Anti-Bribery, Fraud & Corruption Policy

Why we have this policy

At Australian Unity we are committed to complying with the laws and regulations that govern our business and have a zero-tolerance approach to bribery, fraud and corruption. Bribery, fraud and corruption are serious criminal offences and are inconsistent with our values. It is important that all employees actively protect our reputation and conduct business with honesty and integrity.

This policy sets out our collective responsibility to comply with the laws that prohibit bribery, fraud and corruption.

Who it applies to

This policy applies to all employees (including directors, officers, contractors and consultants).

Policy detail

Bribery, fraud, and corruption are forms of improper conduct. Some common forms of corruption are outlined below:

Bribery

- Bribery is the act of offering, promising, giving or accepting a benefit with the intention of influencing a person to do or not do something as they perform their role or function, so that we receive business or an advantage that is not legitimately due.
- It generally includes the offer or acceptance of cash, gifts, political or charitable contributions or employment opportunities).

Fraud

- Fraud is where an individual or organisation is deceived to dishonestly obtain property or get a financial advantage or cause any financial disadvantage. Examples include falsified financial reporting, manipulation of accounts to obtain customer funds or improper alteration of documents.

Corruption

- Corruption is dishonest conduct by someone in a position of power to benefit themselves at the expense of others. Examples include demanding or taking money in exchange for favours ('kick backs'), granting or awarding contracts to associates, collusion, price fixing, using insider information, and facilitating criminal enterprises such as drug trafficking or money laundering.

Facilitation Payments and Secret Commissions

- The provision of facilitation payments and secret commissions is strictly prohibited and is considered a form of bribery.
- Facilitation payments are typically minor, unofficial payments made to secure or speed up a routine government action. Examples include processing work permits or planning permissions.
- Secret commissions are typically where someone offers or gives a commission to an agent or representative of another person that is not disclosed to the person they are

acting for. The payment is usually made to get the agent or representative influence the person's decision.

Acceptance of Inducements

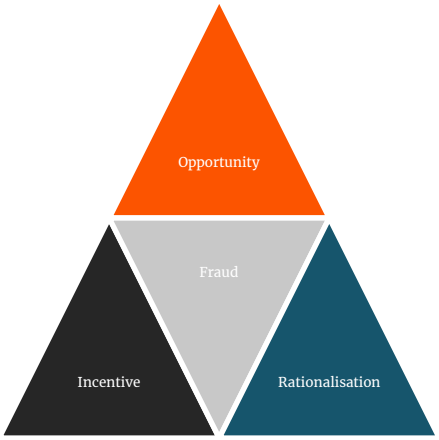
- In accordance with our *Conflict of Interest Policy*, any offer of a gift or entertainment that could lead to an actual or perceived conflict of interest must not be accepted. It is important that there can be no reasonable perception that the gift or hospitality could be s intended to influence decision making or the business relationship in an improper and unprofessional way.
- Paid travel to attend events should not be accepted. If the event is worth attending, it should generally be funded by Australian Unity. There may be an exception granted by the Group or Platform Conflict Officer where travel is paid for by a vendor as part of contractual obligations to perform due diligence activities.
- Gifts, entertainment or hospitality must not be offered to, or accepted from, public or government officials or their associates, including politicians or political parties, except in certain circumstances and with the required approval as outlined in the Political communication and donations section below.

Political Communications and Donations

- All dealings with politicians and government officers relating to our business activities must be conducted at arm's length and with the utmost professionalism to ensure that there is no attempt to gain a business advantage.
- All political communications and donations must be authorised by the Public Affairs and Communication (PAC) team (within Group Managing Director's office). Refer to the Political Contact, Communications and Donations Policy for more information.

Identification and ongoing management

Risk of a person's decision to commit bribery, fraud or corruption is often linked to these components, which are often referred to as the fraud triangle. The Fraud Triangle identifies drivers and potential causes and assists us in being alert to potential weaknesses.



Opportunity: means the circumstances that allow the improper conduct to occur. In the fraud triangle, it is the only component that a company exercises complete control over. Examples that provide opportunity for committing fraud include – weak controls (e.g. no segregation of duties, poor documentation, no supervision), no tone from the top, poor or absent accounting records.

Incentive: refers to an employee's mindset towards committing fraud. Things that can contribute to an employee's mindset for committing fraud include, bonuses linked to a financial metric, investor expectations and personal financial needs such as cost of living or funding addictions.

Rationalisation: refers to an individual's justification for committing fraud. Examples of common rationalisation include an employee feeling justification as they believe they have been mistreated by an employer, they see management doing the same action and they feel they have no other choice.

As part of the *Enterprise Risk Management Framework*, we consider our exposure to bribery, fraud and corruption across our operations and prioritise and address the risks faced.

To maintain effective management of improper conduct, we are committed to ensuring appropriate plans, arrangements and controls are in place that address the following key elements:

- Clear policies: We make it clear via this policy and our Code of Conduct that any action that amounts to bribery, fraud and corruption is forbidden. Code of Conduct training is provided annually and id mandatory.
- Preventative Controls: Senior management are responsible for implementing and overseeing controls to prevent bribery, fraud and corruption. These controls include segregation of duties; system-based controls; training and awareness; employee screening; supplier and customer vetting, peer review / authorisation and data analytics.
- Detective Controls: External audit engagements; Internal Audit reviews and data analytics; avenues for reporting suspected incidents (for example, to Group Audit) and a Whistleblower protection program.
- Response: Investigation; internal reporting and escalation; disciplinary procedures; external reporting; civil action for recovery of losses; review of internal controls; and insurance.

Employee Training

The requirement of employees to avoid any activity that may constitute fraud, bribery and corruption and references to the Anti-bribery Fraud and Corruption Policy is included in our Code of Conduct training. New employees complete training on the Code of Conduct when they join, and all employees will complete the training annually.

Each business unit must ensure that staff who have primary responsibility for the prevention and detection of bribery, fraud and corruption are appropriately trained. Group Risk and Compliance will provide assistance to business areas in the design, implementation and regular review of appropriately targeted fraud awareness training programs.

Record Keeping

Record keeping must allow for quick responses to regulator requests for information or audit investigations.

Records to be retained in line with *Records Retention Policy* include, but are not limited to:

- All records relating to dealings with third parties and any expenditure by our employees (including payments for gifts, entertainment and hospitality), must be maintained with accuracy and completeness and must not facilitate or conceal improper payments.
- Employee training material and training completion records
- Reported conflicts of interests and gift register (please refer to the Conflicts of Interests Policy and Procedure for further information on how transactions which may result in an actual or perceived conflict are to be recorded).

Reporting breaches and suspicious behaviour

We encourage openness and transparency and will provide support to those who raise genuine concerns under this policy.

If you become suspicious that someone may be involved in fraud, bribery or corruption, you must report it. This includes behaviour that makes our employees and others feel threatened or under pressure to engage in improper conduct.

Reports of bribery, fraud or corruption should be reported under the *Whistleblower Policy* so that:

a) a full internal investigation can be carried out to substantiate the allegations and determine actions required to remediate the matter (including reporting any relevant matters to law enforcement agencies).

b) individuals who have engaged in improper conduct are identified and dealt with appropriately, and

c) no one suffers detrimental treatment due to making a protected disclosure which includes suspected fraud, bribery or corruption.

Roles and responsibilities

- Group Executives have primary responsibility for the prevention, detection and identification of bribery, fraud and corruption within their business areas. Managers are responsible for raising awareness of the risks relating to bribery, fraud and corruption with their staff, what to do if you suspect an incident has occurred, and for ensuring compliance with Group policies and procedures.
- Employees are responsible for complying with policies and procedures, in particular the Code of Conduct and ethics, avoidance of conflict of interest, avoiding the receipt of secret commissions or inappropriate benefits and maintaining vigilance in early detection, reporting and prevention of fraud and corruption.
- All employees must report any suspicions of fraud, bribery, or corruption. The Whistleblower policy has details on how to make a disclosure and the protections that apply.
- People and Culture must ensure adequate procedures are in place that address:
  a) required background screening and reference checks are performed
  b) disciplinary procedures are enforced
  c) employment contracts include relevant conditions of employment relating to improper conduct, and
  d) the formulation and enforcement of the annual leave policy requirements in respect of leave.
- Group Audit is responsible for conducting data analytics to detect potential fraud, investigating and reporting on bribery, fraud and corruption incidents and advising Group Risk and Compliance on improvements to fraud and corruption prevention practices (if applicable).
- Finance and accounting employees must ensure all financial records relating to payments are true and accurate and appropriate fraud controls are in place and adhered to.
- Employees who handle Whistleblower disclosures must handle the investigation in line with *Whistleblower Policy and Procedure* (refer to the *Whistleblower Policy and Procedure* for details).

- If you deal with third parties (including agents, intermediaries, distributors, suppliers, purchasers or contractors) you must undertake due diligence checks prior to engaging with a third party, particularly where the engagement may expose us to potential bribery and corruption. Refer to *Group Procurement and Vendor Management Policy* for details.
- Management must consider exposure to bribery, fraud, and corruption across operations and manage the risks in accordance to the Enterprise Risk Management Framework for further details. Refer to Risk & compliance teams for assistance.

Policy non-compliance

All instances of policy non-compliance must be reported in line with the Incident Management Policy. There may be consequence management for non-compliance with this policy.

Non-compliance with this policy may also be a non-compliance of the Code of Conduct.

Policy exemptions

Any requests for an exemption to this policy must be submitted for approval to the Policy Administrator who will refer them to the Policy Owner.

Legal obligations

If you believe you have a legal obligation that is inconsistent with this policy, you should immediately report the inconsistency to your risk and compliance manager and as a general rule should comply with the higher standard.

Where to get help

Please contact your platform risk and compliance manager or the Head of Risk and Compliance, Group Risk & Compliance if you have any queries or need assistance.

Appendix A

Bribery, Fraud and Corruption Potential Scenarios List

Note: this list is a guide only and is not exhaustive

Risk	Scenario
Fraudulent funds transfer/account requests	Transacting on or stealing from customer/corporate accounts
Commissions fraud	False agent/broker set up to claim commission
Theft of assets	Theft of physical assets, customer & business records, IP
Sales/marketing incentive fraud	Falsified sales records to inflate incentives or achieve performance metrics
False reporting (internal)	Inaccurate management reporting to either hide issues or falsely record achievement of performance metrics
IT programming fraud	Manipulating/changing system code for personal gain (e.g. truncating interest calculations and diverting fractions to own account)
Corporate expense fraud	Inappropriate use of corporate credit cards
Inappropriate system access/use	Inappropriate access to or use of company systems (e.g. copying customer data, online gambling, running own business on company resources)
Insider trading	Trading in Group products (including Lifeplan products) by staff with inside knowledge
Anti Money Laundering	False accounts, fake ID documents, Group products being used to launder money or as conduit to finance terrorism
Other external fraud	Phishing, hacking of customer or business data

Policy Administration

Policy Name	Anti-Bribery Fraud & Corruption Policy
Policy Level	Level 1 – Group Policy
Approval Body	Group Executive – Governance
Date of Approval	30 May 2023
Policy Owner	Group Executive – Governance
Policy Administrator	General Manager, Group Risk and Compliance
Related policies	Code of Conduct Conflict of Interest Policy Whistleblower Protection Policy Incident Management Policy Securities Trading Policy Political Contact, Communications and Donations Policy Vendor Management Policy
Supporting procedures or guidelines	Conflict of Interest Procedure Platform Conflict Management Plans Whistleblower Procedure Incident Management Procedure Securities Trading Procedures
Date of last review	25 May 2021
Regulator (if applicable)	Australian Prudential Regulatory Authority (APRA) Australian Securities and Investments Commission (ASIC) Australian Aged Care Quality and Safety Commission (AACQSC) Department of Health Department of Human Services
Compliance mechanism	Compliance with this policy is monitored using: • Annual Code of Conduct Declaration • Risk and Control Assessments under the Enterprise Risk Management Policy • Internal Audit Reviews
Classification	Internal