

Anti Fraud Policy

Reviewed September 2007

Anti-Fraud Policy

1. Introduction

1.1 The Agency requires all staff at all times to act honestly and with integrity and to safeguard the public resources for which the organisation is responsible.

1.2 Fraud is an ever-present threat to these resources and hence must be a concern to all members of staff and persons employed in a similar capacity. Fraud may occur internally or externally and may be perpetrated by staff, consultants, suppliers, contractors or development partners, individually or in collusion with others.

1.3 The purpose of this document is to set out your responsibilities with regard to fraud prevention, what to do if you suspect fraud and the action that will be taken by management.

2. Definitions of Fraud

2.1 In law there is no specific offence of fraud and many of the offences referred to as fraud are covered by the Theft Acts of 1968 and 1978. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation, false representation, concealment of material facts and collusion. For practical purposes fraud may be defined as the use of deception with the intention of obtaining an advantage, avoiding an obligation or causing loss to another party. The criminal act is the attempt to deceive and attempted fraud is therefore treated as seriously as accomplished fraud.

2.2 Computer fraud is where information technology equipment has been used to manipulate programs or data dishonestly (for example, by altering, substituting or destroying records, or creating spurious records), or where the use of an IT system was a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and resources, including unauthorised personal browsing on the Internet, is included in this definition.

3. Safety Net Associates' Responsibilities

3.1 Irrespective of the amount involved, all cases of attempted, suspected or proven fraud shall be reported to the Managing Director or CEO. Where cases of a substantial, novel or unusual nature arise, these will be notified immediately to the Senior Management Team. The organisation will:

- ensure it has suitable policies and practices in place to safeguard itself against fraud and theft;
- ensure that it communicates its policy on fraud to staff in a formal policy statement;
- prepare an annual report on fraud and theft;
- Expect periodic checks by our appointed accountants on whether any new or suspected frauds have been detected.

3.2 The Chief Executive, as Safety Net Associates Limited' CEO, carries overall responsibility for the prevention of fraud, and is liable to be called to account by the Managing Director for specific failures. However, the above responsibilities fall directly on line management and may involve all staff in Safety Net Associates Limited.

4. Associates' Responsibilities

4.1 The day-to-day responsibility for the prevention and detection of fraud rests with line Associates who are responsible for:

- Identifying the risks to which systems, operations and procedures are exposed;
- Developing and maintaining effective controls to prevent and detect fraud; and
- Ensuring that controls are being complied with.

5. Staff Responsibilities

5.1 All staff, including Associates, is responsible for:

- Acting with propriety in the use of Safety Net Associates Limited' resources and in the handling and use of public funds whether they are involved with cash or payment systems, receipts or dealing with contractors, suppliers or customers;
- Reporting details immediately to the CEO if they suspect or believe that there is evidence of irregular or improper behaviour or that a fraud may have been committed.

6. Fraud Response Plan

6.1 The Agency has prepared a Fraud Response Plan (see Annex A), which should act as a checklist of actions and a guide to follow in the event that fraud is suspected. It covers:

- Notifying suspected fraud;
- The investigation process;
- Liaison with police and external audit;
- Initiation of recovery action;
- Reporting process;
- Communication with Law enforcement agencies.

7. Disciplinary Action

7.1 In the case of proven fraud, or suspected fraud of a serious nature, Safety Net Associates Limited reserves the right to refer the matter to the police at the earliest possible juncture.

7.2 Notwithstanding this, and following appropriate investigations, the Chief Executive will determine whether to invoke action in accordance with established disciplinary procedures.

8. Personal Conduct

8.1 As stewards of public funds all staff must have, **and be seen to have**, high standards of honesty, propriety and personal integrity. Staff are required to report any potential conflict of interest to the Managing Director and the Chief Executive. Staff should not accept gifts, hospitality or benefits of any kind from a third party which might be seen to compromise their personal judgement and integrity.

9. Conclusion

9.1 Safety Net Associates Limited views fraud very seriously. All instances will be investigated rigorously and promptly and appropriate action will be taken.

9.2 Further advice may be obtained from the CEO, 0845 094 6478.

ANNEX A: FRAUD RESPONSE PLAN

1. Introduction

1.1. This fraud response plan provides a checklist of actions and a guide to follow in the event that fraud is suspected. It covers:

- Notifying suspected fraud;
- The investigation process;
- Liaison with police and external audit;
- Initiation of recovery action;
- Reporting process;
- Communication with Law enforcement agencies.

1.2 Its purpose is to define authority levels, responsibilities for action and reporting lines in the event of suspected fraud, theft or other irregularity.

2. Notifying Suspected Fraud

2.1. It is important that all staff are able to report their concerns without fear of reprisal or victimisation and are aware of the means to do so. The Public Interest Disclosure Act 1998 (the "Whistle-blowers Act") provides appropriate protection for those who voice genuine and legitimate concerns through the proper channels.

2.2 In the first instance, any suspicion of fraud, theft or other irregularity should be reported, as a matter of urgency, to your line manager. If such action would be inappropriate, your concerns should be reported upwards to one of the following persons:

- Head or Lead Associate (or equivalent);
- Managing Director;
- Chief Executive.

2.3 Additionally, all concerns must be reported to the Company Secretary.

2.4. Every effort will be made to protect an informant's anonymity if requested. However, the organisation will always encourage individuals to be identified to add more validity to the accusations and allow further investigations to be more effective. In certain circumstances, anonymity cannot be maintained. This will be advised to the informant prior to release of information.

3. The Investigation Process

3.1. Suspected fraud must be investigated in an independent, open-minded and professional manner with the aim of protecting the interests of both the organisation and the suspected individual(s). Suspicion must not be seen as guilt to be proven.

3.2. The investigation process will vary according to the circumstances of each case and will be determined by the Chief Executive in consultation with the Managing Director. An "Investigating Officer" will be appointed to take charge of the investigation on a day-to-day basis. This will normally be the CEO or Company Secretary or, exceptionally, another independent associate.

3.3 The Investigating Officer will appoint an investigating team.

3.4 Where initial investigations reveal that there are reasonable grounds for suspicion, and to facilitate the ongoing investigation, it may be appropriate to suspend an employee against whom an accusation has been made. The Chief Executive, in consultation with the Managing Director, will take this decision. Suspension should not be regarded as disciplinary action nor should it imply guilt.

3.5 It is important, from the outset, to ensure that evidence is not contaminated, lost or destroyed. The investigating team will therefore take immediate steps to secure physical assets, including computers and any records thereon, and all other potentially evidential documents. They will also ensure, in consultation with management, that appropriate controls are introduced to prevent further loss.

3.6 The Investigating Officer will ensure that a detailed record of the investigation is maintained. This should include a chronological file recording details of all telephone conversations, discussions, meetings and interviews (with whom, who else was present and who said what), details of documents reviewed, tests and analyses undertaken, the results and their significance. Everything should be recorded, irrespective of the apparent significance at the time.

3.7 All interviews will be conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police will be consulted and interviews may be conducted under caution in compliance with the Police and Criminal Evidence Act (PACE), which governs the admissibility of evidence in criminal proceedings.

3.8 The findings of the investigation will be reported to the Chief Executive, who will determine, in consultation with the Investigating Officer, what further action (if any) should be taken.

4. Liaison with Police & External Audit

4.1. The police generally welcome early notification of suspected fraud, particularly that of a serious or complex nature. Some frauds will lend themselves to automatic reporting to the police (such as theft by a third party). For more complex frauds the Chief Executive, following consultation with the Managing Director and the Investigating Officer will decide if and when to contact the police. The CEO will report suspected frauds to the external auditors at an appropriate time.

4.2. All staff will co-operate fully with any police or external audit enquiries, which may have to take precedence over any internal investigation or disciplinary process. However, wherever possible, teams will co-ordinate their enquiries to maximise the effective and efficient use of resources and information.

5. Initiation of Recovery Action

5.1 The Organisation will take appropriate steps, including legal action if necessary, to recover any losses arising from fraud, theft or misconduct. This may include action against third parties involved in the fraud or whose negligent actions contributed to the fraud.

6. Reporting process

6.1 Throughout any investigation, the Investigating Officer will keep the Chief Executive, and Managing Director informed of progress and any developments. These reports may be verbal or in writing.

6.2 On completion of the investigation, the Investigating Officer will prepare a full written report setting out:

- Background as to how the investigation arose;
- What action was taken in response to the allegations;
- The conduct of the investigation;
- The facts that came to light and the evidence in support;
- Action taken against any party where the allegations were proved;
- Action taken to recover any losses;
- Recommendations and/or action taken by management to reduce further exposure and to minimise any recurrence.

6.4 In order to provide a deterrent to other staff a brief and anonymised summary of the circumstances will be published on organisation's website.

ANNEX B: DOs & DON'Ts

DO	DON'T
<p>Make a note of your concerns</p> <ul style="list-style-type: none"> Record all relevant details, such as the nature of your concern, the names of parties you believe to be involved, details of any telephone or other conversations with names dates and times and any witnesses. Notes do not need to be overly formal, but should be timed, signed and dated. Timeliness is most important. The longer you delay writing up, the greater the chances of recollections becoming distorted and the case being weakened. 	<p>Be afraid of raising your concerns</p> <ul style="list-style-type: none"> The Public Interest Disclosure Act provides protection for employees who raise reasonably held concerns through the appropriate channels – whistle blowing. You will not suffer discrimination or victimisation as a result of following these procedures and the matter will be treated sensitively and confidentially.
<p>Retain any evidence you may have</p> <ul style="list-style-type: none"> The quality of evidence is crucial and the more direct and tangible the evidence, the better the chances of an effective investigation. 	<p>Convey your concerns to anyone other than authorised persons</p> <ul style="list-style-type: none"> There may be a perfectly reasonable explanation for the events that give rise to your suspicion. Spreading unsubstantiated concerns may harm innocent persons.

Report your suspicions promptly	Approach the person you suspect or try to investigate the matter yourself
<ul style="list-style-type: none">• In the first instance, report your suspicions to your line manager. If this action would be inappropriate.•	<ul style="list-style-type: none">• There are special rules relating to the gathering of evidence for use in criminal cases. Any attempt to gather evidence by persons who are unfamiliar with these rules may destroy the case.