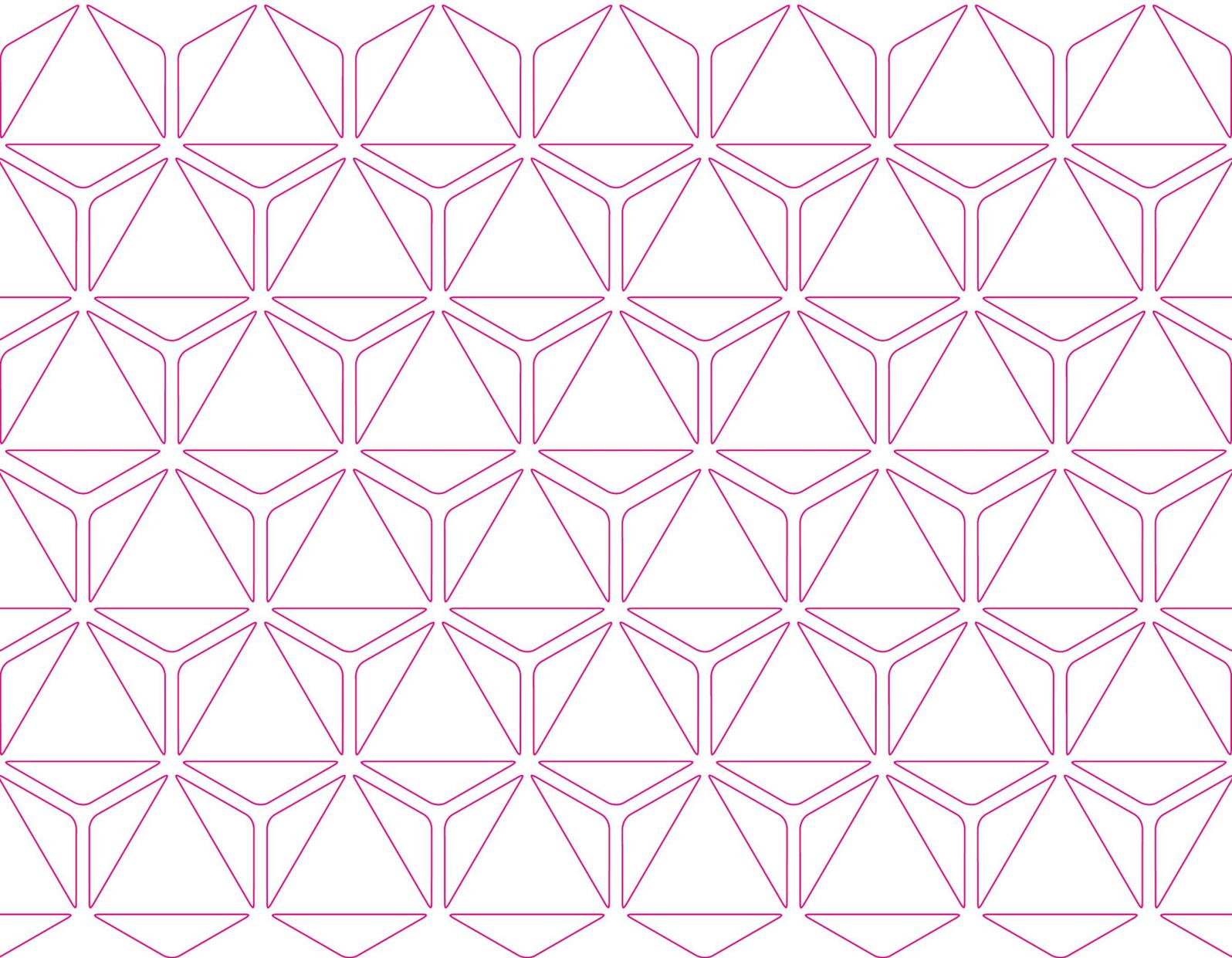


Whistleblower Policy



Group Corporate



Contents

| | |
|----------------------------|----------|
| About this document | 3 |
| Background | 3 |
| Purpose | 3 |
| Adjunct Policies | 3 |
| Non-compliance | 3 |

| | |
|--|----------|
| Policy Content | 4 |
| Who this Policy applies to: | 4 |
| Matters the Policy Applies to | 4 |
| Matters this Policy does not apply to | 5 |
| Who can receive a disclosure? | 6 |
| How to make a disclosure | 7 |
| Legal protections for disclosers | 8 |
| Support and practical protection for disclosers | 9 |
| Handling & Investigating Disclosure | 10 |
| Ensuring fair treatment of individuals mentioned in a disclosure | 11 |
| Ensuring the Policy is easily accessible | 11 |

| | |
|---------------------------------|-----------|
| Authority & Approval | 12 |
| Approval | 12 |
| Authority | 12 |
| Review | 12 |

| | |
|--------------------------------------|-----------|
| Appendix 1 – Reporting points | 13 |
|--------------------------------------|-----------|

About this document

Background

Praemium Limited (**Praemium**) is an ASX listed public company that has subsidiaries across Australia, Asia, Middle East and the UK (collectively 'Group'). The Group provides a number of products and services including financial software and technology, investment administration, financial products and investment platform administration. Policies are applied consistently across the Group, however, where jurisdictional differences arise, particularly in relation to supervisory and/or regulatory obligations, it is necessary to implement additional policies to the relevant areas of the business.

Praemium has obligations under the *Corporations Act 2001* (Cth) (the **Act**) and as an ASX-listed public company, is required to have an appropriate Whistleblower Policy (this **Policy**)¹.

Purpose

Praemium is committed to the highest standards of conduct and ethical behaviour and promoting and supporting a culture of honest and ethical behaviour, corporate compliance and good corporate governance. Praemium recognises the important role whistleblowers play in identifying wrongdoing or conduct that is not consistent with Praemium's Risk Appetite, Code of Conduct and various regulatory obligations-across the Group.

This Policy provides a confidential and secure process for receiving, advising, handling and addressing wrongdoing which may otherwise go undetected. Praemium encourages the reporting of any instances of suspected unethical, illegal, fraudulent or undesirable conduct involving Group businesses. The purpose of this Policy includes:

- (a) encouraging more disclosures of wrongdoing;
- (b) helping deter wrongdoing;
- (c) ensuring individuals who disclose wrongdoing can do so safely, securely and with confidence that they will be protected and supported;
- (d) ensuring disclosures are dealt with appropriately and on a timely basis; and
- (e) providing transparency around Praemium's framework for receiving, handling and investigating disclosures.

This Policy sets out how you can assist us with that process.

Adjunct Policies

This Policy should be read in conjunction with the following Praemium policies available on the [Australian SharePoint page](#):

- Code of Conduct
- Grievance & Complaint Policy
- Complaints Handling Policy and
- Incidents & Breaches Policy

Non-compliance

Any non-compliance with or a 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 the 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).

¹ Section 1317AI (5) of the Act. Whistleblower laws are found in Part 9.4AAA and section 1317AI of the Act.

Policy Content

Who this Policy applies to:

Disclosers who can make a disclosure that qualifies for protection under the Act are called 'eligible whistleblowers'.

Eligible whistleblowers in a body corporate

An eligible whistleblower is an individual who is, or has been, any of the following in relation to Praemium:

- (a) an officer or employee;
- (b) a supplier of services of goods, including their employees;
- (c) an associate; or
- (d) a relative, dependant or spouse of any of the above.

Eligible whistleblowers in a superannuation entity

An eligible whistleblower is an individual who is, or has been, any of the following in relation to Praemium:

- (a) a trustee, custodian or investment manager, including their employees;
- (b) a supplier of services or goods to the trustee, custodian or investment manager, including their employees;
- (c) an officer, employee or supplier of services or goods of a body corporate that is a trustee, custodian or investment manager of a superannuation entity; or
- (d) a relative, dependant or spouse of any of the above.

Matters the Policy Applies to

Disclosures about '**disclosable matters**' will qualify for protection under the Act.

Disclosable matters

Disclosable matters involve information that the discloser has '**reasonable grounds**' to suspect' concerns 'misconduct', or an 'improper state of affairs or circumstances', in relation to Praemium or its related entities. Note: motive is not relevant for a whistleblower to qualify for protection. Although a disclosure may not qualify for protection under this Policy it may be protected under Fair Work.

Misconduct

Misconduct includes fraud, negligence, default, breach of trust and breach of duty.

Improper state of affairs or circumstances

Misconduct or an improper state of affairs or circumstances may not involve unlawful conduct in relation to Praemium or its related entities but may indicate a systemic issue that the relevant regulator should know about to perform its functions. It may also relate to business behaviour and practices that may cause consumer harm.²

Reasonable grounds to suspect

Reasonable grounds to suspect are based on the objective reasonableness of the discloser. A mere allegation with no supporting information is not likely to be considered as having reasonable grounds to suspect. Objective reasonableness does not require a discloser to prove their allegations.

Disclosable matters also involve information about Praemium, if the discloser has reasonable grounds to suspect that the information indicates Praemium has engaged in conduct that:

- (a) constitutes an offence against, or a contravention of, a provision of any of the following:

² See ASIC Regulatory Guide (RG) 270, "Whistleblower policies" at RG 270.52. RG 270 also provided guidance for this Policy.

- the Act;
 - the Australian Securities and Investments Commission Act 2001 (Cth);
 - the Banking Act 1959 (Cth);
 - the Financial Sector (Collection of Data) Act 2001 (Cth);
 - the Insurance Act 1973 (Cth);
 - the Life Insurance Act 1995 (Cth);
 - the National Consumer Credit Protection Act 2009 (Cth);
 - the Superannuation Industry (Supervision) Act 1993 (Cth);
 - an instrument made under an act referred to above;
- (b) constitutes an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months or more;
- (c) represents a danger to the public or the financial system; or
- (d) is prescribed by regulation.

Examples of disclosable matters as they relate to business operations and practices

This Policy covers the following types of wrongdoing:

- (a) illegal conduct, such as theft, dealing in, or use of illicit drugs, violence or threatened violence and criminal damage against property;
- (b) fraud, money laundering or misappropriation of funds;
- (c) offering or accepting a bribe;
- (d) financial irregularities;
- (e) failure to comply with, or breach of, legal or regulatory requirements; and
- (f) engaging in or threatening to engage in detrimental conduct against a person who has made a disclosure or is believed or suspected to have made, or be planning to make, a disclosure.

Disclosable matters may include conduct that does not contravene a particular law

Information that indicates a significant risk to public safety or the stability of, or confidence in, the financial system is also a disclosable matter, even if it does not involve a breach of a particular law.

False reporting

Praemium strongly encourages the reporting of any disclosable matters where there are reasonable grounds to suspect wrongdoing or misconduct. However, individuals who deliberately submit false reports are not afforded protection under the Act and may be subject to scrutiny from the Head of Human Resources or another designated Praemium Manager. Deliberate false reports involve a discloser reporting information they know to be untrue. It does not include situations where a discloser reasonably suspects misconduct, but the suspicions are later determined to be unfounded. Discloser can still qualify for protection even if their discloser turns out to be incorrect

Before you make a disclosure, it is strongly recommended that you read this Policy so you can understand how your disclosure will be treated and options and protections available to you.

Matters this Policy does not apply to

Personal work-related grievances

Personal work-related grievances do not qualify for protection under the Act. These are grievances that relate to the discloser's current or former employment and have, or tend to have, implications for the discloser personally, but do not:

- (a) have any other significant implications for Praemium; or
- (b) relate to any conduct, or alleged conduct, about a disclosable matter.

Examples of personal work-related grievances include:

- (a) an interpersonal conflict between the discloser and another employee;
- (b) a decision that does not involve a breach of workplace laws;
- (c) a decision about the engagement, transfer or promotion of the discloser;
- (d) a decision about the terms and conditions of engagement of the discloser; or

- (e) a decision to suspend or terminate the engagement of the discloser, or otherwise to discipline the discloser.

However, a personal work-related grievance may still qualify for protection if:

- (a) it includes information about misconduct, or information about misconduct includes or is accompanied by a personal work-related grievance (mixed report);
- (b) Praemium has breached employment or other laws punishable by imprisonment for a period of 12 months or more, engaged in conduct that represents a danger to the public, or the disclosure relates to information that suggests misconduct beyond the discloser's personal circumstances;
- (c) the discloser suffers from or is threatened with detriment for making a disclosure; or
- (d) the discloser seeks legal advice or legal representation about the operation of the whistleblower protections under the Act.

Raising grievances that are not covered by this Policy

For work-related grievances and other types of issues or concerns that are not covered by the Policy, staff should refer to the Company's staff grievance and complaints handling policies and processes as referenced in "Adjunct Policies" above.

Who can receive a disclosure?

Eligible recipients within Praemium

A discloser must make a disclosure directly to one of Praemium's 'eligible recipients' to qualify for protection as a whistleblower under the Act.

Eligible recipients in a body corporate include:

- (a) an 'officer' or 'senior manager' of Praemium or its related bodies corporate;
- (b) the internal or external auditor or actuary of Praemium or its related bodies corporate; and
- (c) a person authorised by Praemium to receive disclosures that may qualify for protection.

Eligible recipients in a superannuation entity include:

- (a) an officer of Praemium;
- (b) Praemium's internal or external auditor or actuary;
- (c) an individual who is the trustee of Praemium;
- (d) a director of a body corporate that is the trustee of Praemium; and
- (e) a person authorised by the trustee(s) to receive disclosures that may qualify for protection.

Disclose to Praemium in the first instance

Praemium's priority is to identify and address wrongdoing and misconduct as early as possible. Praemium encourages its employees and external disclosers to make a disclosure directly to Praemium in the first instance and is committed to ensuring the safety and protection of individuals in doing so. Refer to **Appendix 1** for a list of Praemium's eligible recipients.

Moreover, when a whistleblower directly approaches an external party such as a regulator or the media, neither the individual nor Praemium will be able to control the disclosure, messaging or investigation process which may be further damaging to the individual and Praemium.

However, disclosures can be made to certain external parties or directly to regulatory bodies and qualify for protection under the Act without making a prior disclosure to Praemium. Refer to **Appendix 1** for the external eligible recipient list.

Legal Practitioners

Disclosures made to a legal practitioner for the purposes of obtaining legal advice or legal representation in relation to the operation of the whistleblower provisions in the Act are protected (even in the event the legal practitioner concludes that a disclosure does not relate to a disclosable matter).

Regulatory bodies and other external recipients

Disclosures of information relating to disclosable matters can be made to:

- [ASIC](#)
- [APRA](#)
- [ATO](#) (for tax related matters) or
- another Commonwealth body prescribed by regulation, and which qualifies for protection under the Act.

Public interest disclosures and emergency disclosures

In certain circumstances, disclosures can be made to a journalist or parliamentarian and qualify for protection under the whistleblower provisions of the Act.

Public interest disclosure

A public interest disclosure is the disclosure of information to a journalist or a parliamentarian, where:

- (a) at least 90 days have passed since the discloser made the disclosure to ASIC, APRA or another Commonwealth body prescribed by regulation;
- (b) the discloser does not have reasonable grounds to believe that action is being, or has been taken, in relation to their disclosure;
- (c) the discloser has reasonable grounds to believe that making a further disclosure of the information is in the public interest; and
- (d) before making the public interest disclosure, the discloser has given written notice to the body that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the discloser intends to make a public interest disclosure.

Emergency disclosure

An emergency disclosure is the disclosure of information to a journalist or parliamentarian, where:

- (a) the discloser has previously made a disclosure of the information to ASIC, APRA or another Commonwealth body prescribed by regulation;
- (b) the discloser has reasonable grounds to believe that the information concerns a substantial and imminent danger to the health or safety of one or more persons or to the natural environment;
- (c) before making the emergency disclosure, the discloser has given written notice to the body to which the previous disclosure was made that:
 - includes sufficient information to identify the previous disclosure; and
 - states that the discloser intends to make an emergency disclosure; and
- (d) the extent of the information disclosed in the emergency disclosure is no greater than is necessary to inform the journalist or parliamentarian of the substantial and imminent danger.

Seek advice before making a public interest disclosure or emergency disclosure

It is important to understand the criteria for making a public interest or emergency disclosure. Praemium recommends that you seek independent legal advice before doing so.

How to make a disclosure

Internal disclosure

Disclosable matters can be reported to the reporting contacts at **Appendix 1**, or via an Employee's manager, another senior manager or HR department. Disclosable Matters can be made in person, by telephone, or in writing by email or via mail to Praemium's address. Disclosures can be made anonymously and/or confidentially, securely and outside of business hours. For overseas subsidiaries, matters can be disclosed in the same manner noted above to the Local Company Secretary. It is our aim to identify and address any wrongdoing as soon as possible, and thus ensure our bone fides in relation to the whistleblower and the processes and procedures we have implemented.

Alternatively, employees who are not comfortable making a disclosure internally, or feel it is inappropriate to do so, can still make a disclosure directly to any of the entity's 'eligible recipients', not just its internal reporting points, and qualify for protection. The availability of an external reporting recipient (e.g., external

auditor) also enables the entity's non-employees (e.g., former employees and current and former suppliers) to make a disclosure to the entity.

Anonymous disclosures

Disclosures can be made anonymously and still be protected under the Act.

A discloser can choose to remain anonymous while making a disclosure, over the course of the investigation and after the investigation is finalised. A discloser can refuse to answer questions that they feel could reveal their identity during follow-up conversations. However, a discloser who wishes to remain anonymous should maintain ongoing two-way communication with Praemium, so Praemium can ask follow-up questions or provide feedback. In practice, if a disclosure comes from an email address from which the person's identity cannot be determined, and the discloser does not identify themselves in the email, it should be treated as an anonymous disclosure.

Praemium will adopt the following measures and mechanisms for protecting anonymity:

- Where requested, the discloser will be kept anonymous (e.g., through use of a pseudonym); and
- The identity of the whistleblower and the report made by them will be kept confidential and secure.

Legal protections for disclosers

The following protections apply not only to internal recipients, but also to disclosures to legal practitioners, regulatory and other external bodies, and public interest and emergency disclosures that are made in accordance with the Act.

Identity protection (confidentiality)

A person cannot disclose the identity of a discloser or information that is likely to lead to the identification of the discloser. The exception to this is if a person discloses the identity of the discloser:

- (a) to ASIC, APRA or a member of the Australian Federal Police;
- (b) to a legal practitioner (for the purposes of obtaining legal advice or legal representation about the whistleblower provisions in the Act);
- (c) to a person or body prescribed by regulations; or
- (d) with the consent of the discloser.

A person can disclose the information contained in a disclosure with or without the discloser's consent if:

- (a) the information does not include the discloser's identity;
- (b) all reasonable steps are taken to reduce the risk that the discloser will be identified from the information; and
- (c) it is reasonably necessary for investigating the issues raised in the disclosure.

It is illegal to identify a discloser or disclose information that is likely to lead to the identification of the discloser, outside the above exceptions. Should this occur, the discloser can lodge a complaint with Praemium or a regulator such as ASIC, APRA or the ATO. (See links provided in section "Regulatory bodies and other external recipient".

Whistleblowers should note that people may be able to guess their identity where:

- (a) they have previously mentioned to other people they are considering making a disclosure;
- (b) they are a very small number of people with access to the information; or
- (c) the disclosure relates to information that the person has previously been told privately and in confidence.

Protection from detrimental acts or omissions

A person cannot engage in conduct that causes detriment to a discloser, in relation to a disclosure, if:

- (a) the person believes or suspects that the discloser made, may have made, proposes to make or could make a disclosure that qualifies for protection; and
- (b) the belief or suspicion is the reason, or part of the reason, for the conduct.

In addition, a person cannot make a threat to cause detriment to a discloser in relation to a disclosure. A threat may be express or implied, conditional, or unconditional. A discloser need not fear whether or not the threat will be carried out, in order for the conduct to be considered a threat.

Detrimental conduct and threats include:

- (a) dismissal of an employee;
- (b) injury of an employee in his or her employment;
- (c) alteration of an employee's position or duties to his or her disadvantage;
- (d) discrimination between an employee and other employees of the same employer;
- (e) harassment or intimidation of a person;
- (f) harm or injury to a person, including psychological harm;
- (g) damage to a person's property;
- (h) damage to a person's reputation;
- (i) damage to a person's business or financial position; or
- (j) any other damage to a person.

Actions that are not detrimental conduct

Detrimental conduct does not include administrative action that is reasonable to protect a discloser from detriment (e.g., when the disclosure relates to wrongdoing in the discloser's immediate work area). Protecting a discloser from detriment also does not prevent the management of unsatisfactory work performance if the action is in line with the performance management framework. Accordingly, Praemium must ensure a discloser understands the reason for any administrative or management action.

Compensation and other remedies

Eligible whistleblowers can seek compensation and other remedies through the courts if they suffer loss, damage, or injury because of a disclosure and Praemium failed to take reasonable precautions and exercise due diligence to prevent a person from causing the detriment. Eligible whistleblowers should seek independent legal advice, as necessary.

Civil, criminal and administrative liability protection

Eligible whistleblowers are protected from any of the following in relation to their disclosure:

- (a) civil liability;
- (b) criminal liability; and
- (c) administrative liability.

These protections do not grant immunity for any misconduct a discloser has engaged in that is revealed in their disclosure.

Support and practical protection for disclosers

Identity protection (confidentiality)

Praemium will implement the following measures for protecting the confidentiality of a discloser's identity:

- (a) all personal information or reference to the discloser witnessing an event will be changed (i.e., pseudonym);
- (b) the disclosure will be referred to in a gender-neutral context;
- (c) where possible, the discloser will be contacted to help identify certain aspects of their disclosure that could inadvertently identify them; and
- (d) disclosures will be handled and investigated by qualified staff.

Secure record-keeping and information-sharing processes

To ensure the identity of disclosers and information relating to disclosure are adequately protected, Praemium will ensure that:

- (a) all paper and electronic documents and other materials relating to disclosures are stored securely;

- (b) access to all information relating to a disclosure will be limited to those directly managing and investigating the disclosure;
- (c) only a restricted number of people who are directly handling or investigating a disclosure will be made aware of a discloser's identity (subject to the discloser's consent) or information that is likely to lead to the identification of the discloser;
- (d) communications and documents relating to the investigation of a disclosure will not be sent to an email address or to a printer that can be accessed by other staff; and
- (e) each person who is involved in handling and investigating a disclosure will be reminded about the confidentiality requirements, including that an unauthorised disclosure of a discloser's identity may be a criminal offence.

Protection from detrimental acts of omissions

Praemium will implement measures for protecting disclosers from detriment, including:

- (a) processes for assessing the risk of detriment against a discloser and other persons, which will commence as soon as possible after receiving a disclosure;
- (b) support services, including the appointment of a designated person (including those in Appendix 1 to provide support or counselling where appropriate which may include Praemium's Employee Assistance Program which provides anonymity to its clients;
- (c) strategies to help a discloser minimise and manage stress, time or performance impacts, or other challenges resulting from the disclosure or its investigation;
- (d) practical actions, as required for protecting a discloser from risk of detriment;
- (e) processes for ensuring that management are aware of their responsibilities to maintain the confidentiality of a disclosure;
- (f) procedures on how a discloser can lodge a complaint if they have suffered detriment and
- (g) [Interventions for protecting a discloser if detriment has already occurred.](#)

If you feel that after making a disclosure you are experiencing detrimental treatment you can make a further disclosure relating to this conduct.

Handling & Investigating Disclosure

Handling a disclosure

Praemium will assess each disclosure to determine whether:

- (a) it qualifies for protection; and
- (b) a formal, in-depth investigation is required.

Praemium will ensure the process followed is:

- fair
- timely and
- be independent of the person about whom the allegation is made.

Investigating a disclosure

All reports relating to a disclosable matter made by an eligible whistleblower and received by an internal eligible recipient, or where an external party informs an officer or senior manager of a disclosable matter that was reported by the eligible whistleblower directly to the external party, must be investigated thoroughly and completely so as to appropriately substantiate or refute the information reported/disclosed. Upon receipt of such a disclosable matter, the Head of Compliance or Company Secretary must be advised as soon as practicable. At all times, Praemium takes disclosures made whether anonymously, or not, very seriously.

The Head of Compliance or Company Secretary will have ultimate carriage of the matter.

At a minimum, if a matter is deemed a complaint by the Head of Compliance or Company Secretary that needs to be investigated, they will determine:

- the nature and scope of the investigation;
- person(s) within and/or outside the entity that should lead the investigation;

- the nature of any technical, financial or legal advice that may be required to support the investigation; and
- the timeframe for the investigation.

Detailed records of the disclosable matter must be maintained in a secure and confidential manner, including the report/disclosure itself, investigations undertaken, actions taken to address and further correspondence with the discloser in relation to the progress of the matter.

Where investigations substantiate the disclosure in terms of the occurrence of wrongdoing or misconduct, a suitable response and actions to address must be implemented in a timely manner. Each disclosure will be acknowledged within a reasonable period after the disclosure is received if the discloser can be contacted (including through anonymous channels). Note however that Praemium may be impeded in investigating the matter if the discloser cannot be contacted.

Keeping the Informer informed

As soon as practicable, Praemium will keep the discloser apprised of developments in the matter. Such updates may include when the investigation process has begun and progress reports. Such contact will again demonstrate to the person, Praemium's bona fides in taking the matter seriously. The timeframe and frequency of keeping the discloser apprised may vary, especially, when the complaint was made anonymously, and it may be difficult to contact the person. Where the disclosure was made anonymously, Praemium will ensure that anonymity is not compromised when such updates are provided.

Reporting

Findings from investigations will be documented and reported to or by the Company Secretary and Head of Compliance, or if necessary, directly to a Member of the Praemium Audit, Risk & Compliance Committee, while preserving confidentiality. The method for documenting and reporting the findings, will however, depend upon the nature of the disclosure. A summary of the outcomes of the investigation will also be provided to the discloser, upon completion of investigations, when appropriate.

Where a Disclosable Matter that is reported relates to a conduct of an individual that could otherwise be an Eligible Recipient, the matter must be investigated with sufficient independence. Where necessary, this may involve engaging a Member of the Praemium Audit, Risk & Compliance Committee to handle the matter.

The Company Secretary and Head of Compliance, following advice, may report the matter to state or federal police, regulators, or any other state or federal authority as appropriate.

Ensuring fair treatment of individuals mentioned in a disclosure

Praemium will adopt the following measures for ensuring fair treatment of individuals mentioned in a disclosure:

- disclosures will be handled confidentially when it is practical and appropriate in the circumstances;
- each disclosure will be assessed and may be the subject of an investigation;
- the objective of the investigation is to determine whether there is enough evidence to substantiate or refute the matters reported. (Our focus as stated previously, is always on the substance of the complaint, not the motive for disclosure).
- when an investigation needs to be undertaken, the process will be objective, fair and independent;
- an employee who is the subject of a disclosure will be advised about the subject matter of the disclosure as and when required; and
- an employee who is the subject of a disclosure may contact appropriate support services (e.g., counselling).

Ensuring the Policy is easily accessible

Praemium will ensure that this Policy is promoted and made available to employees and officers as follows:

- holding staff briefing sessions, especially when the Policy is updated;
- posting the Policy on the staff intranet or other communication platform;

- (c) posting information on staff noticeboards;
- (d) setting out the Policy in the employee handbook; and
- (e) incorporating the Policy in employee induction information packs and training for new starters.

The Policy will also be made available on the Praemium website.

Authority & Approval

Approval

This Policy is prepared and maintained by the Company Secretary and must be approved by Praemium's Board of Directors ('the Board').

Authority

The Company Secretary is authorised to implement and review this Policy and monitor ongoing compliance with this Policy.

Review

This Policy must be reviewed at least once every two years, or in the event of material changes to regulations or the business which affect the scope of this Policy or its implementation.

The review must be undertaken by a person authorised to do so and the Board must be notified of the outcome of each review.

Any changes to the Policy recommended by the Company Secretary must be approved by the Board prior to implementation.

Appendix 1 – Reporting points

| | |
|----------------|--|
| Name | Rachel Axton |
| Title | Group Company Secretary |
| Contact Number | 0412 020 777 |
| Email | rachel.axton@praemium.com |
| Address | Level 19, 367 Collins Street, Melbourne VIC 3000 |

| | |
|----------------|--|
| Name | Anthony Wamsteker |
| Title | Chief Operating Officer |
| Contact Number | 0434 321 999 |
| Email | anthony.wamsteker@praemium.com |
| Address | Level 19, 367 Collins Street, Melbourne VIC 3000 |

| | |
|----------------|--|
| Name | Angela Godfrey |
| Title | Chief People & Culture Officer |
| Contact Number | |
| Email | angela.godfrey@praemium.com |
| Address | Level 19, 367 Collins Street, Melbourne VIC 3000 |

| | |
|----------------|--|
| Name | External Auditor |
| Title | Audit Partner of Praemium Limited |
| Contact Number | +61 (3) 8320 2222 |
| Email | |
| Address | Grant Thornton, Collins Square Tower 5, 727 Collins Street, Melbourne VIC 3008 |