6.1. HOPE'87 ANTI FRAUD AND CORRUPTION, ANTI MONEY LAUNDERING, COUNTER TERRORISM FINANCING POLICY PAPER
Facts, Awareness, Consequence

(courtesy of and based on the Compliance Toolkit, Protecting Charities from Harm, The Charity Commission UK, Financial Action Task Force FATF)

Revised on 1.12.2023.

Its governs the ethical behaviour of all HOPE'87 staff members as well as local, national and international partners. All BOM are required to bring it to the attention of all staff member as well as local, national and international partners in the field. Non-compliance with this policy paper will result in termination of contract. HOPE'87 and its BO will fully cooperate with the law and order authorities of the respective country to wipe out fraud and corruption.

HOPE'87 commitment is "Zero Tolerance with Fraud and Corruption"

I. INTRODUCTION

Fraud and corruption can take many forms. Fraud is normally characterised by some form of deliberate deception to facilitate or conceal the misappropriation of assets, whereas corruption involves a breach of trust in the performance of official duties and may be considered as official misconduct.

Fraud is a form of dishonesty, involving either false representation, failing to disclose information or abuse of position, undertaken in order to make a gain or cause loss to another.

Corruption is operationally defined (courtesy of Transparency International, TI) as the abuse of entrusted power for private gain. TI further differentiates between "according to rule" corruption and "against the rule" corruption. Facilitation payments, where a bribe is paid to receive preferential treatment for something that the bribe receiver is required to do by law, constitute the former. The latter, on the other hand, is a bribe paid to obtain services the bribe receiver is prohibited from providing.

Theft is dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

Fraud and corruption are criminal offences and have a technical definition set out in the relevant legislation. In practice there is a wide variety of types of fraud that HOPE'87 can experience including fraud connected with fundraising, income and expenditure, property and investments, HOPE'87's identity, banking fraud and others.

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

For HOPE'87, the impact of fraud and corruption can include significant loss of funds, permanent financial or harm of reputation and damage to public confidence. Staff members, partner organisations and business partners of HOPE'87 found guilty of attempting or carrying out fraud and/or corruption will be disqualified from working with HOPE'87 and HOPE'87 will fully cooperate with the law enforcement agencies of the country.

There are many different types of fraud and the methods used are constantly evolving. There are 5 major forms of fraud:

- Fraud by false representation
- Fraud by failing to disclose information
- Fraud by abuse of position
- Fraud by obtaining services dishonestly with intent to avoid payment
- Fraud by possessing, making and supplying articles for use in frauds
- Fraud by participating in a fraudulent business carried on by a sole trader

False or fraudulent accounting refers to a person that dishonestly, with a view to gain for himself or another or with intent to cause loss to another:

(a) destroys, defaces, conceals or falsifies any account or any record or document made or required for any accounting purpose; or
(b) in furnishing information for any purpose produces or makes use of any account, or any such record or document as aforesaid, which to his knowledge is or may be misleading, false or deceptive in a material particular.

A person who is convicted of an offence involving dishonesty or deception is automatically disqualified from holding any position within HOPE'87 and any contract linking HOPE'87 to that person will be declared null and void.

II. TYPES OF FRAUD

Beware of the following types of fraud:

1. Income-related fraud

This occurs when people within or connected to HOPE'87 attempt to divert funds for personal use. Examples of income-related fraud include:

- Redirected resources from charity shops or trading activities
- Intercepted postal donations and cheques being paid into personal accounts fraud by participating in a fraudulent business carried on by a sole trader
- Skimming money from HOPE'87 fundraising collections
- Impersonating HOPE'87 and redirecting the income collected to a fraudulent or bogus body
- Fraudulent Gift Aid claims
- False accounting claiming inappropriate expenses

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

2. Expenditure related fraud

This occurs when people within HOPE'87 attempt to divert funds foreseen for expenditures, especially procurement, for private use.

Examples of expenditure-related fraud include:

- Claiming non-existent, over-inflated or inappropriate expenses or overtime
- Withdrawing cash directly from HOPE'87's bank account for personal use using cheques which have been obtained without authorisation, or by issuing false direct debit/standing order instructions for personal gain
- Misusing HOPE'87's credit and debit cards or internet banking for personal expenditure
- Creating false invoices, purchase orders and supplier identities in order to obtain payment from the charity for goods and services that have not been supplied
- Submitting, or conspiring to submit, false applications from real or fictional individuals for grants or other benefit
- Awarding a contract, or preferential terms, to a supplier in return for payments, personal discounts, commission or other benefits
- Using receipts and records for a completed project to support a further application for funding from another grant-maker
- Creating non-existent beneficiaries or employees for directing payments, or use of a beneficiary identity for personal benefit

3. Property and Investment fraud

This occurs when people within HOPE'87 attempt to use equipment belonging to HOPE'87 for private use:

- Fraudulent use of HOPE'87 property - for example personal use of HOPE'87 vehicles, hiring them out, siphoning off fuel, claiming for overpriced or unnecessary repairs.
- Stealing HOPE'87 letterheads and personal details of trustees, staff or beneficiaries may be part of an identity theft fraud.
- Using the HOPE'87 databases or inventories for personal profit or unauthorised private or commercial use. The theft of donor details or other personal information, for example, might have implications under the Data Protection Act.
- Theft of furniture, computers, plant and other equipment.
- Making grant applications on behalf of HOPE'87 with the intention to intercept the funds for personal use.
- Transferring without authorisation HOPE'87 funds to an organisation with which a trustee or employee is connected.

4. Procurement fraud

Procurement fraud is a generic term describing fraud relating to the purchase of goods and/or the commissioning of services, as opposed to the simple theft of cash. Procurement fraud usually involves collusion between one or more members of the organisations staff and one or more outside suppliers.

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

5. Fraudulent fundraising in the name of HOPE'87

This usually involves misrepresenting to the public or other donors the destination of funds, or the amount going to a named charity:

- Fundraising events and/or competitions which claim to be for HOPE'87 purposes but from which HOPE'87 in fact receives no proceeds.
- Cash collections either in public places or from house to house, which have not be authorised by HOPE'87 and/or the relevant local authority.
- Fundraisers raking off funds and handing over only a proportion of what has been collected.
- Professional fundraisers not being truthful to donors how much of the funds being donated will be used to pay their charges.
- Creating spurious email appeals or false websites, claiming that money donated through them will be given to HOPE'87 which
- may or may not be genuine.

6. Fraudulent invoicing and grant applications

This usually involves providing false information to HOPE'87 about the beneficiaries or the aim of a project or an application for funding.

- Making false or inflated applications to HOPE'87 to win service contracts or misapplying grant funding in breach of trust and contract.
- Making grant applications to HOPE'87 in respect of bogus or non- existent applicants.
- Setting up a false charity to obtain grant funding but with no genuine intention to provide services to beneficiaries.

7. Identity fraud/theft

False identities may be created in order to justify fraudulent payments. Corporate Identity Fraud occurs when a bogus company is set up, or a genuine company's details are used without authorisation, to facilitate unlawful activity.

- Falsifying, creating/fraudulently using trustee or employee details
- Provision of funds or services to non-existent beneficiaries.
- Using the HOPE'87 name or logo in correspondence or on materials for the purpose of deception and fraudulent gain

8. Banking fraud

HOPE'87 HQ and BO, who have online banking arrangements, need to have adequate internet firewall protection. One of the main risks involves fraudulently setting up direct debits and standing orders to transfer funds to the fraudster's own bank account.

9. e-Crime

This involves using HOPE'87 to validate stolen or cloned credit cards as well as Phishing fraud. Fraudsters may use stolen or cloned credit cards to make small online donations

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

through a BO website. Their purpose in doing this is to check whether a stolen card has been blocked or cancelled. If the 'test' donation works the card will be used for more widespread fraud. 'Phishing' is a type of e-crime that involves fraudsters sending emails to many, sometimes thousands, of recipients asking them to disclose sensitive or confidential information. The fraudsters are usually based overseas and may be almost impossible to trace. Typically, the phishing email is made to look like a genuine email from a bank, and it may ask the recipient to confirm information such as account usernames or passwords because, it claims, there has been a security problem with the bank's computer system. In many cases the phishing email will contain a link to another website into which the recipient is asked to enter the confidential information.

10. 419' frauds

These frauds take their name from the section of the Criminal Code of Nigeria, where they are thought to have originated. They can also be known as advance-fee frauds.

HOPE'87 or staff members are contacted by letter or email with an invitation to assist the sender in recovering a large amount of money, usually, but not exclusively, from a bank account originating in Africa. The recipient is promised a large share of the money recovered. There is no money, of course; the aim of the scam is simply to obtain the HOPE'87 bank account details or letterheads that can be used for fraudulent activities, or to obtain money under the pretence that it is needed to assist in the process of recovery.

A variation on the scam is a message informing the recipient that he or she has been identified as having an entitlement to a large sum of money, but will have to pay handling or administration costs before the money can be remitted - this is the 'advance fee'. Not only does this invariably result in the loss of any money sent, but the fraudster is able to obtain bank account information through the cheque or bank transfer.

11. Money Laundering

"Money laundering" is the act by which the proceeds of crime are made to appear legitimate. The UN Convention Against Transnational Organized Crime defines money laundering at Article 6 as:

The conversion or transfer of property, knowing that such property is the proceeds of crime, for the purpose of concealing or disguising the illicit origin of the property or of helping any person who is involved in the commission of the predicate offence to evade the legal consequences of his or her action; or the concealment or disguise of the true nature, source, location, disposition, movement or ownership of or rights with respect to property, knowing that such property is the proceeds of crime.

The act of conversion and concealment amounts to the "laundering" of criminal proceeds but those funds only ever have the "appearance" of legitimacy, not the reality, even though the so-called money trail may be complicated and obscure the original criminal source of the funds.

12. Terror Financing

"Terrorist financing" is defined in the UN Convention for the Suppression of the Financing of Terrorism at Article 2 as follows:

Any person commits an offence within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and wilfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out: (a) An act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex; or (b) Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act.

FATF recommendation 6 expands the scope of the offence:

Terrorist financing offences should extend to any person who wilfully provides or collects funds by any means, directly or indirectly, with the unlawful intention that they should be used, or in the knowledge that they are to be used, in full or in part: (a) to carry out a terrorist act(s); or (b) by a terrorist organisation or by an individual terrorist (even in the absence of a link to a specific terrorist act or acts).

III. SIGNS OF FRAUD

Questions to be asked

Regarding Accounting and transactions

- Are there unusual discrepancies in accounting records and unexplained items on reconciliations?
- Are many financial documents - such as invoices, credit notes, delivery notes, orders etc - photocopies rather than originals? This might indicate counterfeit documents created to support bogus account entries
- Do alterations or deletions frequently appear on documents? Again, this might be evidence that documents have been falsified to support bogus account entries
- Have any documents or account books gone missing?
- Are there high numbers of cancelled cheques?
- Are common names unexpectedly appearing as payees?
- Are there any duplicated payments or cheques?
- Do transactions take place at unusual times with irregular frequency, unusual or 'round' amounts, or to unknown recipients?
- Are suppliers regularly submitting invoices electronically and are these in non-PDF format that can be altered?
- Are there any unexplained variances from agreed budgets or forecasts? Have audits highlighted any inconsistencies or irregularities?
- Are unrestricted reserves being spent without proper prior authorisation?
- Have restricted funds been used for general purposes?

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

- Is there an asset register or inventory, and does it match up with equipment physically on hand?
- Are payments made to individuals or companies with family or business connections to a trustee, and perhaps authorised by that trustee? This might indicate collusion
- Is there any indication that income is being under-reported or expenditure being over-reported?
- Is there any misdescription of purchase and expense items in the accounting system?
- Can cash withdrawals be supported by documents and a full audit trail from approval to expenditure?
- Have any blank cheques been pre-signed?

Regarding changes in behaviour of trustees or staff who handle the accounts

- Are vague responses being given to reasonable and legitimate queries and/or are those queries being left unexplained, or taking a long time to resolve?
- Is there any reluctance by a volunteer, member of staff or trustee involved in handling finances to accept assistance? Does a single member of staff or trustee have control of a financial process from start to finish with no segregation of duties?
- Is any member of finance staff working unsociable hours or working from home without reason? Are there any noticeable changes in behaviour or work patterns, such as a reluctance to take holidays or over-protectiveness of work?
- Has the format of financial information presented to the trustee board or senior managers suddenly changed or become more complicated or difficult to understand?
- Are there inconsistent, vague or implausible responses to questions about the accounts or accounting records?
- Do trustees and members of finance staff always comply with financial policies and procedures?

None of the above warning signs are necessarily indicative of financial abuse on their own, but if one of them is happening frequently or several in combination, further scrutiny may be warranted.

Whistleblowing Guideline

Staff members are called upon to report any of the above warning signs to their respective supervisors. In case the staff member believes in an involvement of his/her supervisor, he/she has the right to inform the Country Representative or the Secretary General of HOPE'87. A staff member of the HOPE'87 General Secretariat has the right to inform the Secretary General or in the case the Secretary General could be involved in such a misbehaviour, the Secretary of the Board.

Informing the HOPE'87 superiors about such warning signs prohibit staff members from being discharged or otherwise discriminated against.

HOPE'87 superiors have the responsibility to guard- as much as possible- the anonymity of the whistleblower, to inform the HOPE'87 HQ immediately, to conduct an investigation, report the results of such an investigation to the HOPE'87 HQ and propose to the HOPE'87 HQ- if need be- sanctions according to the Personnel Code of HOPE'87. The final decision will be take by the HOPE'87 HQ.

HOPE'87 – Generalsekretariat Webpage: www.hope87.at Email: office@hope87.at
ZVR: 482616437

HOPE'87 Country Representatives are required to continuously advise and train staff members regarding fraud and corruption along the HOPE'87 policy. They need to keep themselves up to date with international, regional and country specific legal frameworks, laws and policies regarding Anti Money Laundering (AML) and Counter Terrorism Financing (CTF) as well keep abreast with the FATF recommendation, such as best practices[1].

Prevent – Identify, inform and disrupt - Act promptly and properly!

[1] COMBATING THE TERRORIST FINANCING ABUSE OF NON-PROFIT ORGANISATIONS – FATF November 2023

6.2. HOPE'87 TRAINING GUIDELINES FRAUD & BRIBERY
Fight against fraud and corruption, money laundering and terrorist financing [1]

When:
1. ½ day session on each mission of HQ staff
2. 1 day session led by CR in each CR office annually
3. ½ day session at HQ annually

Participants:
All staff member of the CR office
All staff members of HQ

1. START

- Explain the reason for the session (avoid feelings of panic and/or fear, be objective, clear, friendly, but firm) and repeat the HOPE'87 principle of "Zero tolerance for fraud and corruption, money laundering and terrorist financing"
- Invite participants to explain the terms: bribery, fraud, facilitation payments, payments under duress, gift, hospitality, money laundering and terrorist financing … check if the HOPE'87 manuals have been read and understood. Avoid "know-it-all" attitudes, but rather elaborate together with participants what the terms mean…

2. CONSCIOUS BUILDING

- Discuss the evil effects of fraud and bribery, money laundering and terrorist financing on the national economy and its losses, on the society, on the individual…
- Ask participants to talk about cases of fraud and bribery in their direct environment and how they felt about it
- Ask participants if they know of the consequences for their work with HOPE'87, but also for legal consequences if they are caught with fraud and bribery, money laundering and terrorist financing … let them tell you…. And tell them… Try to focus on a "common understanding"…
- raise attentiveness for possible fraud and bribery, money laundering and terrorist financing:
  - in procurement situation
  - in business with third parties, suppliers and contractors
  - in dealing with partner organisations or agencies
  - in dealing with governmental official and political parties
  - while hiring new staff or supervising or evaluating staff (for payment increments or promotion or transfer or leave or termination of contract…)

[1] This document was elaborated with the help of "Anti Bribery Principles and Guidance for NGOs June 2011" by BOND for International Development

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

3. DETECTION

- Elaborate with the participants how and where potential risks might be detected:

Abnormal cash payments
Pressure exerted for payments to be made urgently or ahead of schedule
Payments being made through 3rd party country (eg. goods or services supplied to country 'A' but payment is being made, usually to shell company in country 'B')
Abnormally high commission percentage being paid to a particular agency. This may be split into two accounts for the same agent, often in different jurisdictions
Private meetings with public contractors or companies hoping to tender for contracts
Lavish gifts being received
Individual never takes time off even if ill, or holidays, or insists on dealing with specific contractors him/herself
Making unexpected or illogical decisions accepting projects or contracts
Unusually smooth process of cases where individual does not have the expected level of knowledge or expertise
Abusing decision process or delegated powers in specific cases
Agreeing contracts not favourable to the organisation either with terms or time period
Unexplained preference for certain contractors during tendering period
Avoidance of independent checks on tendering or contracting processes
Raising barriers around specific roles or departments which are key in the tendering/contracting process
Bypassing normal tendering/contractors procedure
Invoices being agreed in excess of contract without reasonable cause Missing documents or records regarding meetings or decisions Company procedures or guidelines not being followed
The payment of, or making funds available for, high value expenses or school fees etc on behalf of others.

- Guide participants how to react if they feel that
  a.) they have been subject to fraud and bribery, money laundering and terrorist financing
  b.) another staff member has been subject to fraud and bribery, money laundering and terrorist financing
  c.) a supervisor/director/CR has been subject to fraud and bribery, money laundering and terrorist financing
  d.) they have accepted a bribe or committed a fraud

(link your answers to the HOPE'87 Basic Documents available at all CR offices and available for all staff members, but also to other relevant tools such as "Resisting Extortion and Solicitation in International Transactions" [2] also available in all HOPE'87 CR offices.

[2] "Resisting Extortion and Solicitation in International Transactions", Copyright © 2011 International Chamber of Commerce, Transparency International, United Nations Global Compact, World Economic Forum)

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

4. DEALING WITH FRAUD AND BRIBERY, MONEY LAUNDERING AND TERRORIST FINANCING

- Talk with participants about the steps to be taken by staff members and by HOPE'87 in connection with fraud and/or bribery and/or money laundering and/or terrorist financing: Rejection of any attempt of fraud and/or bribe, Investigation into any allegation of fraud and/or bribe, internal consequences for the staff member and external reporting to the law enforcement agency.
- Explain the whistle blowing policy of HOPE'87, reassuring secrecy for the person reporting a possible case of fraud and/or bribery, money laundering and/or terrorist financing, reassuring a swift and thorough dealing of the CR or of HQ with the case, but also reassuring all participants of transparency and fairness.

5. ENDING THE SESSION…

- Summarise the most important points for the participants "to take home"
- Make the participants feel comfortable with the HOPE'87 policy, especially that it is not anything "strange" or "foreign" or "not apt for the country"… call upon the solidarity of the team to work for the benefit of the target groups of the HOPE'87 projects.
- Let all participants sign the attendance list and thank them for their commitment and support.

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

APPENDIX C – Glossary

Bribery - the offering, promising, giving, accepting or soliciting of money, gifts or other advantage as an inducement to do something that is illegal or a breach of trust in the course of carrying out an organisation's activities.
Corruption – the abuse of entrusted power for private gain.
Extortion - the unlawful use of one's position or office to obtain money through coercion or threats. One example would be when customs officials request undue 'customs duties' from importers as a condition to clear their goods.
Facilitation payments - These are bribes and are usually small unofficial payments made to secure or expedite the performance of a routine or necessary action to which the payer of the facilitation payment has legal or other entitlement.
Gifts and hospitality – these can range from small gifts (such as diaries) to expensive hospitality (tickets for major events, holidays etc). Extravagant gifts and hospitality may be used to disguise bribes that are intended to induce improper behaviour.
Solicitation – the act of a person asking, ordering or enticing someone else to commit bribery or another crime.
Whistleblowing – the sounding of an alarm by an employee, director or external person to express concerns about or to attempt to reveal neglect or abuses within the activities of a company.
Money laundering - the act of concealing the transformation of profits from illegal activities and corruption into ostensibly "legitimate" assets.
Terrorism financing - refers to activities that provide financing or financial support to individual terrorist or terrorist groups.

HOPE'87 – General Secretariat Webpage: www.hope87.at Email: office@hope87.at
Wassergasse 29/3, 1030 Vienna, Austria
Tel: (43-1) 982 71 15 Fax: (43-1) 982 71 15 17

6.3. HOPE'87 Fraud and corruption, money laundering and terrorist financing Investigation Policy

This Policy covers the action required when fraud or corruption, money laundering or terrorist financing is suspected and to whom the criminal act or suspicion should be reported.

1. Introduction

1.1. It is important that managers and others know what to do in the event of a fraud or corruption, money laundering or terrorist financing so that they can act without delay. This Policy covers the action required when fraud or corruption, money laundering or terrorist financing is suspected and to whom the act or suspicion should be reported. The Fraud Investigation Policy is a guide to how and by whom the suspicion will then be investigated, reported and closed.
The Fraud Investigation Policy provides an outline of many of the areas that will need to be considered when investigating a large and complex fraud or corruption, money laundering or terrorist financing. For smaller less complex frauds, there will be parts of the plan that will not be applicable. It is however important to keep an open mind and consider whether a small fraud is concealing a much larger fraud.

1.2. This policy covers fraud or corruption, money laundering or terrorist financing investigation. Regarding easy readability the terms fraud, corruption, money laundering and terrorist financing will henceworth be summarized- if so appropriate- by the term "fraud".

1.3. There are numerous facets to the management of a suspected case of fraud, which may involve desk officers from different departments, including audit, finance, human resources as well as police. All specific legislative requirements must be adhered to. It is vitally important therefore that the investigation policy is followed by all concerned in order to ensure that the situation is handled professionally and to safeguard against the case being compromised.

1.4. Once fraud or corruption is suspected, there are four immediate issues to be addressed:
- the proper internal investigation of the matter;
- what action, if any, should be taken in relation to any staff member concerned;
- the facilitation and management of the investigation; and
- subsequently whether to involve the police and if so at what stage.

1.5. It is important that all suspected fraud or irregularity is brought promptly to the attention of the Country Representative (CR) who will consult the CFO or SG.

2. Overview of Response

2.1. The HOPE'87 Basic Documents and Financial Regulations in conjunction with the HOPE'87 Anti Fraud and Anti Corruption Policy require that awareness or suspicion of fraud, and irregularity, improper use or misappropriation of property or resources be reported promptly to the CR.

2.2. The CR will determine, after consultation with appropriate staff members, what action should be taken. This could be the resolution of the issue within the department of the Country Office (CO), or a full investigation.

2.3. If the CR determines that an investigation should be carried out, an investigation team will be identified. Depending on the nature and scale of the issue this team, led by the CR,

may comprise;
Director of Finance, Director Operations, senior staff members or
any other combination deemed appropriate by the CR if necessary.

2.4. The GS (General Secretary) or CFO (Chief Financial Officer) will be notified that an investigation is taking place.

2.5. Where the allegation involves a member of staff a member of the staff representation body has to be kept informed about all matters.

2.6. The investigation team will be responsible for the proper investigation of the matter, with reference to all relevant legislation and disciplinary procedures of HOPE'87.

3. Initial Actions to be taken when a Fraud is suspected

3.1. Anyone suspecting that a fraud is or has taken place should raise their concern formally. This should normally be with their supervisors. If the suspect is the supervisor, the person raising the concern should discuss it with the CR, or in case the CR is the suspect with the CFO or GS.

3.2. Staff members with concerns should avoid discussing their suspicions with anyone other than the officer with whom they formally raised the issue. Under no circumstance should any staff member attempt to investigate any matter on their own without first consulting one of the above named officers.

3.3. Staff members raising concerns in good faith are protected by the provisions made in the HOPE'87 Whistleblowing Policy.

3.4. Officers with whom issues are raised should ensure that the matter is reported confidentially to the CR.

3.5. Care should be taken, by any officer who suspects fraud and any officer to whom this suspicion is reported, to retain any evidence and make immediate note of the issues and concerns.

3.6. All records relating to the issue under investigation should be secured as soon as suspicions arise to ensure they are not destroyed or amended. In some circumstances this may be straightforward and can be done immediately by the supervisor.
However, securing records may, in some circumstances, alert a perpetrator to the possibility of an investigation, risking the destruction or alteration of records. Unless there is an immediate danger to the integrity of records the CR should be contacted for urgent advice prior to taking any actions to secure records.

3.7. At this stage, suspects should not be subject to investigation or interview (including private contractors): this will be done as necessary by the staff appointed to do so. The requirements of the Police and law and order agencies and their associated codes will apply to any such interviews, so it is vital that any staff conducting interviews is aware of these requirements to avoid jeopardising the investigation.

3.8. Any decision to suspend a staff member on the grounds of suspected fraud will be taken by the CR or the GS.

3.9. Where, in accordance with the appropriate disciplinary procedure a staff member is to be suspended pending investigation, arrangements should be made by the suspending officer to secure any mobile phones, laptop computers, passes, keys etc to ensure access is denied to HQ or CO systems and offices.

4. Fraud management process

4.1. The process will be co-ordinated by the investigation team and the team leader will liaise with the legal representatives of HOPE'87 as appropriate.

4.2. The investigation team will manage:
- issues concerning staff members or independent contractors
- the actual investigation
- any necessary external liaison with the police, law enforcement agencies or other relevant authorities

5. Surveillance

5.1. Surveillance should only be carried out if authorised by valid law.

6. Issues concerning staff members or independent consultants and contractors

6.1. Throughout the investigation, the member of the staff representation body and the legal representatives of HOPE'87 will provide advice to all parties, on any issue concerning staff.

6.2. The HOPE'87 Personnel Manual as well as the HOPE'87 Anti Fraud and Anti Corruption Policy are very clear regarding the standards of behaviour expected of staff members.

6.3. Examples of behaviour that could lead to disciplinary action and summary dismissal- if so proven-include:

- stealing from the CO/HQ, its members, staff or the public
- any fraudulent act, including falsification of any document, for monetary or other advantages
- soliciting or accepting gifts or gratuities not in accordance with the HOPE'87 Anti Fraud and Anti Corruption Policy
- attempted use of official positions for private advantages;
- dishonest or improper use of information obtained in the employment of HOPE'87
- involvement in criminal activities such as fraud or corruption, money laundering or terrorist financing

6.4. It is possible that staff under investigation will be suspended immediately. Any suspensions, however, must be carried out by the CR and the GS as well as the staff representation body has to be informed immediately.

6.5. The nominated member of the staff representation body will advise on issues such as:

- liaison with Trade Unions
- management of staff, suspended under suspicion, but who is subsequently reinstated

disciplinary proceedings

- provision of references to prospective employers for staff who have been investigated;

7. Management of the Investigation - Employees

7.1. Provided that the CR is satisfied that sufficient concern or evidence exists to indicate that a fraud may have been committed, the investigation team will manage the investigation. The investigation will be performed by Internal Audit and under guidance of the CFO or GS. Members of staff with key skills or external specialist may be called in for assistance for very technical matters, for example electronic data capture.

7.2. The CR will set the terms of reference, its scope of operations and an initial time allocation with specific monitoring points. There will be full compliance with the requirements of the HOPE'87 procedures and guidelines.

7.3. Where the investigation team feels that an interview will be necessary this will be discussed with the CR who will verify compliance with all national laws.

7.4.All prosecution cases will be reviewed by a member of legal representative of HOPE'87, dealing with all aspects of court proceedings, including arranging trial dates and arranging for any HOPE'87 opinions.

7.5. The CR has direct access to the relevant police authorities who can be consulted at an early stage and then as appropriate to provide informal advice on the conduct of the investigation.

7.6. The CR will report back to the Director of Finances, Director Operations or the supervisor at the agreed points or earlier, should the results of the investigation dictate.

7.7. The update will include discussion of decisions regarding:

- involvement of the police
- action to be taken (if any) against the suspected perpetrator
- communications with external bodies
- proposed action regarding recovery of losses
- the level of any additional routine or ad hoc investigations required
- in related areas;
- producing and issuing of reports to the CFO and GS

8. Losses

8.1. Where there is a reasonable chance of recovery, HOPE'87 will take steps to recover losses through all available means available.

9. Management of External Affairs

9.1.Dependent on the size of the fraud and the extent of the investigation, the CR in discussion with the CFO or GS will consider whether and when to:

- involve the police
- consult with third parties, such as legal advisors

9.2. Individuals involved in the investigation must not take decisions alone to involve external organisations. These decisions must lie with the main team since any ill-thought-out or spontaneous comments/acts may jeopardise the whole investigation.

10. Witness Support

10.1. HOPE'87 acknowledges that fraud investigations may place witnesses in a stressful situation, both during the course of the investigation and during any subsequent disciplinary or court appearance where they may be required to give evidence. HOPE'87 will attempt to support witnesses, in accordance with the following principles as discussed below:
10.2. Support at Work: in serious circumstances, HOPE'87 would consider redeploying witnesses where a difficult relationship would result because of allegations being made.
10.3. Support at a Disciplinary/Court hearing: if a witness is appearing at a disciplinary or a Court hearing, HOPE'87 will support the witness with access to confidential counselling services to be provided by the organization.

11. Review of Fraud Investigation Policy

11.1. This Policy will be reviewed every third year and following any major fraud.

6.4. HOPE'87 Basic Document

HOPE'87 fully endorses the Whistleblowing Protection Policy of the International Federation of the Red Cross and Red Crescent Societies as follows.

For this purpose,
the term „The Federation" shall be read as „HOPE'87"
the term „ Federation's" shall be read as „HOPE'87's"
the term „Federation Personnel" shall be read as „HOPE'87 Personnel"
the term „Human Resources in Geneva" shall be read as „HOPE'87 Vienna HQ"
the term „through Safecall, a confidential service run by an independent third party, at ifrc@safecall.co.uk." shall read as "through e-mail to the HOPE'87 e-mail address"
the term "Federation's Internal Rules" shall be read as „HOPE'87's Internal Rules"
the term " Head of the Human Resources" shall be read as „(the) HOPE'87 Secretary General"
the term " Head of the Human Resources" or „Head of the Human Resources Department" shall be read as „(the) HOPE'87 Assistant Secretary General"

Whistleblower Protection Policy

Document reference number: 205

Version number: 1.00 Authorization date: 3 August 2015

Table of contents

1. Purpose, scope and audience

1.1 The Federation has a zero tolerance policy to any form of retaliation against a person who either reports reasonably held suspicions of a breach of the Federation's Internal Rules or who cooperates in an audit or investigation process carried out under the authority of the Secretary General. In furtherance of this zero tolerance policy, the Secretary General is committed to ensuring:

- ➢ ·compliance with the Federation's rules, regulations, policies and procedures ("Federation's Internal Rules") by establishing controls intended to prevent and deter their violation; and
- ➢ ·that the Federation benefits from prompt notification of a possible breach of the Federation's Internal Rules ("alleged misconduct") so that appropriate action can be taken in the best interests of the organization; and
- ➢ ·the protection of any person in the service of the Federation ("Federation Personnel") against retaliation for reporting a suspicion of alleged misconduct or for cooperating in an authorized audit or investigation process.

1.2 With this in mind, the purpose of this Whistleblower Protection Policy ("the Policy") is to:

- ➢ ·set out the principles and processes for reporting a suspicion of alleged misconduct;
- ➢ ·establish the procedures for protecting individuals who report a suspicion of alleged misconduct from any form of retaliation; and
- ➢ ·reinforce a culture in which the Federation functions and is seen to function in an open, transparent and fair manner.

1.3 Protection against retaliation is extended to any Federation Personnel (regardless of the type of contractual arrangement or its duration) when that individual both:

- ➢ ·has reported a suspicion of alleged misconduct or participated in an authorized audit or investigation, and
- ➢ ·claims, on reasonable grounds, that retaliation has occurred or is apprehended, as a direct result of reporting his/ her suspicion of alleged misconduct or participating in an authorized audit or investigation.

2. Definitions, principles and procedures

2.1 Definitions

2.1.1 “Alleged misconduct” refers to allegations of a possible breach of the Federation’s Internal Rules.

2.1.2 “Federation’s Internal Rules” refers to the Staff Rules, the Staff Regulations, including the Code of Conduct and any other regulations, rules and policies adopted by the Secretary General and considered to be binding.

2.1.3 “Federation Personnel” refers to any person in the service of the Federation, including: Employees, National Staff, Seconded Staff, Staff-on-Loan, Volunteers, Interns and service providers engaged under a contractor/consultancy agreement.

2.1.4 “Retaliation” or “retaliatory action” means any direct or indirect detrimental action recommended, threatened or taken because an individual has reported a suspicion of alleged misconduct or participated in an authorized audit or investigation. Retaliation may include adverse administrative actions, such as, but not limited to, unwarranted poor performance evaluations, changes in job duties or other negative decisions affecting the individual’s terms and conditions of employment. Retaliation may also take the form of verbal abuse or harassment.

2.1.5 “Whistleblower” refers to an individual who reports a suspicion of a breach of the Federation’s Internal Rules. Whistleblowers provide information, based on a reasonably held suspicion that a wrongdoing has occurred.

2.2 Principles

2.2.1 All Federation Personnel have a duty to report potential breach of the Federation’s Internal Rules that may come to their attention, and thus help protect the organisation and the resources entrusted to it. It is also the duty of all Federation Personnel to cooperate with an authorized audit or investigation.

2.2.2 An individual who reports in good faith a suspicion of alleged misconduct or cooperates in an authorized audit or investigation has the right to be protected by the Federation against retaliation.

2.2.3 It is the Federation’s responsibility to take all necessary, relevant measures to protect Federation Personnel against retaliation in the context of a report of a suspected alleged misconduct or for participating in an authorized audit or investigation. For these reasons, the Federation maintains an environment where it can receive and address concerns and complaints in confidence.

2.2.4 Retaliation against individuals who have reported a suspicion of alleged misconduct or participated in an audit or investigation violates the obligation of all Federation Personnel to

uphold the highest standards of integrity and to discharge their functions and regulate their conduct with the best interests of the organization in view.

2.2.5 When established, retaliation constitutes misconduct in itself and will be subject to appropriate administrative or disciplinary action.

2.3 Reporting a Suspicion of Alleged Misconduct through the Established Channels

2.3.1 A suspicion of alleged misconduct should be reported in writing as soon as possible and normally not later than 6 months after the whistleblower has come to learn of the specific event(s). The report should be factual and contain as much information as possible to allow for a proper assessment of the nature, extent and urgency of the matter.

2.3.2 Reports of a suspicion of alleged misconduct should be made through the established internal channels, as follows, either:

- ·directly to Human Resources in Geneva or in the field, or
- ·to the whistleblower's line manager(s) or any Senior Manager, or
- ·to the Risk Management and Audit department, or
- ·through Safecall, a confidential service run by an independent third party, at ifrc@safecall.co.uk.

2.3.3 In all cases, the line manager or Senior Manager or the Risk Management and Audit Department shall refer the matter to the Head, Human Resources, who shall acknowledge receipt of the report of the alleged misconduct normally within three days of receipt thereof.

2.4 Reporting a Suspicion of Alleged Misconduct to Outside Entities

2.4.1 Federation Personnel are expected to report any suspicions of alleged misconduct through the established internal channels as stated in paragraph 2.3 above.

2.4.2 Nonetheless sub-paragraph 2.4.1, the Federation will also extend the protections in this Policy to a whistleblower who reports alleged misconduct by a Federation Personnel to an entity or individual outside of the Federation, on condition that the whistleblower did not accept payment or any other benefit from any party for such report, and he/she did not use the internal channels set out in paragraph 2.3 above because:

- ·at the time the report was made, he/she had reasonable grounds to believe that he/she will be subjected to retaliation by the person(s) he/she should report to pursuant to the internal channels; or
- ·he/she could show that it was likely that evidence relating to the alleged misconduct would have been concealed or destroyed if he/she had reported to the person(s) he/she should report to pursuant to the internal channels; or
- ·a previous report was made with the same information through the internal channels, and the Federation took no action.

2.4.3 In addition, the whistleblower must show that he/she reported to an outside entity because he/she considered that such reporting was necessary to avoid:

- a significant threat to public health and safety; or
- substantive damage to the Federation's operations; or

- violations of national or international law.

2.5 Confidentiality and Anonymity

2.5.1 Reports of a suspicion of alleged misconduct will be kept confidential to the maximum extent possible, consistent with the need to conduct a proper review and, if determined, an investigation. In situations whereby the whistleblower is needed to provide evidence, his/her identity shall be revealed only with his/her consent or if required by law.

2.5.2 The Federation discourages anonymous reporting as the protections extended in this Policy cannot then be accorded to the whistleblower. Notwithstanding, in case of a reasonable fear of adverse reaction from the person reasonably suspected as having committed alleged misconduct, or a superior, reports may be made anonymously through Safecall as per sub-paragraph 2.3.2 above. Any reports received by anonymous means shall be investigated at the discretion of the Federation depending on an assessment of the credibility of the information provided.

2.6 Reports made in Bad Faith

2.6.1 Anyone reporting a suspicion of alleged misconduct must be acting in good faith and have reasonable grounds for believing the information disclosed constitutes a potential breach of the Federation's Internal Rules.

2.6.2 Any report, accusation or statement that is shown to have been intentionally false, defamatory or misleading, or is made with reckless disregard as to the accuracy of the information, or is done with malice, will be considered a violation of acceptable standards of conduct and will lead to administrative or disciplinary action in accordance with the procedures applicable to the whistleblower's type of appointment.

2.7 Addressing Reports of Suspicions of Alleged Misconduct

2.7.1 Upon receipt of a report of a suspicion of alleged misconduct, the Head of Human Resources, in consultation with the Legal department shall conduct a preliminary assessment of the report. Such assessment may include preliminary fact-finding.

2.7.2 If the report might involve a fraud or financial matters, Human Resources and the Legal department will consult with the Risk Management and Audit department.

2.7.3 Human Resources and/or the Risk Management and Audit department shall investigate the matter, as deemed necessary, in accordance with the established procedures set out in the Staff Regulations and Rules, the Internal Audit Charter and the Standards of Investigations, or national law, as applicable.

2.8 Retaliation Claims

2.8.1 Individuals who have reasonable grounds to believe that retaliatory action has been taken against them, or will be taken against them, because they reported a suspicion of alleged misconduct or participated in an authorized audit or investigation should forward all information and documentation available to them to support their claim to the Head of the Human Resources department.

2.8.2 The retaliation claim should be made as soon as possible and in any case normally no later than 6 months after the date of the alleged act of retaliation has occurred (or the date of the last act of retaliation if a series of such acts is alleged to have occurred).

2.8.3 The functions of the Human Resources department with respect to protection against retaliation are as follows:

- ➢ ·to receive and acknowledge a retaliation claim;
- ➢ ·to keep a confidential record of all claims received; and
- ➢ ·to conduct a preliminary review of the claim to determine if there is a prima facie case that the reporting of the alleged misconduct or the participation in the authorized audit or investigation was a contributing factor in causing the alleged retaliation.

2.8.4 If the Head of the Human Resources department finds that there is a prima facie case of retaliation or threat of retaliation, he/she will refer the matter to the Secretary General with a recommendation that the claim be investigated in accordance with the applicable procedures.

2.8.5 The Human Resources department shall notify the whistleblower that the matter has been referred to the Secretary General, and of the Secretary General's decision thereon.

2.9 Interim Measures

2.9.1 Pending the completion of the investigation and without prejudice to its outcome, the Head of the Human Resources department may on the basis of its own preliminary review recommend that the Secretary General take appropriate interim measures to safeguard the protection of the claimant, including but not limited to temporary suspension of the implementation of the action reported as retaliatory and, with the consent of the claimant, his/her temporary reassignment or, to the extent necessary, his/her placement on special leave with full pay.

2.10 Measures in respect of a finding of Retaliation

2.10.1 If retaliation is established, the Head of the Human Resources department will, after consultation with the Legal department and, as appropriate, the Risk Management and Audit department, and the individual concerned who has suffered retaliation, recommend to his/her manager(s) appropriate measures aimed at correcting negative consequences suffered as a result of the retaliatory action. Such measures may include, but are not limited to, the withdrawal of the retaliatory decision, or other actions such as reinstatement or a transfer, if applicable, with the individual's consent to another office away from the person who engaged in retaliation.

2.11 Action against a Federation Personnel who engages in Retaliation

2.11.1 Any retaliatory actions by a Federation Personnel against a whistleblower, including a contractor or its employees or representatives, or any other individual engaged in any dealings with the Federation, because such person has reported alleged misconduct is a violation of the Federation's standards of conduct and will lead to appropriate administrative or disciplinary actions in accordance with the applicable procedures.

2.12 Internal Recourse Procedures

2.12.1 The procedures set out in this Policy are without prejudice to the rights of the whistleblower who has suffered retaliation, or the individual who is found to have engaged in retaliation, to appeal or seek redress, as the case may be, through the internal recourse mechanisms applicable to their type of appointment.

6.5. Basic Document HOPE'87 **Incident Report and Preliminary Investigation**

Case opened on: **Case closed on:**	
Case in charge of (tick and give details as to the investigating officer in charge): **HQ:** **CO:** **Law enforcement agency**:	
Incident reported under the HOPE'87 Whistleblowing Policy:	Yes: No:
If the incident was reported outside the HOPE'87 Whistleblowing Policy, give details:	
Give details to the person reporting and the ways of reporting:	
In case of anonymous concern, how did the concern raised reach HQ?	
In case of anonymous concern, did the person reporting request to remain anonymous?	
In case of anonymous concern, did the person reporting request to be contacted and /or informed?	
Outline concern:	
Facts disclosed:	
The suspected irregularity relates to: - questionable or inappropriate accounting practices, internal (accounting) controls or auditing matters; - a criminal offence (e.g. theft or fraud); - a violation of laws and regulations; - an intentional provision of incorrect information to public authorities; - a danger to the public or employees' health, safety and/or security; - sexual harassment; - abuse of authority, including instructions not to report a Suspected Irregularity under a Whistleblower and Internal Complaints Procedure;	

- another violation of the HOPE'87 Code of Conduct or related internal policies; - any other conduct that could have a detrimental or adverse effect on the reputation or financial situation of HOPE'87; - an intentional suppression, destruction, or manipulation of information regarding or relating to any suspicion referred to above.	
Individuals/ units suspected to be involved:	
Supporting evidence:	
Risk to organisation, unit or individual suspected:	
Measures taken by officer in charge:	
Who else has been informed about this case and/or the measures taken (adhering to the EU General Data Protection Regulation (GDPR)?	
Are the allegations substantive (if the allegations are true, would this suggest that there is a significant irregularity or misconduct for which HOPE'87 needs to take action, especially against the accused)?	
Can the allegations be substantiated with the details provided by the person reporting?	
Details of the preliminary investigation:	
Is the information received sufficient to facilitate a full investigation?	
If the information received is sufficient to facilitate a full investigation, which action was taken?	**If the information received is not sufficient to facilitate a full investigation, which action was taken?**

Result of the preliminary investigation:	
Was a respective note made in the HOPE'87 Security Incident Register (Basic Doc 8.7.)?	
Individuals/ units suspected informed about the result of the preliminary investigation on:	
Person reporting informed about the result of the preliminary investigation (while respecting the wishes of the whistle-blower to remain anonymous) on**:**	
Any further information:	