| Integrated Management System | | Date | 22/11/23 |
|---|---|---|---|
| Title | Anti-Fraud Policy and Procedure | Issue | 1 |
| Ref | IMSM.050 | Approved | N. Catton |

# CIS Security Anti-Fraud Policy and Procedure

This Anti-Fraud Policy and Procedure Policy encompasses all actions relating to fraudulent behaviour.

The Policy statements contained represent the basic intentions and goals of the company. They establish the permanent foundation upon which the company operates and are expected to be relatively independent of the changing technologies and methods used to carry them out.

These policies are subject to change from time to time as circumstances dictate, and these changes, when approved by the Board of Directors, will be distributed to all staff. We would like to maintain the highest level of ethics.

The overall goal of Anti-Fraud Policy and Procedure is to prevent fraud and the promotion of an anti-fraud culture. CIS operates a zero-tolerance attitude to fraud and requires all colleagues employed by CIS Security Ltd to act honestly and with integrity at all times, and to report all reasonable suspicions of fraud.

CIS will investigate all instances of actual, attempted, and suspected fraud by employees and will where appropriately seek to recover funds lost to the CIS through fraud. Perpetrators may be subject to appropriate action, including legal action, consistent with company objectives while maintaining the highest ethical standards.

## Definition of fraud

The term ‘fraud’ is commonly used to describe the use of deception to deprive, disadvantage or cause loss to another person or party, or secure unwarranted personal gain.

Examples include (but are not limited to) falsely claiming academic and other achievements,

submitting false documentation, falsely claiming expenses, finance and payroll unauthorised transactions, not declaring absences from the UK, failing to repay advances of stipend or payments an individual is not otherwise entitled to. Individuals can be prosecuted under the Fraud Act 2006 if they make a false representation, fail to disclose information, or abuse their position.

### Reporting suspicions

Those suspecting actual, attempted, or suspected fraud should report their concerns in the first instance to their line manager unless there is suspicion of the line manager, (in these cases report to the Head of Department). Individuals should not attempt to investigate any fraud themselves.

The Line Manager will report all suspicious fraudulent behaviour to the head of their department who will then investigate the suspect behaviour in line with HR policy. The investigation will provide a report on the evidence gathered within 21days, or as soon as practicable thereafter, to the HR Director. The HR Director will normally decide, within 7 days, whether any further action is required, and together with the investigating officer, shall be responsible for the introduction of any change in procedures, or action against any individual.

The HR Director also has responsibility for reporting any circumstances deemed necessary to the Police, and to CIS Senior Management Team as required. Where any complaint is wholly or partially upheld, the HR Director shall provide a report on this, and actions taken as a result, to the next meeting of the Board of Directors.

In the event that any complaint or suspicion should rest on the Board of Directors of the company, then the initial approach may be made to the Managing Director. Alternatively, in such cases approaches may be made as per the CIS Whistleblowing procedures.

## ETHICAL CONSIDERATIONS

Employees shall at all times in the performance of their assigned duties:

- Conduct themselves in a manner consistent with the highest ethical standards including the company's Conflict of Interest Policy and will purchase without prejudice
- Uphold their positions of trust in the conservation and expenditure of company funds
- Be vigilant in preserving and protecting the integrity of the company through daily contacts and business dealings

Sound business relations with vendors are essential in order to maintain a dependable, competent source of supply for the uninterrupted flow of quality goods and services. Honesty, integrity, confidence, and tact should be employed by all CIS Staff when dealing with any suspicious behaviours.

## CONFIDENTIALITY

It is recognised that most of the transactions relating to the company's purchases are confidential, especially with regard to our suppliers and competitors.

It is considered unethical and illegal, as well as damaging to the company's competitive position, and a breach of trust, to allow company proprietary information about one supplier's quotation to pass to another supplier. Discussing proprietary information in telephone calls made/taken while vendors are present, leaving documents on desks during supplier interviews, and conversing with other buyers within hearing of suppliers in other offices are some examples of behaviour that can allow proprietary information to pass to others inappropriately.

Passage of pricing, technologic or strategic information from an employee of the company to an employee of a competitor is not only unethical but is likely to be in violation of one or more of the various antitrust laws and should be scrupulously avoided.

Proprietary information requires protection of the name, composition, process of manufacture, or rights to unique or exclusive information which has marketable value and is upheld by patent, copyright, or non-disclosure agreements. Others in the organisation may be unaware of the possible consequences of the misuse of such information. The Procurement personnel should therefore avoid releasing information to other parties until assured they understand and accept the responsibility for maintaining the confidentiality of the material. Extreme care and good judgement should be used if confidential information is communicated verbally. Such information should be shared only on a "need to know" basis.

Some examples of information which may be considered confidential or proprietary are:

- Pricing
- Bid or quotation information.
- Cost sheets
- Formulas and/or process information
- Design information
- Company plans, goals, strategies, etc
- Profit information
- Asset information
- Wage and salary scales
- Personal information about employees
- Supply sources or supplier information
- Customer lists and/or information
- Computer software programs

The following are recommended guidelines in dealing with confidential information:

- The attitude of the purchasing personnel regarding the preservation and proper disbursement of confidential information should be one of vigilance; ie, divulging information only on a "need to know" basis.

- When transmitting confidential information, document the information in writing, and clearly label it as confidential.

- Consider the use of a formal confidentiality agreement (ie, disclosure or non-disclosure agreements) clarifying parameters for use of the information and responsibilities inherent in its use.

- When dealing with any information, whether or not classified as confidential, extreme care, sound judgement and integrity should be exercised in determining the effects of its use, and in providing adequate protection based on its content.

Signature:

Date:
22/11/2023

Date
reviewed.