Anti-Fraud, Bribery and Corruption Policy

Group Corporate

Review:	Bi-Annually (next due March 2027, unless required earlier)
Document Owner:	Chief Risk and Corporate Operations Officer (CRCOO)
Classification:	General Use
Approved:	

Praemium Limited (PPS)	April 2025
Powerwrap Limited AFSL 329829 (PWL)	May 2025
MWH Capital Pty Ltd AFSL 338141 (MWH)	May 2025
Praemium Australia Limited AFSL 297956 (PAL)	May 2025
OneVue Wealth Services Ltd AFSL 308868 (OVWS)	May 2025
Investment Gateway Pty Ltd AFSL 239117 (IG)	May 2025
OneVue Wealth Assets Pty Ltd (OVWA)	May 2025

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 8001-2021: Fraud and Corruption Control* 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 and third parties acting for or on behalf of Praemium (hereafter referred to as "employees" unless otherwise indicated).

All employees must be aware and are responsible for understanding the key principles, assignment of roles, methodology and responsibilities contained in this Policy.

4. Training

The People & Culture 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 be considered a serious matter and may result in disciplinary action against the individual involved.

Failure to comply with Bribery and Corruption laws may lead to criminal, civil or regulatory liability.

6. Related Policies

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

» Conflicts of Interest policy
» Our Ways of Working
» Whistleblower Policy
» Trading Policy
» Designated Employee Trading Policy
» Delegation of Authority Policy
» Supplier and Outsourcing Policy
» AML/CTF Program
» Information Security Policy

7. Roles and Responsibilities

Roles	Responsibilities
Board	» Review and approve this Policy. » Assess fraud, bribery and corruption risks and issues in accordance with this Policy
Audit Risk and Compliance Committee (**ARCC**)	» Monitor compliance with this Policy and report risks and issues to the Board as applicable. » Review and provide feedback on this Policy. » Recommend this Policy to the Board for approval. » Independent supervision of internal investigations
Chief Risk and Corporate Operations Officer (**CRCOO**)	» Responsible for the overview and maintenance of the Fraud, Anti-Bribery and Corruption Management Program » Provide oversight of fraud and corruption risk.
Risk and Compliance (**R&C**)	» Recommend this Policy to the ARCC for Board approval. » Conduct periodic assessments of Praemium's fraud and corruption risks. » Escalate and monitor compliance with this Policy, including coordinating internal and external reporting. » Conducting internal investigations and coordinating external investigations, as well as monitoring all investigations into allegations of fraud, bribery and corruption.
People and Culture (**P&C**)	» Organise training on this Policy for all staff at induction and on an ongoing basis. » Manage any disciplinary action associated with breaches of this Policy and taking proper disciplinary management actions, as required.
Managers and People Leaders	» Ensure compliance with *Our Ways of Working*, Praemium's Code of Conduct 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	» Be aware of responsibilities under this Policy in mitigating risks of fraud, bribery and corruption. » Comply with *Our Ways of Working* and other organisational policies and procedures. » Report suspected fraud, bribery or corruption as per the requirements in this Policy.

8. 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. » Offering gifts, payments, or favours to influence a business decision. » Accepting bribes to award contracts or expedite processes.
Corruption	Dishonestly obtaining a personal benefit by misuse of power, position, authority or resources, including bribery, secret commissions, conflicts of interest, or manipulating processes for unfair advantage.

Term	Definition
	» Paying or receiving secret commissions (bribes) » Giving out confidential information in exchange for a benefit or advantage » Collusive tendering » Serious nepotism and cronyism, especially in recruitment and promotion » Manipulating the procurement process to favour one tenderer
Fraud	Any deliberate act of deception to gain an unlawful or unfair advantage, including theft, false representation, misuse of funds, or manipulation of financial or non-financial information. » False invoicing or exaggerating the value of goods delivered or services provided. » Misappropriating company funds or assets » Engaging in Insider Trading (as defined in the *Trading Policy*) or financial reporting fraud.
Public Official	Any individual holding a government position, working in public administration, or employed by a state-owned enterprise, including politicians, judges, military personnel, and employees of international organisations.
Facilitation Payments	A small, unofficial payment made to a public official to hasten or secure a routine government action (e.g., processing a visa or licence). It does not involve decisions about new or existing business.
Secret commission	A bribe or kickback given to an agent or representative to influence a business decision without the knowledge or consent of their principal.
Supplier/Third Party	Any individual or organisation providing goods, services, or advice to the company, including consultants, contractors, vendors, agents, and joint venture partners.
Political Donations	A gift, payment, or service provided to a political party, candidate, or official, which could create the perception of favouritism. It excludes lawful fees, taxes, or contributions.

9. Prohibited Conduct

This Policy strictly prohibits the following types of improper payments and conduct:

- Bribery: Bribing a Public Official or any individual or entity in the public or private sector.
- Facilitation Payments: Making payments to hasten or secure routine government actions.
- Secret Commissions: Offering, making, asking for, or receiving undisclosed payments or kickbacks.
- Gifts and Entertainment: Providing or accepting gifts, hospitality, or entertainment that violates Praemium's *Conflict of Interest Policy*.
- Money Laundering: Engaging in or facilitating activities that disguise the origins of illegally obtained funds.
- Encouraging Improper Conduct: Authorising, encouraging, or facilitating bribery or related misconduct by others, such as suppliers or third parties.
- False Records: Maintaining false, misleading, incomplete, or inadequate accounting records or books.

10. Policy Requirements

All employees and representatives must:

- Conduct Due Diligence: Perform appropriate due diligence on third parties before engagement.
- Communication Standards: Ensure third parties are aware of and comply with the standards set out in this Policy and incorporate these requirements into contracts as approved by Risk and Compliance and external legal consultant.
- Maintain Accurate Records: Keep transparent and accurate books and records, ensuring all expenditures are properly documented.
- Report Violations: Immediately report any suspected or actual breaches of this Policy to your manager or CRCOO.

. Anti-Fraud, Bribery & Corruption Program

Praemium's Anti-Fraud, Bribery and Corruption Program follows *AS 8001:2021, Fraud and Corruption Control* and consists of the following measures against internal and external fraud:

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

11. 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 Compliance Team and involves the following elements:

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

12. Awareness and Prevention

Praemium promotes a culture of integrity and ethical behaviour through strong governance and leadership. 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. The Managers and People Leaders of each Business Unit is responsible for ensuring awareness throughout the Business Unit of the requirements of this Policy.

12.1 Training and awareness programs for employees includes:

- Making this Policy available to all employees.
- Ensuring employees are aware of the indicators of fraud, bribery and corruption.
- Inform employees about the available reporting channels and grievance mechanisms, including protections for whistleblowers.
- Clearly outline the responsibilities of both management and employees when fraud, bribery, or corruption is detected or suspected.
- Emphasize the implications of non-compliance or failure to adhere to the Policy, including potential disciplinary actions and consequences.
- Regular training for all employees at both induction and on an ongoing basis.

Praemium has in place a range of policies and procedures frameworks to proactively prevent instances of internal and external fraud, bribery and corruption. These frameworks are supported by comprehensive training and communication programs that ensure employees are aware of their responsibilities and the mechanisms in place to report and address potential issues.

12.2 Integrity Framework

- *Code of Conduct (Our Ways of Working)* provides an ethical foundation for employees to follow.
- Career and employment Standards and Guidelines are provided in relation to Travel, Corporate Credit cards, Staff Account and Personal Expense Reimbursement.
- *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, political donations and similar benefits.
- *Trading Policy & Designated Employee Trading Policy*: employees are subject to rules relating to the trading of Praemium securities to prevent the misuse of price sensitive and inside information.
- *Workforce Screening:* Prospective employees are appropriately screened before being offered employment with Praemium.
- *Recruitment and Selection Policy* outlines procedures undertaken to select the best person for the job.

12.3 Compliance Framework

» *AML/CTF Program:* Provides guidance on how Praemium complies with anti-money laundering and counter terrorism financing obligations.
» *Document Retention Policy:* keeping transparent and accurate books and records helps to prevent, detect and respond to any fraud, bribery or corruption exposures and events.

12.4 Risk Management Framework

» *Internal Control Framework* that includes fraud, bribery and corruption risks.
» *Supplier and Outsourcing Policy:* Guidance on how to select and manage business activities outsourced to external service providers.
» *Payment Procedure:* Operations employees follow procedures to prevent internal or external fraudulent attempts to misappropriate funds.
» *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.
» *Information Security Policy:* Praemium has implemented an information security management system to help prevent technology-enabled fraud and corruption risks, including physical security and asset management.

13. Detection

While the key to a successful anti-fraud, bribery and corruption control program is to take 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.

13.1 Detective Methods

The following detective methods are employed across the business:
» Internal accounting reviews to ensure compliance and identify anomalies.
» Use of internal and external auditors to review processes, compliance and detect anomalies.
» Monitoring of activity on client and staff accounts, particularly for large and/or unusual transactions.
» Reviewing interactions with advisers and direct clients to identify red flags.
» Verification process for onboarding new advisers.
» All employees must report suspected or actual fraud, bribery, or corruption incidents as per *the Incident and Breach Handling Policy* and *Whistleblower Policy*.

13.2 Warning signs of possible internal fraud

Managers and staff should be alert to the common procedural warning signs of internal fraud:
» Unauthorised changes to systems, process or documentation.
» Missing records relating to client or organisational financial transactions.
» The same employee performing conflicting roles (e.g., both processing and approving the same transaction).
» "Blind approval", approvals made without sighting supporting documentation.
» Repeated or duplicate invoices.
» Leave Patterns, employee refusing to take leave or to take leave unusually.
» Sudden or unexplained changes in employee behaviour.
» Potential conflicts of interest not declared, and
» Bypass employment checks before appointing a prospective employee to commence work.

13.3 Warnings signs of possible external fraud

» Unusual patterns on client accounts, such as sudden surge in transactions or irregular transaction sizes
» Sudden changes in account activity, such as dormant user becomes active after a long time.
» 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

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 CRCOO, or if the CRCOO is implicated, then
» Company Secretary or Director of the Board

Employees and third parties can also submit anonymous reports through Praemium's Whistleblowing Hotline, which is managed by an external and independent provider in accordance with the *Whistleblowing Policy*.

14.2 External Reporting

Where required by regulatory or contractual obligations, the CRCOO will decide the appropriate external bodies for reporting, such as ASIC, ASX or others. Where appropriate, the police may also be notified.

15. Response and Investigation

The Risk and Compliance Team is responsible for conducting, coordinating, and monitoring investigations into allegations of fraud, bribery, and corruption. The outcome of such investigations shall be reported to the ARCC.

All employees must fully cooperate with both internal investigations and external investigations conducted by regulators, law enforcement, or other authorised bodies.

» This includes promptly providing accurate information, documents, or any other assistance requested during such investigations.
» Employees must also immediately report any contact from external investigators to the Risk and Compliance Team for guidance and support.
» Failure to cooperate, or any attempt to obstruct or mislead investigators, will be treated as a serious breach of this Policy and may result in disciplinary action, including termination of employment.