideally)*

- An internal administrative investigation does not replace criminal proceedings but is Cordaid's way of ensuring our Duty of Care. For safeguarding investigation guidelines, see also [CHS Guidelines for Investigations](#).
- The Investigation Team, as part of their contract, signs a Confidentiality Agreement [see Annex 4].
- The Investigation Team, in consultation with the Decision Maker/Committee, revises and adjusts the Investigation Plan if necessary. The Investigation Plan, at a minimum, includes the documentation and materials to be revised, a list of interviewees, and an investigation timeline to determine the substantiation of the allegation.

- Where necessary, and with the guidance of a risk assessment, the Subject of Complaint may be put on administrative leave for the time of the investigation, unless the risks of doing so (e.g., security risks) are higher than the risk of not putting the SoC on leave.
- The Decision Maker/Committee, the Country/Cluster Director/and, if applicable, a local contact person, are responsible for supporting the Investigation Team with regards to logistics, accommodation, access to documents and contact to interviewees.
- The Investigation team gathers evidence around the allegation(s) and produces an investigation report including a conclusion on the substantiation of the allegation(s), recommendations, and, if applicable, management observations. The report is shared with the Decision Maker/Committee and Case Committee.
- The substantiation of allegation(s) will be assessed on the basis of evidence that the allegation(s) can be reasonably believed to be upheld.

The roles and responsibilities of the Investigators are concluded at the end of the Investigation.

Step 6: Follow-up 1 week

- The Case Committee finalises the investigation report, with conclusions on the complaints which are made (substantiated, partly substantiated or not substantiated) and sends it to the Decision Maker/Committee.
- The Decision Maker/Committee studies the investigation report and asks for recommendations on disciplinary measures (if any) from HR director/HR manager in CO's and (if this is not the same person) the Line Manager/Supervisor of the Subject of Complaint's.
- The Decision Maker/Committee then decides on the investigation report including disciplinary measures in line with the HR policy and procedures. and other management decisions and is responsible for coordinating the agreed-upon follow-up measures, usually with a Follow-up plan including the implementation of organizational improvement measures.
- The Decision Maker/Committee as Line Manager/Supervisor and, if applicable, the local contact person, is responsible to inform the Subject of Complaint about the result of the investigation and the disciplinary action.
- The Line Manager/Supervisor or the Decision Maker/Committee with the support of HR director/HR manager in CO's are responsible for implementing disciplinary measures decided upon. If the allegation(s) were substantiated, a disciplinary hearing is organised, and the case is registered in the Subject of Complaint's personnel records. If the allegation(s) were not substantiated, no data should be stored on the Subject of Complaint's personnel records.
- If the allegation seems to amount to a crime in the country where the case happened, it wasn't reported earlier, and the person affected (if 18+) consents, the case file will by default be handed over to local authorities after asking advice from a local lawyer and the legal advisor of Cordaid.
- Where Cordaid has suffered a loss, full restitution will be sought of any benefit or advantage obtained and the recovery of costs will be sought from the individual or organisation responsible for the loss. If the individual or organisation cannot or will not compensate for the loss, Cordaid considers taking legal action to recover the loss.
- The Decision Maker/Committee and, if applicable, the local contact person, is responsible for ensuring appropriate follow-up communication with the person affected, e.g. information about the outcome of the investigation.
- The Integrity and safeguarding Officer and the Anti-Corruption and Anti-Fraud Officer together with the integrity support officer are responsible for archiving all case documents in a safe way, ensuring that only authorized staff can access the case files.
- Upon implementation of all follow-up measures, the Decision Maker/Committee, in consultation with the Case Committee, closes the case in the Case Registry and informs the person affected as well as the complainant (if different from the person affected). The level of information shared with the person affected or complainant will be appropriate with regards to the privacy rights of the Subject of Complaint as well as the right to justice of the person affected. A complainant who is not the person affected might only be informed that the complaint was followed up, and that appropriate measures have been taken, without providing further details.
- If a Subject of Complaint resigns during an investigation, this will be noted on their personnel records, and indicated when a potential future employer requests a professional reference.

Special cases:

Children: If a child is affected by the alleged misconduct, the persons involved in handling the case, in particular the Decision Maker/Committee and the Case Committee including the investigators, must be able to ensure that the response is done in a child-friendly way, and that appropriate support services are made available wherever necessary. The parents/caretakers, unless implicated in the alleged misconduct, must be informed in an appropriate way.

High Risk: (see also the criteria under step 2: severity of the case): If a case holds extraordinary risks to the persons involved including well-being, reputation, or other risks other than security, the CEO will call on the integrity crisis team consisting of different experts who will be freed up to support the crisis.

Implication/Conflict of Interest: If a person responsible for the response to a case is implicated in the case or has a Conflict of Interest, the tasks are taken up by a person/body in a higher position. For example, if a member of the Board of Directors is implicated, the case will be managed by the Supervisory Board.

Management Concerns: Issues that are brought forward as integrity complaints that are not clearly definable as per Cordaid's integrity policies, but still present potential integrity risks (for instance by creating an unsafe working environment), are defined as 'management concerns' and will be referred to the line manager of the Subject of Complaint for follow-up.

Particularities: This procedure explains the standard procedure. If a particular case requires a different approach because of safety or other needs or wishes of the person affected, or because of particular contextual or factors, the Integrity Officer or the Anti-corruption and Anti-fraud Officer will adjust the procedure as required and under due consideration and thorough documentation.

Partner: If a case involves a partner organisation, but Case Management is taken up by Cordaid, a representative of the partner organisation might take up certain functions in the response, including joining the Investigation Case Committee and the Integrity Committee in relation to the case. Ideally, the organizations should at the beginning of a partnership agree upon a Memorandum of Understanding about the division of responsibilities when integrity cases come up, including the funding of investigations.

Security: If an integrity case also constitutes a security incident or risk, the Security Advisor, the Integrity and Safeguarding Officer and the Anti-corruption and Anti-fraud Officer coordinate who is in the lead, with the other department involved if and when necessary. As a general rule, security takes precedence if acute security risks are present. Information will be shared between the departments on a need-to-know basis. If such a case is registered as security incident and the security response is finalized, the Security Advisor informs the Integrity and safeguarding Officer to enable assessing a potential additional integrity response.

6. DISCIPLINARY MEASURES

Disciplinary measures are regulated per Country/Cluster Office HR Manual and for Global Office the Legal Status Regulations (LSR). They range from mandatory training, verbal and written warnings in cases of less severe misconduct and management shortcomings, up to termination of contract in cases of severe misconduct.

Disciplinary measures are decided on a case-by-case basis following due consideration and documentation. As a guideline, 'Severe Misconduct' refers to cases of serious actual or potential harm to people, assets, resources, and funds, or misuse of power or authorities, including – but not limited to – child abuse, sexual abuse and exploitation, and repeated misconduct.

7. GRIEVANCE PROCEDURE

Should a complainant, Subject of Complaint, or someone otherwise involved in a case perceive that their case was not handled appropriately, i.e. that Due Process was not followed, a grievance can be made via the following channels:

1. Grievance Procedure laid out in the national HR Manual, if applicable,
2. Through the [Grievance Committee](#). The Grievance Committee follows the procedure laid out for Cordaid's *Dispute Resolution Commission*, as described Cordaid's [Legal Status Regulations](#). The committee consists of three members, including:
 - the chair, appointed by the other two members.
 - one member from the GO Works Council, and
 - one member being an external integrity advisor.
3. *Externally* through the Dutch *House of Whistle-blowers*, who can make an investigation into the manner in which an employer has treated the reporter of a suspected work-related integrity issue:
<https://www.huisvoorklokkeluiders.nl/onderzoek-naar-een-misstand/verzoek-tot-onderzoek>. Note that the House of Whistle-blowers only considers complaints about 'of social interest', thus, among others, where the law was broken, where there is danger to the safety of persons, or where there is a 'danger to the proper functioning of the organization as a result of improper acts or omissions'.
4. The ACT Alliance by sending an email to the secretariat via complaintsbox@actalliance.org

8. GLOSSARY

Allegation: Assumed misconduct.

Complainant: A person who makes a complaint/report about misconduct to the organization / authorities. This can be the person affected by the misconduct, or a witness / whistle-blower. The term is *not* to be understood in a negative way as in 'nit-picker'.

Complaint: Report of concern, suspicion, or allegation of (potential) misconduct.

Concern: Perception of potential misconduct.

Do No Harm: The Principle of ensuring careful consideration so that through our work, no (further) harm is done intentionally or unintentionally.

Duty of Care: As a legal obligation, Duty of Care is imposed on an individual or organization by law requiring that they adhere to a standard of reasonable care while performing acts (or omissions) that present a reasonably foreseeable risk of harm to others. This includes staff and those who come into contact with our programs.

Management Concerns: Issues that are brought forward as integrity complaints that are not clearly definable as per Cordaid's integrity policies, but still present potential integrity risks (for instance by creating an unsafe working environment).

Misconduct: Any behaviour that can be reasonably be understood as breaching the standards of behaviour set out in Cordaid's Integrity Framework, Code of Conduct and related policies.

Report: See 'Complaint'.

Person affected: A person affected by misconduct, e.g., someone who was (sexually) harassed.

SoC (Subject of Complaint): The person who commits the misconduct. When speaking about someone who is suspected to have committed a misconduct, refer to 'alleged perpetrator'.

Survivor/Victim: Both terms can be used to describe persons affected by interpersonal misconduct. While some – especially those who have reached a certain state of recovery – might identify as having ‘survived’ the distressing incident(s), others feel more ‘victimized’ by them. One option that doesn’t rely on knowing a person’s self-identification is to refer to ‘persons affected’ by misconduct.

Suspicion: Perception, concern or fear about potential misconduct.

ANNEX 1 REPORTING FORM

With this form, you can report observations or suspicions of misconduct of Cordaid representatives. Fill in as much of information as you have at this point – including date, time, location, incident, names - and send it to integrity@cordaid.org as soon as possible. Do not attempt to 'investigate' yourself. Your report will be treated with utmost confidentiality and in line with Cordaid's procedure for handling Integrity breaches.

In case of *acute* security risks, including sexual assault, follow the security reporting lines.
In case of otherwise urgent issues, contact the Integrity Officer immediately.

DATE OF REPORT	
COUNTRY AND PLACE OF INCIDENT	
COMPLAINANT (NAME, POSITION, COUNTRY)	
SUBJECT OF COMPLAINT (NAME, POSITION, COUNTRY OF THE ACCUSED)	
PERSON(S) AFFECTED (IF INTERPERSONAL MISCONDUCT)	
EXTERNAL PEOPLE INVOLVED?	
ESTIMATED LOSS (IN CASE OF FINANCIAL MISCONDUCT)	
DATE AND TIME OF THE INCIDENT(S)	

TYPE ² AND DESCRIPTION OF ALLEGATION	
WHO IS AWARE OF THIS ISSUE?	

² Financial; Sexual harassment, exploitation or abuse; Weapons; Drugs and Alcohol; Discrimination; Violence and Aggression; Destruction and Theft, Conflict of Interest, other interpersonal undesirable behaviour (including bullying, intimidation, harassment); Other

ANNEX 2 FLOWCHART



Suspicion, concern, or allegation of Misconduct
(Safeguarding, Fraud, Conflict of Interest, Anti-Terrorism and Anti-Money Laundering) of a Cordaid representative.



Report Misconduct via any of the following:

Report online via www.cordaid.org/en/reporting-integrity-concerns-and-security-incidents/.

Speaking to your or higher supervisor, the Integrity and safeguarding Officer or Anti-corruption and Anti-fraud Officer via integrity@cordaid.org,

Fill in the reporting form and send it to the Integrity and safeguarding Officer or Anti-corruption and Anti-fraud Officer via integrity@cordaid.org

Reaching out to the external Whistle-blower Service via +31 (0)88 1331 030, via email to advies@huisvoorklokkenluiders.nl, or directly online (Dutch).

Make use of ACT Alliance or Caritas Internationalis reporting mechanisms.



Referral to third party

Where a report doesn't fall under the mandate of Cordaid's integrity system, the issue will be referred to the appropriate stakeholder for follow up, or referred back to the complainant.

Pre-assessment & Registration

The report is pre-assessed and registered.

Support to those affected

Any necessary psychosocial, medical, legal or security-related services will be offered to those affected.



Fact-finding, preliminary, or full-scale investigation

An inquiry (Fact-finding, preliminary, or full-scale investigation) will be made by the Case Committee or external investigators to find out the facts about the suspicion, concern, or allegation of misconduct.



Follow-up

Decision-making on follow-up measures, including disciplinary and organisational improvement measures, if appropriate.

ANNEX 3 CASE MANAGEMENT RACI-TABLE

	Timeline	#	Task	Complainant (person affected or other)	Person affected (if different from complainant)	Recipient of report	Integrity & Safeguarding Officer	Anti-Corruption and Anti-fraud Officer (in fraud cases)	I) Decision Maker/ Committee	Case Committee incl. Investigation team (if internal)	Line Manager	HR & Authorised Personnel (if substantiated)	Global Security Advisor (where relevant)
<input type="checkbox"/>	asap	1	Identification & Reporting of concern.	R									
<input type="checkbox"/>	24 hrs	2	Receipt and acknowledgment of report, notification of Integrity Officer. Facilitation of first aid if required.			A	I	I					I/C
<input type="checkbox"/>	48 hrs	3	Pre-Assessment and registration of the complaint.				A+R	A+R					I/C
<input type="checkbox"/>	48 hrs	4	Identification of Decision Maker/ Committee .				R	R	A+R				I/C
<input type="checkbox"/>	ongoing	5	Case Management.		I/C		I/C	I/C	A	R			I/C
<input type="checkbox"/>	Ideally month	6	Investigation	I	I/C		I/C	I/C	A	R	I		I/C
<input type="checkbox"/>	1 week	7	Decision making disciplinary actions if any and Follow-up	I	I/C		I/C	I/C	A+R	C	R	C	I/C

R = Responsible A = Accountable C = Consulted I = Informed

The level of information shared will depend on the case, aiming for maximum transparency while ensuring due consideration of all risks and privacy rights involved. Identifying details, such as names, will only be shared on a strict need-to-know basis. For instance, HR and Authorized Personnel will only receive the necessary information to ensure that a staff members’ personnel file and misconduct history is up to date and reliable to ensure that future references are accurate. Other advisors, such as Security or Legal Advisor, might be consulted if the case requires it.

ANNEX 4 CONFIDENTIALITY AGREEMENT TEMPLATE

Confidentiality Agreement

I understand and agree that in my function as _____ in the case _____, I will have access to confidential information, including but not limited to sensitive personal information from Cordaid and/or partner staff. To ensure the protection of such information, and to preserve any confidentiality necessary, the Recipient agrees to protect all sensitive information from unauthorized access and not to disclose the confidential information obtained to anyone unless approved in writing by Cordaids senior management or required to do so by law.

WHEREFORE, I have read and understand this Agreement and voluntarily accept the duties and obligations set forth herein.

RECIPIENT OF CONFIDENTIAL INFORMATION		ON BEHALF OF CORDAID	
Name:		Name:	
Function:		Function:	
Signature:		Signature:	
Date:		Date:	

ANNEX 5 INVESTIGATION TERMS OF REFERENCE TEMPLATE

STRICTLY CONFIDENTIAL

Terms of Reference

Investigation into allegation of misconduct by [Cordaid/partner] representative in [location, country]

1. Introduction

Cordaid is committed to ensure that Cordaid is a safe and welcoming workplace for everybody, that we treat everyone who comes into contact with Cordaid with respect and dignity, and that we use all powers, authorities, assets, resources, and funds entrusted to us appropriately. Any type of harm or misuse of the resources intended to achieve our mission jeopardizes our efforts to contribute to a world where each person is free to flourish and can live in peace. Therefore, Cordaid is committed to appropriately follow up on any concerns or suspicions of misconduct by Cordaid or partner representatives.

2. Allegation[s]

This investigation seeks to follow up on the following allegation[s] of misconduct:

Location: Country, town, [Country Office/program site]

Dates and times: []

Subject[s] of Complaint: [name and role of the alleged perpetrator]

Description of the Allegation[s]:

- [in case of interpersonal violation:]

Type of misconduct: [sexualized, bullying, intimidation, etc.]

Person[s] affected by the misconduct: [names and details of those affected – e.g. role in Cordaid beneficiary, gender, age, etc.]

- [in case of fraud:] *Value of assets, funds or stock estimated to be involved:* []

3. Objective of the investigation:

The objective of the investigation is to establish the facts around the allegation[s] and to make recommendations as well as management observations to help Cordaid prevent the (actual or suspected) misconduct.

4. Cordaid's Integrity principles

The investigation will be guided by Cordaid's integrity principles:

- Shared commitment to integrity by all Cordaid representatives
- Survivor-centeredness
- Compassion for all involved
- Confidentiality
- Transparency
- Professionalism and *Do No Harm* approach
- Zero-tolerance for not acting and impunity

In addition to this, the investigations will be conducted in principles of impartiality, independence, timeliness, and will be evidence-based. Where possible and necessary, all parties involved will have the opportunity to provide relevant information.

5. Deliverables

- 1.1 Finalised Investigation Plan including Risk Assessment, investigation methodology, timeline, to be approved by Decision Maker/Committee

- 1.2 Investigation Report including findings about the allegation[s], recommendations as well as management observations to help Cordaid prevent the (actual or suspected) misconduct in the future.

6. Roles and Responsibilities

ROLE	NAME AND CONTACT	RESPONSIBILITIES
<i>Lead Investigator</i> [must be trained and experienced in conducting integrity investigations in the given domain, i.e. safeguarding, fraud]	[name, agency/role in Cordaid/partner, contact details]	Lead the investigation in line with best practice Ensure quality of deliverables as well as adherence to Terms of Reference and Cordaid's Integrity policies and procedures Comply with Confidentiality Agreement
<i>Co-investigator[s]</i>	[name, agency/role in Cordaid/partner, contact details]	Support the lead investigator. Comply with Confidentiality Agreement
<i>Decision Maker/Committee</i>	[name, role, and contact details]	Appoints investigation team Enables the investigation by coordinating logistical, security, and other support (e.g. translators) Approves Investigation Plan Receives and approves Investigation Report
<i>Decision Committee Chair</i>	[name, role and contact details]	Receives appropriate information about the investigation and its findings Ensures management follow-up
<i>Other relevant contacts</i> [security advisor, contact person in-country, support for logistics, accommodation, access to documents and contact to interviewees, etc.]	[names, roles and contact details]	

7. Timeline

The investigation is to be launched within [usually max. 1 week] of the approved Terms of Reference, in line with the timeline established in the Investigation Plan. The investigation report is to be submitted within [10 days] of conclusion of fact-finding.

8. Budget

The investigation services will be remunerated with [full amount OR day rate] [incl./excl.] VAT. In case travel is required, [add regulations for travel, accommodation, insurance and security costs]. The full amount is to be paid within [30 days] of approval of the investigation report.

Signature Cordaid: [name, date & signature Case Manager]

Signature Lead Investigator: [name, date & signature Lead Investigator]

Annex: signed Confidentiality Agreement[s], Cordaid/Integrity Framework

SITUATION	LEVEL	DECISION MAKER/ COMMITTEE	CASE COMMITTEE	INVESTIGATORS -ALWAYS 2 PERSONS (4 EYES PRINCIPLE)
1. Complaint involves local partner performance or partner staff behaviour?				Can be external; in case of internal:
In case of finance violation	Programme/Country level	Programme manager + CD	AfACO, IFP, Include local finance manager + programme manager+ CD and maybe others in case necessary	IFP + AfACO for instance or local finance manager AfACO or ISO in leading or more support role depending on the situation
In case of interpersonal violation	Programme/ Country level In case of child abuse or other reputational risks will be CEO informed	Programme manager + CD	ISO, IFP, Include local safeguarding officer if any + programme manager+ CD and maybe others in case necessary	IFP + ISO support or programme manager
2. Complaint involves local staff or Expat staff <u>NOT</u> being the CD				
Financial violation				
Minor violation	Country level GO Finance manager will be informed	CD together with Local Finance manager	AfACO, IFP, Include local finance manager + CD and maybe others in case necessary	AfACO with IFP and/ or local finance manager with support finance GO (in case necessary)
Major violation	SEVERE-> Global level CFO will be informed.	BoD, CD together with Finance manager/Corporate controller GO	AfACO, IFP, Include local finance manager + CD and Finance manager or Corporate Controller GO	AfACO, IFP, local finance manager with support Finance GO
Interpersonal or safeguarding violation				
Minor violation	Not severe - Country level	CD together with local manager of the staff member	ISO, IFP, perhaps local HR officer, CD, local manager if any	ISO + IFP

SITUATION	LEVEL	DECISION MAKER/ COMMITTEE	CASE COMMITTEE	INVESTIGATORS -ALWAYS 2 PERSONS (4 EYES PRINCIPLE)
Medium violation	Medium - Country level, CEO will be informed	CD, local manager (if any)	ISO, IFP, CD, BoD on information basis	ISO+ IFP
Major violation severe: possible abuse of a child or a beneficiary?	SEVERE - depends, can be Country level but also Global level for decision making	BoD with CEO	ISO, IFP, CD, BoD and a content specialist.	ISO with internal or external content specialist.
3. Complaint involves behaviour of the CD, GO manager	SEVERE-> BOD level (both financial and interpersonal/safeguarding)	BoD if the is no Conflict of Interest or member implicated. Supervisory Board if BoD is implicated or a Conflict of interest.	BoD + ISO/AFACO + Supervisory Board.	For: CD: Global level by ISO/AFACO +second investigator (depending on the nature of the case). Or external investigator for GO: External investigators;
4. Complaint involves behaviour of staff member GO or BoD Member				
Financial violation				
Minor violation	GO level-> CFO will be informed	GO manager together with Finance manager or BoD	AFACO, IFP, GO manager, Include GO finance manager + and maybe others in case necessary	AFACO, IFP, finance manager
Major violation	SEVERE -> Global level CFO will be informed. Supervisory Board will be informed in BoD is Compromised	BoD if the is no Conflict of Interest or member implicated. Supervisory Board if BoD is implicated or a Conflict of interest.	AFACO, IFP, GO manager and GO finance manager or Corporate Controller GO	AFACO, IFP ,finance manager /corporate controller or external Investigators.

SITUATION	LEVEL	DECISION MAKER/ COMMITTEE	CASE COMMITTEE	INVESTIGATORS -ALWAYS 2 PERSONS (4 EYES PRINCIPLE)
Interpersonal or safeguarding violation				
Minor violation	Not severe- Global level	CD together with local manager of the staff member	ISO, IFP perhaps HR officer, GO Manager	ISO + IFP
Medium violation	Medium- Global level, CEO will be informed	GO manager together with CEO	ISO, IFP, GO Manager, CEO on information basis	ISO+ IFP
Server Violation: possible abuse of a child or a beneficiary?	SEVERE -> Global level Supervisory Board will be informed in BoD is Compromised	GO Manager together with BoD BoD if the is no Conflict of Interest or member implicated. Supervisory Board if BoD is implicated or a Conflict of interest.	ISO, IFP, GO Manager, CEO	ISO with external or internal specialised gender specialist
5. Complaint involves behaviour BOD member?	SEVERE-> Supervisory Board level	Supervisory Board	2 Members SB, ISO/AFACO	External investigators

ABOUT CORDAID

Cordaid works to end poverty and exclusion. We do this in the world's most fragile and conflict-affected areas as well as in the Netherlands. We engage communities to rebuild trust and resilience and increase people's self-reliance.

Our professionals provide humanitarian assistance and create opportunities to improve security, healthcare, education and agrifood systems. We are supported by 250,000 private donors in the Netherlands and by a worldwide partner network. Cordaid is a founding member of Caritas Internationalis, CIDSE, and ACT Alliance.

CONTACT

Integrity & Safeguarding Office
Email: Integrity@cordaid.org

Postal address
PO Box 16640
2500 BK The Hague
The Netherlands

Address
Grote Marktstraat 45
2511 BH The Hague

+31(0)70-31 36 300
info@cordaid.org
www.cordaid.org

**CARE.
ACT.
SHARE.
LIKE CORDAID.**
