

Finance Policies & Procedures

Anti-Fraud Policy


Contents

1	REVISION HISTORY	2
2	APPROVALS	2
3	SCOPE.....	3
4	INTRODUCTION	3
5	DEFINITIONS OF FRAUD.....	3
6	RESPONSIBILITIES	4
6.1	Staff Responsibilities.....	4
6.2	Managers' Responsibilities.....	4
6.3	Responsibility of Executive Management Team (EMT) and Board.....	4
6.4	Notifying Suspected Fraud.....	4
6.5	The Investigation Process.....	4
6.6	Liaison with Police, Internal and External Audit	5
6.7	Initiation of Recovery Action.....	5
6.8	Reporting process.....	5
6.9	Communication with Audit and Risk Committee and Governing Board	5
7	CONCLUSION.....	5

1 REVISION HISTORY

Revision	Date	By	Change
0	24.11.11	I Barry	
1	25.09.15	R Sloley	Updated
2	31.08.22	R Sloley	Updated and supersedes previous policies on fraud and money laundering.
3	14/10/2022	R Sloley	Updated section 3

2 APPROVALS

Name / Role	Signature and Date
Robert Sloley Chief Financial Officer	 14/10/2022

Anti-Fraud Policy and Response Plan

3 SCOPE

This policy applies to all employees of CABI. This policy does not form part of any employee's contract of employment and may be amended at any time.

4 INTRODUCTION

CABI requires that all staff act with honesty and with integrity and act to safeguard CABI's assets. Fraud is a threat to these assets and all members of staff should be aware of the need to prevent and detect fraud or attempted fraud and act accordingly.

Fraud related prevention and detection in third parties should form part of preliminary due diligence and contractual processes. See also the policies on

- **Authorisation**
- **Procurement**
- **Collaborators**
- **Exclusion from Access to Funding**
- **CABI Code of Business Conduct**

The purpose of this document is to set out the responsibilities for fraud prevention, what to do if fraud is suspected, and subsequent action.

5 DEFINITIONS OF FRAUD

In law there is no specific offence of fraud. The term is used to describe such acts as deception, bribery, forgery, extortion, corruption, money laundering, theft, conspiracy, embezzlement, misappropriation, false representation and accounting (including the falsification of documentation including receipts), 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.

Cyber fraud is where information technology and/or communication devices including mobile phones are used to manipulate or gain access to programs or data dishonestly (for example, by reading, copying altering, substituting, or destroying records, or creating spurious records), to make false representation e.g. phishing emails or texts, or where the use of such systems are a material factor in the perpetration of fraud. Theft or fraudulent use of computer time and assets, including unauthorised personal browsing on the internet, is included in this definition. Cyber is by far the most prevalent category of attempted fraud and so it is important that Information Security policies are followed, and appropriate training completed.

Acts of fraud could be perpetrated by staff, consultants, suppliers, collaborators, or agents, individually or in collusion with others. It is increasingly the case however,

particularly in the case of cyber related incidents, that acts of fraud are perpetrated by individuals or organisations unknown to CABI.

6 RESPONSIBILITIES

6.1 Staff Responsibilities

All CABI staff have responsibility for:

- Acting with propriety in the use of CABI's assets or resources and in the handling and use of funds whether they are involved with cash or payment systems, receipts or dealing with collaborators, agents, suppliers, or customers.
- Using their time and any CABI assets or resources only for the conduct of approved CABI business
- Ensuring compliance with internal systems of control which include policies and procedures.
- Reporting details immediately if they suspect or believe that there is evidence of irregular or improper behaviour or that a fraud may have been committed (see also the '**Whistle Blowing**' Policy)
- Attending the relevant courses of training e.g., Security Awareness Modules

6.2 Managers' Responsibilities

The day-to-day responsibility for the prevention and detection of fraud rests with line managers 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.
- Ensuring compliance with those controls

6.3 Responsibility of Executive Management Team (EMT) and Board

The EMT and Governing Board have overall responsibility for the creation of a culture and framework of controls which minimises the risk and impact of fraud.

6.4 Notifying Suspected Fraud

In the first instance, any suspicion of fraud, theft or other irregularity should be reported to the staff members immediate line manager then escalated as follows:

- in the case of a cyber security issues e.g., phishing emails, to the IT help desk. The IT help desk then has the responsibility to escalate more serious incidents to the CABI IT Director who should then inform EMT.
- for non cyber related fraud issues, to Regional Director or Head of Department and then to member (s) of EMT.

The suspected fraud could also be reported through the process described in the **Whistle Blowing policy** if appropriate.

6.5 The Investigation Process

Suspected fraud must be investigated in an independent, open-minded and professional manner. The investigation process will vary according to the circumstances of each case with the nature and extent of that investigation being determined by EMT. For more serious cases, an "Investigating Officer" may be appointed by EMT to take charge of the investigation and, if required, be supported by

an investigating team comprising staff from CABI and/or externally e.g., the internal auditors.

The Investigating Officer will ensure that a detailed record of the investigation is maintained with any interviews conducted in a fair and proper manner. Where there is a possibility of subsequent criminal action, the police should also be informed.

The findings of the investigation should be formally fed back to EMT who will determine what further action (if any) should be taken. Any internal disciplinary process will be based upon CABI's disciplinary rules and procedures.

6.6 Liaison with Police, Internal and External Audit

Some frauds will lend themselves to automatic reporting to the police (such as theft by a third party). For incidents of suspected fraud, the CFO and/or CFO should be consulted prior to local police being informed.

All staff should co-operate fully with any police 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 assets and information.

6.7 Initiation of Recovery Action

CABI 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.

6.8 Reporting process

The Executive Director IT is responsible for regular reporting of Cyber security related incidents to EMT whether in aggregate or on an individual case basis.

Where a formal fraud investigation has been initiated by EMT, the Investigation Officer will keep the Chief Executive Officer and the rest of EMT informed of progress and developments. A formal written report should be produced and submitted to EMT at the conclusion of the investigation.

6.9 Communication with Audit and Risk Committee and Governing Board

Significant cases of attempted, suspected or proven fraud should be reported (at the next scheduled meeting (s) or earlier) to the Audit and Risk Committee and the Governing Board by the Chief Executive Officer and/or the Chief Financial Officer.

7 CONCLUSION

CABI views fraud very seriously and is committed to taking all reasonable steps in the prevention, detection, investigation, reporting and, where appropriate, the prosecution of fraud. Further advice may be obtained from the Chief Financial officer based at Wallingford in the UK.