The OT Group Limited - Anti Fraud Policy

Background

OT Group has a commitment to high legal, ethical and moral standards. All members of staff are expected to share this commitment and act honestly and with integrity, and ensure their activities and behaviours do not conflict with these obligations.

Definition of Fraud

Fraud describes a number of activities including theft, false accounting, embezzlement, bribery and deception. The Fraud Act 2006 defines three clauses of fraud:

- False representation: a person commits fraud by intentionally and dishonestly making a false representation. A false representation includes intentionally giving a misleading or untrue statement.
- Failing to disclose information: a person commit a fraud if they dishonestly fail to disclose information.
- Abuse of position: a person commits a fraud if they dishonestly abuse their position.

To have committed a fraud a person must have acted dishonestly, and with the intent to: make a gain for themselves or anyone else and/or cause loss to anyone else or expose anyone else to a risk of loss.

The following activities are among those considered to fall in the definition of fraud:

- theft of company property, including information;
- forgery or alteration of company documents;
- wilful destruction or removal of company records;
- falsification of expense claims;
- unauthorised disclosure of confidential information to third parties;
- misappropriation or use of company assets for personal gain;
- undertaking or assisting in illegal activity (including money laundering);
- acceptance of bribery or gifts to favour third parties – see the Group's Anti Bribery Policy);
- knowingly generating or paying false claims or invoices.

OT Group's Policy

Fraud risk can best be managed through preventative and detective control measures. The Group is committed to the continuous improvement of fraud prevention and detection techniques. Management has a responsibility to ensure adequate anti-fraud measures and controls are present in the Group's systems. However all staff are expected to be vigilant and play an active part in anti-fraud activity.

The overt investigation of all actual or suspected instances of fraud and the prosecution of offenders provides an effective deterrent. Therefore, all known or suspected incidences of fraud will be thoroughly and impartially investigated.

Corporate Objectives

To develop an anti-fraud culture and define management and employee responsibilities in this area.

To reduce the opportunity for fraud by introducing preventive and detective measures into systems and processes.

To promote an open and ethical culture within the organisation which deems unethical behaviour unacceptable.

To increase the vigilance of management and staff through raising fraud risk awareness.

To ensure that the directors of the group meet their statutory responsibilities towards fraud, as per the Companies Act and the Turnbull requirements for corporate governance.

To learn from previous incidents and recycle lessons and experiences in fraud prevention and detection globally.

To encourage management and staff to report their suspicions while guaranteeing anonymity where requested.

Reporting Suspicions of Fraud

OT Group wishes to encourage anyone having reasonable suspicions of fraud to report them. Therefore it is also OT Group's policy, which will be rigorously enforced, that no employee will suffer in any way as a result of reporting reasonably held suspicions.

All members of staff can therefore be confident that they will not suffer in any way as a result of reporting reasonably held suspicions of fraud. For these purposes reasonably held "suspicions" shall mean any suspicions other than those, which are raised maliciously and found to be groundless. The organisation will deal with all occurrences in accordance with the Public Interest Disclosure Act.

FRAUD CONTROL PRINCIPLES - SUMMARY

PREVENT

- Employees – pre-employment check
- Customers/Suppliers:
    - credit checking
    - payment detail confirmation
    - matching of all invoices of goods to confirmed deliveries
    - authorisation for payment of all invoices for services by senior manager
    - review of all payments by Group FD and for stock Group Procurement Director
    - new supplier process and assessment
    - payments require bank authorisation by 2 separate authorised individuals, one of which is from the management board
- Staff Updates: reminders/updates issued to staff on cyber security and other similar threats

DETECT

- Monitoring of information systems
- Monitoring network activity and responding to alerts and notifications
- Staff reporting

RESPOND

- Any breach/suspected breach of information security is reported and investigated.
- Actions will be agreed to disable/prevent/notify outcome of investigation.
- Communication with affected parties.

REMEDIATE

- Investigation will include analysis of cause and any actions needed

This policy is reviewed on an annual basis, or more frequently should systems/processes or legislation change.