SEUPB

Anti-Fraud Policy

V1.0 Updated 02/10/17

SEUPB

Anti-Fraud Policy

Contents

1 Introduction

1.1 Our commitment to the prevention of fraud

The Special EU Programmes Body (SEUPB) is committed to the prevention of fraud and the promotion of an anti-fraud culture and has adopted a proactive, structured and targeted approach to address all four aspects of the fraud cycle - Prevention, Detection, Corrections and Prosecution.

Any attempt to defraud the EU budget is unacceptable and will not be tolerated. Our policy is to investigate all suspected frauds and allegations. The procedure to be followed in the event of a fraud being detected or suspected is detailed in our Fraud Response Plan.

Staff are required to act honestly and with integrity at all times and to report all suspicions of fraud. Staff are assured that any information which they provide will be treated confidentially, as far as possible, although disclosure may be required if a case goes to court. Staff should consult The SEUPB Reporting Concerns at Work (Whistleblowing) Policy and report their suspicions of fraud without fear of prejudice or harassment.

Every case of attempted, suspected or proven fraud will be thoroughly investigated and where appropriate referred to the Police Service of Northern Ireland (PSNI) and / or An Garda Siochana and / or Police Scotland at the earliest juncture.

The SEUPB will seek to recover funds and assets lost through fraud. After full investigation, the SEUPB will take civil, criminal and/or disciplinary action in all cases where it is appropriate to do so.

1.2 Purpose of this document

The overall purpose of this Anti-Fraud Policy document is to provide a definition of fraud and to outline the key responsibilities regarding the prevention of fraud.
This policy is concerned with:

- External fraud committed by an organisation in receipt of EU funding awarded by SEUPB;
- External fraud committed against the SEUPB, for example by suppliers of goods and services or contractors in the course of their work, or other persons;
- Internal fraud committed against the SEUPB, for example travel and subsistence fraud, theft of assets; and
- Internal fraud committed against SEUPB employees, for example theft of personal property.

This policy should be read in conjunction with the following SEUPB documents available on the SEUPB Intranet:

- SEUPB Code of conduct
- Fraud Response Plan
- Reporting Concerns at Work (Whistleblowing) Policy

2. What is Fraud?

2.1 Definition

The term fraud is commonly used to describe the use of deception to deprive, disadvantage, or cause loss to another person or party. This can include theft, the misuse of funds or other resources or more complicated crimes such as false accounting or the supply of false information. The term fraud is used generically in this policy and covers criminal acts such as bribery, forgery, extortion, corruption, theft, conspiracy, embezzlement, misappropriation and collusion.

Computer fraud is where information technology (IT) equipment has been used to manipulate computer programs or data dishonestly (for example by altering or substituting records, destroying or suppressing records, duplicating or creating spurious records), or where the existence of an IT system was a material factor in the perpetration of fraud (i.e. where the fraud was unlikely to have occurred if there had been no IT system). Theft or fraudulent use of computer facilities, computer programs and the Internet is included in this definition. The suspicion that any of these acts have taken place should be regarded as potentially fraudulent and dealt with as such.

2.2 Legislation

The key legislation which may be used to prosecute fraud is the Fraud Act 2006. The Act refers to three main offences of fraud. An individual can be prosecuted under the Fraud Act 2006 if he makes a false representation, fails to disclose information or abuses his position with the **intention** of making a gain or causing a loss or risk of loss to another. The gain or loss does not actually have to take place.

> **Fraud by false representation**, i.e.: if an individual dishonestly makes a false representation and intends by making the representation to make a gain for himself or another, or to cause loss to another or expose another to risk of loss. A representation is false if it is untrue or misleading, and the person making it knows that it is, or might be, untrue or misleading;
>
> **Fraud by failing to disclose information**, i.e.: if an individual dishonestly fails to disclose to another person information which he is under a legal duty to disclose

and intends, by failing to disclose the information, to make a gain for himself or another, or to cause loss to another or expose another to risk of loss; and

Fraud by abuse of position, i.e.: if an individual occupies a position in which he is expected to safeguard, or not act against, the financial interests of another person, and he dishonestly abuses that position, and intends, by means of the abuse of that position, to make a gain for himself or another, or to cause loss to another or to expose another to a risk of loss.

The Fraud Act 2006 supplements other legislation such as the Theft Act (NI) 1969 and the Theft (NI) Order 1978 which have traditionally been used to cover acts of fraud. In addition, the UK Bribery Act 2010 clarifies the law in relation to bribery and corruption.

In Ireland fraud is criminalized by the Criminal Justice (Theft and Fraud Offences) Act 2001 which creates the offences of theft and dishonesty. The Act also contains provisions on forgery and counterfeiting.

2.3 Examples of fraud

Examples of fraud that may be perpetrated against the SEUPB and its staff are:

- Dishonest use of an SEUPB credit card;
- The dissemination of an email / correspondence to large groups of people falsely representing that the email / correspondence was sent by SEUPB;
- Theft, the misappropriation or misuse of assets for personal benefit;
- Bribery and corruption, offering, giving, soliciting or accepting an inducement or reward that may influence the actions taken by staff, for example, in the procurement of goods and services;
- False accounting and / or making fraudulent statements with a view to personal gain, for example falsely claiming overtime, travel and subsistence, sick leave or special leave (with or without pay);
- Dishonest claims for reimbursement made by project partners within the EU Programmes;
- Falsifying bids in a tender process within an EU funded project; or

- Externally perpetrated fraud against the SEUPB, for example in the procurement and delivery of goods.

The appendices to this document provide a list of fraud indicators; common methods and types of fraud; and examples of good management practices which may assist in combating fraud.

2.4 Anti-Fraud Measures

The SEUPB has put in place proportionate anti-fraud measures based on a thorough fraud risk assessment of our operations. Further to this we have:

- Developed an Anti-Fraud Policy and Fraud Response Plan;
- Developed an anti-fraud culture within SEUPB, training all staff in fraud awareness and key staff in fraud investigations;
- Allocated responsibilities for the overall management of fraud risk
- Commenced the use of IT tools and open source resources to detect risky operations;
- Established well publicized avenues for staff and members of the public to report their suspicions of fraud.

We carry out a vigorous and prompt review into all cases of suspected and actual fraud which have occurred with a view to improve the internal management and control system where necessary.

3. SEUPB's Responsibilities

The SEUPB is committed to preventing fraud from occurring and to developing an anti-fraud culture. To achieve this the SEUPB will take appropriate disciplinary and legal action in all cases, where justified, and review systems and procedures to prevent similar frauds.

It is SEUPB policy that there will be consistent handling of all attempted, suspected or proven fraud cases without regard to the position held or length of service of the individual(s) involved.

SEUPB has a responsibility to report all cases of suspected fraud to the Member States and Accountable Departments.

3.1 Chief Executive Officer's responsibilities

The Chief Executive as Accounting Officer is responsible for developing and maintaining effective internal controls to prevent fraud and ensure that if it does occur it will be detected without delay.

The system of internal control is based on an ongoing process designed to identify the principle risks, evaluate the nature and extent of those risks, and manage them effectively. This embraces all SEUPB activities and relationships and applies to fraud by the SEUPB's staff, members of the public and by contractors supplying goods / services to the SEUPB, or any other contractual or working relationships entered into by the SEUPB including Lead Partners in their Letters of Offer. Specific references are made in agreements with this parties, the content of which is compatible with this policy.

3.2 Director of Corporate Services' responsibilities

The overall responsibility for managing the risk of fraud has been delegated to the Director of Corporate Services. Their responsibilities include:

- Developing a fraud risk profile and undertaking a regular review of the fraud risks associated with each of the key organizational objectives;
- Establishing an effective anti-fraud policy and Fraud Response Plan, commensurate to the level of fraud risk identified in the fraud profile;
- Designing an effective control environment to prevent fraud commensurate with the fraud risk profile;
- Establishing appropriate mechanisms for:
- Reporting fraud risk issues;
- Reporting significant incidents of fraud to the Accounting Officer; and

- Reporting to the Department of Finance (DoF), Department of Public Expenditure and Reform (DPER), the Comptrollers and Auditors General, and all other relevant parties.
- Coordinating assurances about the effectiveness of anti-fraud policies to support the Statement on Internal Control;
- Liaising with the Audit & Risk Committee;
- Making sure that all staff are aware of the organization's anti-fraud policy and know what their responsibilities are in relation to combating fraud;
- Ensuring fraud awareness training is provided as appropriate and, if necessary, more specific anti-fraud training and development if provided to relevant staff;
- Ensuring that vigorous and prompt investigations are carried out if fraud occurs, is attempted or is suspected;
- Ensuring where appropriate, legal and / or disciplinary action against perpetrators of fraud;
- Ensuring, where appropriate, disciplinary action against supervisors where supervisory failures have contributed to the commission of fraud;
- Ensuring, where appropriate, disciplinary action against staff who fail to report fraud;
- Taking appropriate action to recover assets and losses; and
- Ensuring that appropriate action is taken to minimize the risk of similar frauds occurring in the future.

3.3 Line Managers' responsibilities

Line Managers (i.e. staff at Clerical Supervisory level and above) are responsible for ensuring that the system of internal control within their areas of responsibility operates effectively. The responsibility for the prevention and detection of fraud, therefore, rests primarily with managers. There is a need for all managers to assess the types of risk involved in the operations for which they are responsible; to review and test regularly the control systems for which they are responsible ensuring that controls are being complied with; and to satisfy themselves that their systems continue to operate effectively.

A major element of good corporate governance is a sound assessment of the organisation's business risks. **Managers must ensure that**:

- fraud risks have been identified within risk frameworks encompassing all operations for which they are responsible;
- each risk has been assessed for likelihood and potential impact;
- adequate and effective controls have been identified for each risk;
- controls are being complied with, through regular review and testing of control systems; and
- risks are reassessed as result of the introduction of new systems or amendments to existing systems.
- Where a fraud has occurred, or has been attempted, controls are reviewed and new controls implemented as necessary, to reduce the risk of fraud recurring; and
- Fraud occurrences are quantified on an annual basis and Risk Registers/Risk and Control Frameworks updated to reflect the quantum of fraud within the Business Area.

Where appropriate, strategies should be devised to combat recurrence of fraud and targets set to reduce the level of fraud.

In terms of establishing and maintaining effective controls it is desirable that:

- there is a regular rotation of staff, particularly in key posts;
- there is a separation of duties so that control of a key function is not vested in one individual;
- backlogs are not allowed to accumulate; and
- in designing any new system, consideration is given to building in safeguards to prevent and/or detect internal and external fraud.

Senior Management (i.e. Director/Head of Unit level or above), as part of their overall responsibilities, are responsible for providing advice and assistance, where necessary, on risk and control issues. They, in turn, should utilise as appropriate, the services of professional Audit support or the advice of an appropriate source. As fraud prevention is the ultimate aim, anti-fraud measures should be considered and incorporated in every system and programme at design stage, for example the design of application forms.

3.4 Internal Audit's responsibilities

Internal Audit is responsible for the provision of an independent and objective opinion to the Accounting Officer on risk management, control and governance. The adequacy of arrangements for managing the risk of fraud and ensuring the SEUPB promotes an anti-fraud culture is a fundamental element in arriving at an overall opinion.

Internal Audit has no responsibility for the prevention or detection of fraud. However, internal auditors are alert in all their work to risks and exposures that could allow fraud. Individual audit assignments, therefore, are planned and prioritised to assist in deterring and preventing fraud by examining and evaluating the effectiveness of control commensurate with the extent of the potential exposure/risk. Risk and Control Frameworks are also reviewed as a constituent part of each audit assignment to ensure that management have reviewed their risk exposures and, where appropriate, identified the possibility of fraud as a business risk.

3.5 Staff responsibilities

SEUPB staff must have, and be seen to have, the highest ethical and personal standards and be honest and objective in their work. Every member of staff is responsible for conducting themselves in accordance with the seven principles of public life set out in the first report of the Nolan Committee "Standards in Public Life". They are: selflessness, integrity, objectivity, accountability, openness, honesty and leadership.

The SEUPB Code of Conduct sets out the duties and responsibilities of staff and states that "staff should endeavour to ensure the proper, economical, effective and efficient use of resources". Every member of staff has a duty to ensure that public funds are safeguarded, whether they are involved with cash or payments systems, receipts, assets, or dealings with contractors or suppliers.

The appendices to this document provide a list of fraud indicators; common methods and types of fraud; and examples of good management practices which may assist in combating fraud. Staff should familiarise themselves with these documents and should

alert their line manager or a more senior manager where they believe the opportunity for fraud exists because of poor procedures or lack of effective oversight.

Staff should also be vigilant to the possibility that unusual events or transactions could be indicators of fraud and alerting their line manager where they believe the opportunity for fraud exists.

In addition, it is the responsibility of every member of staff to report details immediately to their line manager or a more senior manager if they suspect that a fraud has been committed or see any suspicious acts or events. The Reporting Concerns at Work (Whistleblowing) Policy sets out the procedure that should be followed in these circumstances.

As stewards of public funds staff must have, and be seen to have, high standards of personal integrity. Staff should not accept gifts, hospitality or benefits of any kind from a third party that might be seen to compromise their integrity. Further guidance on the acceptance of gifts and hospitality can be found in the SEUPB Code of Conduct.

It is also essential that all staff understand and adhere to laid down systems and procedures including those of a personnel/management nature such as submission of expenses claims, records of absence, flexi and annual leave.

4. Reporting suspicions of fraud

The SEUPB has in place avenues for reporting suspicions of fraud, without fear of prejudice or harassment. All matters will be dealt with in confidence and the identity of the whistleblower will not be revealed unless the SEUPB is legally required to do so.

4.1 Reporting Concerns

Members of the public may report any concerns they have about an EU funded project or other external fraud by email or by post. A dedicated area on the SEUPB website contains all the contact details for reporting a suspected fraud.

Concerns may be reported anonymously if wished however, providing contact details will assist us should we need to clarify any of the details provided. Although not essential, members of the public may it useful to present the detail of their concern in the format of the SEUPB Concerns Form which is available on our website. The Concerns Form can then be emailed or posted to the SEUPB.

4.2 Reporting Concerns at Work (Whistleblowing)

It is the responsibility of all staff to comply with the Reporting Concerns at Work (Whistleblowing) Policy if they suspect that a fraud has been committed or see any suspicious acts or events.

Staff must assist any investigations by making available all relevant information to the investigating officer (s) and by cooperating in interviews.

Any information provided by staff will be treated confidentially. The Public Interest Disclosure (NI) Order 1998, the Employment Law Compliance Bill 2008 and the Prevention of Corruption (Amendment) Bill 2008 in Ireland protects the rights of staff who report wrongdoing.

4.3 Fraud Response Plan

The SEUPB has established guidelines on how staff and others should report suspicions or allegations of fraud and how the SEUPB will handle them.

The Fraud Response Plan sets out the procedure to be followed when a suspected fraud is identified. A copy of the Fraud Response Plan is available on the SEUPB Intranet and on the public facing website.

5. Conclusion

Fraud can manifest itself in many different ways. The SEUPB has a zero tolerance policy to fraud and corruption, and has in place a robust control system that is designed to prevent and detect, as far as is practicable, acts of fraud and correct their impact should they occur.

This policy and all relevant procedures and strategies are supported by the Audit & Risk Committee who will proactively review and update them on a continual basis.

Any queries in connection with this guidance should be directed to the Director of Corporate Services.

Gina McIntyre
Chief Executive

APPENDIX I - Indicators of Fraud

These include, but are not limited to:

- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured business climate
- Excessive variations to budgets or contracts
- Refusals to produce files, minutes or other records
- Related party transactions
- Increased employee absences
- Borrowing from fellow employees
- Covering up inefficiencies
- No supervision
- Staff turnover is excessive
- Figures, trends or results which do not accord with expectations
- Bank reconciliations are not maintained or can't be balanced
- Excessive unexplained movement of cash funds
- Unauthorised changes to systems or work practices
- Employees with outside business interests or other jobs
- Excessive overtime
- Large backlogs in high risk areas
- Lost assets
- Absence of controls and audit trails
- Lack of thorough investigations of alleged wrongdoing
- Employees suffering financial hardships
- Placing undated/post-dated personal cheques in petty cash
- Employees apparently living beyond their means
- Heavy gambling debts
- Signs of drinking or drug abuse problems
- Conflicts of interest
- Lowest tenders or quotes passed over with scant explanations recorded
- Managers bypassing subordinates
- Subordinates bypassing managers
- Large sums held in petty cash
- Lack of clear financial delegations
- Secretiveness
- Marked character changes
- Excessive ambition
- Apparent lack of ambition
- Excessive control of all records by one officer
- Poor security checking processes over staff being hired
- Unusual working hours on a regular basis
- Refusal to comply with normal rules and practices
- Personal creditors appearing at the workplace
- Non taking of leave

APPENDIX II – Common methods and types of fraud

These include, but are not limited to:

- Payment for work not performed
- Forged endorsements
- Altering amounts and details on documents
- Collusive bidding
- Overcharging
- Writing off recoverable assets or debts
- Unauthorised transactions
- Selling information
- Cheques made out to false persons
- False persons on payroll
- Theft of official purchasing authorities such as order books
- Unrecorded transactions
- Transactions (expenditure/receipts/deposits) recorded for incorrect sums
- Cash stolen
- Supplies not recorded at all
- False official identification used
- Damaging/destroying documentation
- Using copies of records and receipts
- Using imaging and desktop publishing technology to produce apparent original invoices
- Charging incorrect amounts with amounts stolen
- Transferring amounts between accounts frequently with inappropriate authorisation documentation
- Delayed terminations from payroll
- Bribes
- Over claiming expenses
- Skimming odd pence and rounding
- Running a private business with official assets
- Using facsimile signatures
- False compensation and insurance claims
- Stealing of discounts
- Selling waste and scrap

APPENDIX III - Examples of Good Management Practices Which May Assist in Combating Fraud

These include, but are not limited to:

- All income is promptly entered in the accounting records with the immediate endorsement of all cheques
- Regulations governing contracts and the supply of goods and services are properly enforced
- Accounting records provide a reliable basis for the preparation of financial statements
- Controls operate which ensure that errors and irregularities become apparent during the processing of accounting information
- A strong internal audit presence
- Management encourages sound working practices
- All assets are properly recorded and provision is made known or expected losses
- Accounting instructions and financial regulations are available to all staff and are kept up to date
- Effective segregation of duties exists, particularly in financial accounting and cash/securities handling areas
- Close relatives do not work together, particularly in financial, accounting and cash/securities handling areas
- Creation of an agency climate to promote ethical behaviour
- Act immediately on internal/external auditor's report to rectify control weaknesses
- Review, where possible, the financial risks of employees
- Issue accounts payable promptly and follow-up any non-payments
- Set standards of conduct for suppliers and contractors
- Maintain effective security of physical assets; accountable documents (such as cheque books, order books); information, payment and purchasing systems
- Review large and unusual payments
- Perpetrators should be suspended from duties pending investigation
- Proven perpetrators should be dismissed without a reference and prosecuted
- Query mutilation of cheque stubs or cancelled cheques
- Store cheque studs in numerical order

APPENDIX III - Examples of Good Management Practices Which May Assist in Combating Fraud (Continued)

- Undertake test checks and institute confirmation procedures
- Develop well defined procedures for reporting fraud, investigating fraud and dealing with perpetrators
- Maintain good physical security of all premises
- Randomly change security locks (if feasible and economical)
- Conduct regular staff appraisals
- Review work practices open to collusion or manipulation
- Develop and routinely review and reset data processing controls
- Regularly review accounting and administrative controls
- Set achievable targets and budgets, and stringently review results
- Ensure staff take regular leave
- Rotate staff
- Ensure all expenditure is authorised
- Conduct periodic analytical reviews to highlight variations to norms
- Take swift and decisive action on all fraud situations
- Ensure staff are fully aware of their rights and obligations in all matters concerned with fraud