

## **Fraud and Corruption Prevention Policy**

### **Introduction**

Generator Property Management (GPM), just like all other organisations may be subject to fraudulent or corrupt activity and must therefore implement effective prevention strategies to minimise legal and financial exposure.

### **Purpose**

The purpose of this Policy is to:

1. Ensure that all parties are aware of their responsibilities regarding the identification and prevention of fraudulent or corrupt activity.
2. Ensure that staff, contractors, or community members understand who to report to in the event that they suspect fraudulent or corrupt activity.
3. Provide a step-by-step guide to respond to an allegation regarding fraudulent or corrupt activity.
4. Express a clear statement to staff and contractors forbidding fraudulent or corrupt activity for the benefit of the organisation.

### **Policy**

Generator Property Management will not tolerate fraud or corrupt activity in any aspect of its operations.

Generator Property Management will investigate any suspected acts of fraud, misappropriation, corruption, or other similar irregularity. An objective and impartial investigation, as deemed necessary and as per the procedure below will be conducted regardless of the position, title, length of service or relationship with the organisation of any party who might be the subject of such investigation.

Any fraud or corrupt activity shall constitute grounds for dismissal or termination of contract. Any serious case of fraud, whether suspected or proven, shall be reported to the NSW Independent Commission Against Corruption (ICAC). Further, any suspected criminal activity shall be reported to the NSW Police.

Any person who suspects the commission of a fraud or other corrupt activity related to the operations of Generator Property Management is to follow the procedure outlined in GPM's Public Interest Disclosure (PID) Policy. Any person reporting a fraud or corruption action or a suspected fraud, or corrupt activity shall not be penalised for raising a concern of this nature.

## Fraud and Corruption Risk Management Procedures

### Responsibilities

The **Board** of Generator Property Management has ultimate responsibility for the prevention and detection of fraud and corruption and is responsible for ensuring that appropriate and effective internal control systems are in place within the Company.

The **Chief Executive Officer (CEO)** is responsible for implementing these procedures and investigating instances of fraud or corruption reported to him.

All **staff** must ensure that they:

- Assess the risk of fraud within their area of control;
- Educate staff and contractors about fraud and corruption prevention and detection; and
- Facilitate the reporting of suspected fraudulent or corrupt activities.

Management should be familiar with the types of improprieties that might occur within their area of responsibility and be alert to any indications of such conduct.

All **staff and contractors** share in the responsibility for the prevention and detection of fraud or corruption.

### Fraudulent and Corrupt Actions

Fraudulent actions arise from deliberate or intentional wrongdoing, not negligence or a mistake. It can take many forms and, in all cases, will be dealt with by these procedures. Corrupt activities arise when an individual takes advantage of their work situation to receive improper personal gain. This can take the form of abusing their position of power to make a personal gain or seeking personal benefits in return for providing certain favours to individuals or companies with whom they interact.

For the avoidance of doubt, Generator Property Management, (GPM), will treat the following matters as fraudulent or corrupt behaviour requiring action:

1. Stealing GPM property,
2. Stealing private property while on GPM premises or property,
3. Unauthorised use of GPM assets,
4. Receiving payments or other benefits to encourage use of a supplier or disclose confidential information,
5. Receiving payments or other benefits to reduce obligations of a supplier to deliver goods or services to GPM,
6. Offering or requesting payment or other benefits to achieve outcomes detailed in 4) and 5) above
7. Falsely claiming GPM entitlements,
8. Falsifying employment or pre-employment records, including falsifying or overstating personal qualifications,
9. Falsifying documentation to determine an outcome that would not have arisen based on the facts.

## Reporting

All staff and contractors have the responsibility to report suspected fraud or corruption.

Any staff member, contractor or community member who suspects fraudulent or corrupt activity must immediately notify the Chief Executive Officer, (CEO) (or the Chair of the Board in circumstances where the suspected fraud involves the CEO) about their concern.

### **Step-by-step guide: Responding to suspected fraud and/or corruption**

1. Upon notification an allegation pertaining to fraud or corruption, the CEO (or Chair of the Board) will promptly arrange to carry out an initial review into the allegation.
2. After an initial review and a determination that the suspected fraud or corruption warrants additional investigation, the CEO (or Chair of the Board) shall coordinate the investigation with an appropriate external investigator or law enforcement officer as deemed appropriate. Legal representatives will be involved in the process, if deemed appropriate. The matter being investigated will also be reported to the NSW Independent Commission Against Corruption (ICAC).
3. Once a suspected fraud or corrupt activity is reported, immediate action will be taken to prevent the theft, alteration, or destruction of relevant records. Such actions include, but are not necessarily limited to, removing relevant records / information and placing them in a secure location, limiting access to the location where the records / information currently exists, and preventing the individual suspected of committing the fraud from having access to the records / information, either in paper or electronic form.
4. If an allegation of fraud or corruption is substantiated by the investigation, disciplinary action, up to and including dismissal (or termination of an individual's right to work as a contractor), shall be taken.
5. GPM will also pursue every reasonable effort, including court ordered restitution, to obtain recovery of any losses from the offender.

Where a prima facie case of fraud or corruption has been established, the matter shall be advised to the NSW Independent Commission Against Corruption (ICAC) and the relevant authorities. If an allegation is made in good faith, but it is not substantiated by the investigation, no action will be taken against the complainant.

GPM will make every effort to keep the investigation confidential; however, members of the management team may need to be consulted to assist with a review or investigation.

## Routine Surveillance

GPM will take all steps necessary to deter fraudulent or corrupt behaviour and deter fraudulent or corrupt activities from occurring. This will include undertaking routine surveillance of its transactions and business operations to identify if fraudulent or corrupt activities are occurring.

This surveillance includes the engagement of external expertise to undertake detailed data analytics to identify anomalies and suspicious payments. In addition, an external company is engaged to undertake routine independent audits of commercial arrangements and business processes to ensure they are being conducted in accordance with GPM procedures.

GPM business processes have also been designed to involve clear separation of duties between approval of expenditures and payments of funds. The initial approval of invoices is undertaken by the Manager who oversaw the works/supply and approval of payments involves at least two officers who review the reasons for expenditure and supporting information as well as scrutinising the destination accounts for payments to be made.

The delegation of authority limits an individual's capacity to engage works and results in the necessity to convince either the CEO or the Board of the merits of engaging particular entities, limiting any preferential treatment arising from inappropriate benefits.

GPM requires all staff and Directors to register any conflicts of interest into a register to ensure appropriate separation from decisions.

## Related Documents

Mechanisms pertaining to fraud prevention shall be incorporated into the organisation's accounting and human resources policies and procedures including (but not limited to):

- Code of Ethics
- Delegations of Authority
- Credit Card Procedures
- Annual Audit Plan
- Fraud Control Checklist

## Review

This document will be subject to review every 2 years or as required to meet GPM's business requirements. Internal audits will also be conducted.

### Authorisation:



David Wood

Chief Executive Officer

# Resource one: Fraud control checklist

---

## Attribute 1: Leadership

1. CEO and management staff commitment to fraud control:
  - ☐ CEO visibly endorses fraud control activities, and
  - ☐ Management staff demonstrate their commitment to mitigate fraud risks.
2. Clearly defined the CEO's and management staff's accountability and responsibility:
  - ☐ The CEO assigned responsibility for implementing the fraud control framework
  - ☐ Management staff have a responsibility to ensure GPM has successful fraud control.

## Attribute 2: Ethical framework

3. Clear policies setting out acceptable standards of ethical behaviour:
  - ☐ staff have easy access to all ethical behaviour policies
  - ☐ ethical behaviour policies are included in the induction process.
4. Demonstrated compliance with the ethical framework:
  - ☐ staff annually evidence their commitment to acceptable standards of behaviour.
5. Employees can articulate obligations to ethical behaviour and the organisation's position on fraud:
  - ☐ staff understand fraud is not tolerated and the consequences of committing fraud.

## Attribute 3: Responsibility structures

6. Management and all staff have clearly defined responsibilities for managing fraud:
  - ☐ staff are aware of the responsibility structure in the organisation
  - ☐ responsibilities for fraud control are contained in role descriptions, where appropriate.
7. Fraud management is integrated with core business:
  - ☐ managing fraud risks included in business plans.
8. Resources are allocated to managing fraud.
  - ☐ fraud committee established, and/or a Fraud Prevention Manager appointed.
9. Clearly defined roles for audit and risk committee and auditors:
  - ☐ proactive and influential audit and risk committee
  - ☐ internal audit work covers controls over high risk fraud areas.
10. Staff with responsibility for fraud control and staff in high risk fraud areas are provided with training:
  - ☐ refresher and knowledge update training are provided on an ongoing basis
  - ☐ training program is integrated within a wider education and awareness campaign.



#### **Attribute 4: Fraud control policy**

11. Risk-based policies appropriate to the organisation:

- ☐ appropriate policies address the level and nature of internal and external fraud risks
- ☐ fraud control policy addresses the ten attributes of fraud control.

12. Holistic and integrated:

- ☐ fraud control policy does not operate in isolation and has strong links to other ethical behaviour policies.

13. Regularly reviewed, current and implemented:

- ☐ fraud control policy is responsive to changes in the operating environment and reviewed at least every two years.

#### **Attribute 5: Prevention systems**

14. Proactive and integrated fraud risk assessment:

- ☐ fraud risk assessment is part of organisation's enterprise risk management process
- ☐ risk assessment reviewed after substantial change and at least every two years.

15. Planning follow up and accountability:

- ☐ fraud control plan in place and outcomes reported to senior managers and audit and risk committee.

16. Analysis of and reporting on suspected and actual frauds:

- ☐ fraud database established containing all reports of fraud, action taken and outcomes
- ☐ database kept up to date and published on website.

17. Ethical workforce:

- ☐ pre-employment screening.

18. IT security strategy:

- ☐ specific IT security strategy aligned with the organisation's business strategy
- ☐ cybercrime included as a risk on the risk register.

#### **Attribute 6: Fraud awareness**

19. Comprehensive staff education and awareness program:

- ☐ ongoing ethical behaviour and fraud education and awareness program
- ☐ fraud control message repeated and reinforced using a variety of communication channels
- ☐ fraud control expectations included in the induction process
- ☐ staff have a good understanding of what fraud is
- ☐ guidance material deals with real life situations, conflicts and fraud risks staff face in their work area.

20. Staff awareness of fraud control responsibilities:

- ☐ staff have a good appreciation and understanding of their responsibilities for preventing, detecting and reporting fraud.

21. Customer and community awareness:

- ☐ publicity campaigns developed where appropriate
- ☐ customers and the community encouraged to report suspicions of fraud and provided with easy to use channels to make reports
- ☐ customers and the community have confidence in the integrity of the organisation
- ☐ statement of business ethics setting expectations and mutual obligations.

**Attribute 7: Third party management systems**

22. Targeted training and education for key staff:

- ☐ targeted training and education programs for staff with responsibilities for dealing with third parties.

23. Third party due diligence and clear contractual obligations and accountabilities:

- ☐ structured risk-based due diligence before engaging contractors or third parties
- ☐ contracts and service level agreements include clear accountabilities for managing the risk of fraud
- ☐ position descriptions for staff with responsibilities for managing third parties include accountabilities for managing fraud risks.

24. Effective third party internal controls:

- ☐ specific internal controls relating to third parties in place
- ☐ checks and reviews carried out on dealings with third parties.

25. Third party awareness and reporting:

- ☐ contractors and suppliers understand organisation will not tolerate corruption including fraudulent dealings
- ☐ statement of business ethics setting expectations and mutual obligations
- ☐ reporting mechanisms established for reporting suspected fraud
- ☐ contractors and suppliers encouraged to provide information if they suspect fraud is occurring.

26. Staff disclosure of conflicts of interest and secondary employment:

- ☐ staff regularly required to disclosure conflicts of interest and secondary employment
- ☐ records of conflicts of interest and secondary employment reviewed and kept up-to-date.

**Attribute 8: Notification systems**

27. Culture that supports staff reporting fraud and management acting on those reports:

- ☐ well-publicised options for staff to report fraud
- ☐ staff feel confident they will be protected from reprisal action
- ☐ demonstrated action taken in response to reports of fraud.

28. Policies, systems and procedures that support reporting:

- ☐ reporting system appropriate to organisation
- ☐ different channels available to report fraud
- ☐ feedback and follow-up with internal reporters.

29. Processes to support upward reporting:

- ☐ actual and suspected frauds reported to CEO and audit and risk committee
- ☐ fraud database published on organisation's website.



30. External reporting:

- ☐ staff are clear on policy and procedures for external reporting
- ☐ external reporting in accordance with legislation and policy
- ☐ clear and consistent approach to external reporting.

**Attribute 9: Detection systems**

31. Robust internal controls:

- ☐ well documented risk-based internal controls
- ☐ routine checks of activities, processes controls and transactions
- ☐ range of internal controls that 'prevent, detect and correct'.

32. Monitoring and review:

- ☐ available data monitored and reviewed to ensure irregularities and warning signals are picked up early
- ☐ early warning signs acted on quickly and red flag behaviour recognised.

33. Risk-based internal audit program:

- ☐ internal audit program evaluates the potential for fraud and how fraud risk is managed
- ☐ internal audit recommendations assigned to individuals with timeframes for response.

**Attribute 10: Investigations systems**

34. Clear documented investigation procedures:

- ☐ reports of fraud investigated promptly and to the highest standards
- ☐ investigations are independent
- ☐ sufficient resources allocated, including budget.

35. Investigations conducted by qualified and experienced staff:

- ☐ investigations conducted by appropriately qualified personnel with recognised qualifications and appropriate experience.

36. Decision-making protocols:

- ☐ documented decision-making processes
- ☐ proportionate responses to incidents of fraud.

37. Disciplinary systems:

- ☐ staff understand fraud will not be tolerated and the perpetrators will face disciplinary action
- ☐ commitment to taking action against the perpetrators of fraud
- ☐ consistent application of sanctions.

38. Insurance:

- ☐ consider a fidelity guarantee insurance policy to protect against the financial consequences of fraud.