Anti-Fraud, Bribery and Corruption Policy

Group Corporate

Review: Annually (next due March 2025, unless required earlier)
Document Owner: Chief Risk Officer (CRO)
Classification: General Use

Approved by:

- Praemium Limited (PPS) 20 March 2024
- Praemium Australia Limited (PAL) 25 March 2024
- Powerwrap Limited (PWL) 25 March 2024
- MWH Capital Pty Ltd (MWH) 25 March 2024

Contents

1 Background

Praemium Limited (ASX:PPS) and each of its incorporated subsidiaries (**Praemium**) has a zero-tolerance stance towards fraud, bribery and corruption. Acts (or threats) of internal and external fraud, bribery and corruption can affect our reputation, our relationship with our clients and stakeholders and our revenue sources.

This Anti-Fraud, Bribery and Corruption Policy (**this Policy**) gives effect to Praemium's commitment to proactively minimise the occurrence of fraud, bribery, and corruption.

2 Purpose

The purpose of this Policy is to protect against, detect and respond to instances of fraud, bribery and corruption in order to protect the interests of clients, employees, shareholders and other stakeholders.

This Policy is based on the guidelines and principles of Australian Standard 8001-2008: Fraud and Corruption Control (**AS8001-20021**) and is consistent with the Praemium's Corporate Code of Conduct. This Policy is also an integral part of Praemium's Risk Management Framework, which includes Praemium's Risk Appetite Statement and other associated risk and compliance policies.

3 Scope

This Policy applies to all directors, managers and employees including contractors of Praemium (hereafter referred to as "employees" unless otherwise indicated).

All employees are expected to ensure that they understand the key principles, assignment of roles, methodology and responsibilities contained in this Policy.

4 Training

The Risk & Governance Team will ensure that training on this Policy is conducted for all staff at induction and on an ongoing basis.

5 Non-compliance

Any non-compliance with and breach of this Policy will be taken seriously, and all matters will be investigated. In assessing non-compliance, each matter will be considered on a case-by-case basis according to its merits. Considerations may include level of non-compliance, reasons for non-compliance (e.g., training), frequency and any other circumstances (e.g., other breaches of a reporting entities or professional standards).

Failure to comply with this Policy may lead to criminal, civil or regulatory liability.

6 Roles and Responsibilities

Roles	Responsibilities
Board	• Review and Approve the Policy. • Assess fraud, bribery and corruption risks and issues in accordance with the Policy
Audit Risk and Compliance Committee (**ARCC**)	• Monitor compliance with the Policy and report risks and issues to the Board as applicable • Review and provide feedback on the Policy to R&R • Recommend the Policy to the Board for approval

Chief Risk Officer (CGRO)	• Responsible for the overview and maintenance of the Fraud, Anti-Bribery and Corruption Management Program, including planning, resourcing and monitoring the effectiveness of prevention controls and detection measures and management of the investigation and the organisational response.
Risk and Compliance (R&C)	• Provide regular training to Employees. • Recommend the Policy to the CRGO to take to the Board • Conduct periodic assessments of Praemium's fraud and corruption risks. • Escalate and monitor fraud, bribery and corruption events in accordance with this Policy, including coordinating internal and external reporting. • Conducting, coordinating, and monitoring investigations into allegations of fraud, bribery and corruption.
People and Culture (P&C)	• Manage any disciplinary action associated with breaches of the Policy and taking appropriate disciplinary management actions, as required.
Information Technology	• Manage an Information Security Management System to mitigate the risks of fraud, bribery and corruption
Managers and People Leaders	• Ensure compliance with Our Ways of Working and other organisational policies and procedures in their area of responsibility. • Ensure awareness and understanding of fraud, bribery and corruption issues in their area of responsibility. • Monitor for non-compliance and fraud warning signs. • Report suspicious behaviour. • Implement remedial actions.
Employees	• Comply with Our Ways of Working and other organisational policies and procedures. • Be aware of responsibilities under this Policy in mitigating risks of fraud, bribery and corruption. • Report suspected fraud, bribery or corruption as per the requirements in this Policy.

7 Definitions

Term	Definition
Bribery	The offering, promising, giving, accepting or soliciting of an advantage as an inducement for action which is illegal, unethical or a breach of trust.
Corruption	Dishonestly obtaining a personal benefit by misuse of power, position, authority or resources, including: - Paying or receiving secret commissions (bribes) - Giving out confidential information in exchange or a benefit or advantage - Collusive tendering - Serious conflict of interest involving a Director or Senior Executive - Serious nepotism and cronyism, especially in recruitment and promotion - Manipulating the procurement process to favour one tenderer - Providing gifts or entertainment to achieve a commercial outcome which breaches the Conflicts of Interest Policy
Fraud	Dishonest activity to obtain or arrange a benefit by deception or other means, including: • Theft of plant, equipment or inventory by employees • False invoicing or exaggerating the value of goods delivered or services provided • Thefts of funds or cash • Accounts received fraud (misappropriate or misdirecting payments received from a debtor) • Unauthorised use of credit card • Running a private business during work time • Forged qualifications

- Theft of intellectual property or other confidential information
- Insider Trading (as defined in the Trading Policy)
- Misuse of position by managers or directors gain financial advantage
- Financial reporting fraud
- Tax evasion
- Money laundering

8 Related Policies

This Policy should also be read in conjunction with the following Company policies:

- Trading Policy
- Conflicts of Interest policy
- Our Ways of Working
- AML/CTF Program
- Whistleblower Policy
- Outsourcing Policy
- Information Security Policy

9 Anti-Fraud, Bribery & Corruption Program

Praemium's Anti-Fraud, Bribery and Corruption Program follows *AS8001-2008*, and consists of the following measures against internal and external fraud:

»Planning and Resourcing
- Awareness
- »Prevention
- »Detection
- Reporting
- Investigation
- »Response

10 Planning and Resourcing

Proper planning and coordinated resourcing are key elements of an anti-fraud, bribery and corruption program.

This is overseen by the Risk and Governance Team and involves the following elements:

- Risk identification and establishment of control measures.
- Allocation of responsibility for implementation and maintenance of the control measures.
- Allocation of adequate resources.
- Review and monitoring of effectiveness of control measures; and
- Framework for incident, reporting and response.

11 Awareness

Awareness is raised across the business to ensure employees at all levels are aware of fraud, bribery and corruption exposures and how to respond to them.

Praemium's awareness program includes:

- Making this Policy available to all employees.
- Ensuring employees are aware of the indicators of fraud, bribery and corruption
- Ensuring employees are aware of how allegations or concerns regarding fraud, bribery, corruption or unethical conduct can be reported, including protection for whistleblowers
- A clear outline of what is expected of management and employees if fraud, bribery or corruption is detected or suspected
- Regular training for all employees at both induction and on an ongoing basis.

12 Prevention

Praemium has in place a range of initiatives to proactively prevent instances of internal and external fraud, bribery and corruption. These include:

12.1 Integrity Framework: Our Ways of Working, Praemium's Code of Conduct, provides an ethical foundation for employees to follow. All employees are given training on Our Ways of Working at induction and on an ongoing basis.

12.2. Managing Conflicts of Interest: The Conflicts of Interest Policy includes procedures to ensure decisions are made in Praemium's best interest and to avoid actual or perceived allegations of bribery, including managing risks connected to gifts, hospitality, donations and similar benefits.

12.3. Internal Controls and Internal Control Environment: Praemium has an internal control system that includes fraud, bribery and corruption risks.

12.4. Managing Performance-Based Targets. Ensuring performance measures include not only financial-based targets but also ethical conduct.

12.5. Workforce Screening. Potential employees are appropriately screened before being offered employment with Praemium. The Recruitment and Selection Policy outlines procedures undertaken to select the best person for the job.

12.6. Training. Regular training is provided on this Policy to employees.

12.7.Whistleblower Policy. Procedures are in place to ensure wrongdoings can be disclosed with protection.

12.8 AML/CTF Program. Provides guidance on how Praemium complies with anti-money laundering and counter terrorism financing obligations.

12.9. Trading Policy. Employees are subject to rules relating to the trading of Praemium securities to prevent the misuse of price sensitive and inside information.

12.10. Outsourcing Policy: Provides guidance on how to select and manage business activities outsourced to external service providers.

12.11. Payment Procedures. Operations employees follow procedures to prevent internal or external fraudulent attempts to misappropriate funds.

12.12 Maintenance of Business Records. The Document Retention Policy helps to prevent, detect and respond to any fraud, bribery or corruption exposures and events.

12.13 Information Security Management System. Praemium has implemented an information security management system to help prevent technology-enabled fraud and corruption risks, including physical security and asset management.

12.14 Platform Administration Checklists. Monitoring of activity on client and staff accounts through checklists and process guides, particularly for large and/or unusual transactions

12.15. External Screening: Praemium may be exposed to fraud, bribery and corruption risks through its external environment and undertakes regular external environment scans of the political, economic, social, technological, legal and environmental environments within which Praemium operates.

13 Detection

13.1 While the key to a successful anti-fraud, bribery and corruption control program is to take proactive steps to prevent it occurring, if our prevention systems fail, it is critical that it is detected as soon as possible to minimise the impact on the organisation.

13.2 The following detective methods are employed across the business:

- internal accounting reviews which analyse compliance and detect anomalies
- incident and breach handling processes are followed used the Incident & Breach Handling Policy
- use of external auditor to review processes, compliance and detect anomalies

- monitoring of activity on client and staff accounts through checklists and process guides, particularly for large and/or unusual transactions
- reviewing interactions with advisers and direct clients
- verification process when onboarding a new adviser to the platform all employees to be alert to suspicious activities
- all employees are obliged to report suspected or actual incidents of fraud, bribery, or corruption.

13.3 Warning signs of possible internal fraud

Managers and staff should be alert to the common procedural warning signs of fraud:

- Unauthorised changes to systems or work practices.
- Missing documentation relating to client or organisational financial transactions.
- The same employee performing an excessive number of duties e.g., both processing and approving the same transaction.
- "Blind approval", where the person signing does not sight supporting documentation.
- Duplicates of invoices.
- Refusal of employee to take leave or to take leave rarely
- Altered behaviour of employee
- Unusual leave taking
- Alterations to documents such as logbooks and time sheets.
- Senior staff involved in routine process work such as purchasing, ordering and receiving of goods.
- Potential conflicts of interest not declared.
- Undue secrecy, or excluding people from available information; and
- Failure to conduct reference checks on staff prior to appointment.

13.4 Warnings signs of possible external fraud

- Unusual transaction patterns on client accounts, such an unusual surge in transactions within a short time frame or irregularities in the size and frequency of transactions
- Sudden changes in account activity
- Failed Know Your Customer (KYC) or any other screening checks
- When the client ID does not match the certified ID on file
- Unusual emails from direct clients, including if the email is different to the registered email on file

14 Reporting process

14.1 Internal Reporting

If an employee suspects that instances of either internal or external fraud are occurring or have occurred, they must report the allegation to:

- Their immediate manager;or
- The Chief Risk Officer, or if the Chief Risk and Governance Officer is suspected of fraud, bribery or corruption, then;
- Company Secretary or a Director of the Board

Any disclosure made in accordance with the Whistleblower Policy will be protected under the law.

If an Employee or external party suspects a fraudulent or corrupt activity or any other Improper Conduct is taking place which involves Praemium, its Employees, Third Parties or Partners, that person or company is encouraged to raise their concerns in accordance with the Whistleblowing Policy

14.2 External Reporting

Where required, such as where there are regulatory or contractual requirements, the event must be reported to third parties e.g. ASIC, ASX etc. Where appropriate, the police may also be notified.

15 Investigation process

The following steps are to be taken following an allegation of fraud, bribery or corruption:

Step 1 - Investigation of the allegation, overseen by the Chief Risk Officer, to be undertaken by an impartial and competent third party, either internal or external to the organisation. The investigation should:

- Identify as quickly as possible all parties involved and whether any funds have been removed or appropriated fraudulently
- Capture and collate evidence, including interviewing of relevant witnesses, enquiries with internal and external parties, examination of documents, tracing funds, assets and/or goods
- Risk assess the impact upon the business
- Document all action taken including how the event was identified and the considerations, actions and assessments made.
- Produce a report outlining the findings and recommended actions
- Be conducted in confidence and on a "need to know" basis.
- Allow for the suspect to be given an opportunity to respond to the allegation.

Step 2 – Where appropriate disciplinary action, including dismissal, can be taken against an employee, where fraud, bribery or corruption is established.

Step 3 – Procedures will be reviewed, and remedial action taken if required, to remove or reduce the risk of the fraud, bribery or corruption recurring. This includes assessing internal controls, systems and processes to minimise the likelihood of the event reoccurring.

Step 4 – Where appropriate, legal action will be taken to recover the losses caused by the fraud, bribery or corruption.

Step 5 – The Board and/or relevant Compliance Committees will be informed of any material incidents of fraud, bribery or corruption.

Step 6 – A Fraud and Corruption event register will be kept, outlining the details in relation to every reportable fraud and corruption event, including:

- Date and time of report
- Date and time event was detected
- How the event was reported
- The nature of the event
- Value of loss to Praemium
- Any action taken following the discovery of the event

.