TEG FRAUD POLICY

Current as of March 2024

Purpose

This policy defines the TEG Group's fraud control principles, mandatory requirements, and accountabilities. It clearly articulates that the Group does not tolerate fraud and is committed to promoting and maintaining a sound ethical culture.

All employees, temporary staff, contractors, and service providers must ensure they are aware of their responsibilities and obligations with respect to the prevention, detection, and reporting of fraud.

This Policy is applicable to all businesses within the Group, including entities where the Group has a controlling interest.

Scope

All TEG employees

Policy Statement

This policy is designed to ensure the prevention, detection, and reporting of fraud.

Policy Owner and Effective Date

Group Chief Financial Officer
Effective Date: 12 August 2022
Review Date: 1 February 2025

TEG Fraud Policy

MONITORING COMPLIANCE

All department heads are required to identify and manage their fraud risks to protect the Group's customers, assets, and reputation. All employees, temporary staff, contractors, and service providers are required to:

- Report all allegations, suspicions or detection of fraud or forgery.
- Adhere to the relevant fraud policy, standards, guidelines, and procedures.
- Complete mandatory fraud and security training on a timely basis.
- Comply with applicable legislation including the Crimes Act 1900 (NSW) and Criminal Code Act 1995 (Cth) and Corporate Criminal Offence (CCO) legislation in the UK

Any irregularity that is detected or suspected must be reported immediately to your department head who will refer it to the Group CFO and/or Group Financial Controller, who will manage all investigations with the People & Culture Department and the impacted department/s. If deemed appropriate, the matter will also be referred to the appropriate regulatory authorities for the specific market.

We place great importance on fostering a culture that encourages employees and others that partner with TEG Group to speak up when noticing something which just doesn't feel quite right to serious misconduct.

ACTIONS CONSTITUTING FRAUD

Fraud or fraudulent activity is broadly defined as obtaining property belonging to another, obtaining a financial advantage, or causing a financial disadvantage by deception. This extends to the use of an electronic device to cause an outcome it is not authorised to undertake.

Types of fraud include, but are not limited to:

- Asset misappropriation.
- Misdirection of company funds into an unauthorised personal bank account (including superannuation funds).
- Impropriety in the handling of company funds.
- Inflated expense claims.
- Use of expense accounts or company credit cards for personal expenses.
- Destroying or concealing accounting records; and/or
- Unauthorised personal use of company assets.

Similarly, it is also an offence to intentionally make or publish a false or misleading statement or destroy or conceal an accounting record with the intention to commit fraud as defined above.

If there is any question as to whether an action constitutes fraud, contact the Group CFO and/or Group Financial Controller for guidance.

ACTS CONSTITUTING FORGERY

Forgery is the use or making of a false document intending it to be used to induce a person to accept it as genuine, and, due to that acceptance, commit fraud in the manner defined above.

Types of forgery include, but are not limited to:

- The creation or altering of financial records.
- Utilisation of false invoices; and/or
- The creation of false emails.

MITIGATING FRAUD CONTROLS

Control procedures to mitigate the risk of fraud can either be preventative or detective, or both, in nature. Examples of each include:

Preventative:

- workplace policies and culture promoting and encouraging ethical behavior
- new employees and contractors' acknowledgement of policies upon commencement
- regular policy updates and communication to staff
- online fraud awareness training
- high-risk employees subject to annual acknowledgement of some policies
- Authorisation and dual check controls within key processes
- segregation of duties (including some enforced by systems and automated workflow)
- periodic review of fraud risks and scenarios
- pre-employment screening and background checks
- system access controls
- centralised operations
- automated daily transaction processing
- physical security controls

Detective:

- escalation and provision of whistleblowing (Refer to Whistleblower Policy)
- reviews of exception reports and reconciliations and other management reporting
- exception reporting for some systems
- periods of consecutive staff leave without office/telecommunication contact
- assurance and compliance functions

INVESTIGATION RESPONSIBILITIES

The Group CFO will determine the staff to be involved in the investigation of all suspected fraudulent acts as defined in this policy. If the investigation substantiates that fraudulent activities have occurred, the relevant SLT member and/or Group CFO will inform the Group CEO, SLT, and, if appropriate, the TEG Board of Directors.

Any investigative activity required will be conducted without regard to the suspected wrongdoer's length of service, position/title, or relationship to the Company.

Decisions to prosecute or refer the case to the appropriate law enforcement and/or regulatory agencies for independent investigation will be made in conjunction with the SLT, as will final decisions on disposition of the case.

CONFIDENTIALITY

The Investigating Team will treat all information received confidentially, where possible. Any staff member who suspects dishonest or fraudulent activity will notify their relevant department head and/or the Group CFO immediately and should not attempt to personally conduct investigations or interviews/interrogations related to any suspected fraudulent act.

Investigation results will not be disclosed or discussed with anyone other than those who have a legitimate need to know. This is important in order to avoid damaging the reputations of persons suspected but subsequently found innocent of wrongful conduct and to protect the TEG Group from potential civil liability.

AUTHORISATION FOR INVESTIGATING SUSPECTED FRAUD

Members of the Investigating Team will have:

- Free and unrestricted access to all Company records and premises, and
- The authority to examine, copy, and/or remove all or any portion of the contents of files, desks, cabinets, and other storage facilities on the premises without prior knowledge or consent of any individual who might use or have custody of any such items or facilities when it is within the scope of their investigation.

BREACH OF POLICY

TEG Group has zero tolerance for fraudulent or dishonest activity within the organisation. A breach of this policy may result in disciplinary action (including termination of employment or engagement).

If an investigation results in a recommendation to terminate an individual, the recommendation will be reviewed and actioned by the People & Culture function in conjunction with the relevant SLT member.

APPENDIX – The following table includes guidance on areas to be considered in the event of a suspected fraud event

Area	Action	Considerations	Responsibility
Investigation Team	Agree composition on investigation team	• Independence/Objectivity/ • Conflicts of interest • Size and nature of fraud • Required skills sets • Establishment of specific investigation team	Group CFO
Police Notification	Determine requirements to notify law enforcement agencies of events	• State Police • Notification to other regulatory bodies	Group CEO together with Group CFO / Group P&C Director / SLT member
Asset Recovery	Make recommendations to seek to recover missing monies or assets	• Speedy recovery response action more likely to be successful	SLT member
Staff	Make recommendations regarding appropriate remediation/ disciplinary actions	• Employment laws • Suspensions	Group P&C Director
Confidentiality	Remind and enforce confidentiality requirements around fraud investigation activities	• Confidential treatment of response actions is important in the management of potential negative impacts of fraud • Internal and external parties	Investigation Team
Evidence	Implement arrangements to secure evidence	• Potential to seek legal remedy influenced by sufficiency of evidence • Interviews • Telephone records • Data recovery • External parties	Investigation team / Group GC
Insurance	Notify insurers of fraud as required	• Insurance Policies	Group Financial Controller
Stakeholders	Implement appropriate stakeholder interaction procedures	• Staff • Regulators • Board (if relevant)	Investigation Team and Group CFO
Investigation	Define and conduct investigation procedures	• Scope • Procedures • Event facts • Accountabilities • Root causes	Investigation Team
Recommendations	Assess investigation results and propose recommended actions	• Present results to SLT and Board as relevant	Group CFO and relevant SLT member