Whistleblower Policy

AUB Group Limited
ACN 000 000 715

Adopted by the Board on 7 December 2023

Policy

1 What is the purpose of this Policy?

AUB Group Limited (the **Company**) and its controlled entities (together with the Company, the **Group**) are committed to conducting business honestly, with integrity, and in accordance with the Group's values and standards of expected behaviour.

As part of that commitment, the Group values developing and fostering a culture of corporate compliance, ethical decision-making and protecting eligible whistleblowers who make protected disclosures from suffering detriment.

The purpose of this Policy is to:

- encourage people to report suspected wrongdoing they see in connection with the Group's business;
- help deter wrongdoing, in line with the Group's risk management and governance framework;
- explain how to report suspected wrongdoing and what protections a discloser will receive;
- outline the Group's processes for responding to reports of suspected wrongdoing;
- promote a workplace environment in which everyone feels safe, supported and encouraged to report suspected wrongdoing; and
- support the Group's values and Code of Conduct.

A failure to report suspected wrongdoing exposes the Group to additional risks and will undermine our culture and values.

The Group will not tolerate anyone being discouraged from reporting suspected wrongdoing or being subject to detriment because they want to report suspected wrongdoing or they have done so. Disciplinary action, up to and including termination of employment or engagement, may be imposed on anyone shown to have caused or threatened to cause detriment to a person because they want to report, or have reported, suspected wrongdoing.

The Group operates in various locations globally and certain countries may have local whistleblowing laws that affect the application of this Policy. A non-exhaustive summary of country-specific provisions that may affect the operation of this Policy are set out at Annexures 1 to 6. This Policy should be read in conjunction with the Annexure applicable to the country in which a person is based and where there is an inconsistency between the relevant Annexure and this Policy, the Annexure will take precedence.

This Policy should be read in the context of the Group's other policies and procedures as varied from time to time (as made available on the Group website).

2 Who does this Policy apply to?

This Policy applies to the Group and:

- all of the Group's current and past employees, volunteers, officers, contractors, suppliers (including employees of suppliers), and associates; and

- a relative, dependant or dependant of the spouse of any person referred to above.

The above persons are '**Eligible Whistleblowers**' and may also qualify for protections under the law when reporting wrongdoing in certain circumstances.

3 What is Potential Misconduct?

Potential Misconduct is any suspected or actual misconduct or improper state of affairs or circumstances in relation to the Group.

Without limitation, this could include conduct by an employee or officer of the Group which is in breach of certain laws or which represents a danger to the public or to the financial system.

If you are unsure if something is Potential Misconduct, you can contact the Chief Legal and Risk Officer for more information.

Potential Misconduct does **not** generally include **personal work-related grievances**.

Personal work-related grievances are grievances about something in relation to your current or former employment or engagement that have implications for you personally (such as a disagreement between you and another employee or a decision about your promotion).

Generally, these grievances should be raised in accordance with the Grievance Policy to allow those issues to be resolved most effectively.

Examples of Potential Misconduct can include, but are not limited to:

- breach of laws or regulations;
- material or systemic breaches of the Code of Conduct or other Group policies, standards or codes;
- criminal activity;
- bribery or corruption;
- conduct endangering health and safety, or causing damage to the environment;
- dishonest, unethical, or corrupt behaviour, including soliciting, accepting or offering a bribe, facilitation payments or other such benefits;
- conflicts of interest;
- information that indicates a danger to the public or to the financial system;
- anti-competitive behaviour;
- financial fraud or mismanagement;
- insider trading;
- breach of trade sanctions or other trade controls;
- unauthorised use of the Group's confidential information;
- conduct likely to damage the Group's financial position or reputation;
- in respect of a particular country, any other 'disclosable matter' (or equivalent) listed in the Annexure for that country; and
- deliberate concealment of the above.

While personal work-related grievances will not generally amount to Potential Misconduct, they may be covered by this Policy in certain situations. For example, a personal work-related grievance may be covered by this Policy if it:

- relates to detriment that has been suffered or is threatened because an individual has raised a concern about suspected Potential Misconduct;
- relates to both a personal work-related grievance and Potential Misconduct; or

- relates to concerns that the Group 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 information that suggests misconduct beyond the discloser's personal circumstances.

4 Who should I tell?

You are encouraged to report Potential Misconduct to one of the following **Recipients**:

Recipient Name	Name and/or Contact Details
Chief Legal and Risk Officer	**Richard Bell** +61 2 9935 2235 Level 14, 141 Walker Street, North Sydney NSW 2060 RichardB@aubgroup.com.au
Chair of the Board Audit & Risk Committee	**Richard Deutsch** Contact details available on request from AUB Group Head of Company Secretarial
SafeCall (independent hotline provider)	Hotline available 24/7. Contact telephone numbers for all countries are available at www.safecall.co.uk/file-a-report/telephone-numbers/

The role of Recipients is to ensure that the information is heard by the Group and proper follow-up occurs, as well as to ensure that you feel supported and protected. You can make your disclosure to a Recipient by using any listed method you prefer.

SafeCall is an independent hotline service that gives you the opportunity to report Potential Misconduct to a third party at any time, including anonymously if preferred. Suspected Potential Misconduct reported via Safecall will be notified to one or more designated members of the Group Risk and Audit and Legal and Compliance Teams and/or their respective delegates. Details of your report may also be shared with other people who will be involved in investigating, reporting on or taking other action to address your report.

People must not discourage you from making a report under this Policy, and to do so will itself breach this Policy. If you are told not to raise or pursue a concern, even by your manager or a person in authority, you are encouraged to raise the concern with a Recipient.

While we encourage you to report Potential Misconduct to one of the Recipients listed in the table above, there may be certain other additional people to whom you can make a report under the law in your country and still receive protections. For example, for Australia, see those listed in Annexure 1.

5 What information should I provide?

You should provide as much information as possible in your report, including details of the Potential Misconduct, people involved, dates, locations and if any more evidence may exist.

You are encouraged to feel supported and safe in providing information, and to consent to the limited sharing of your identity. This will assist the Group to protect and support you in relation to your report and facilitate the Group in investigating, reporting on and taking action arising as a result of your report.

Please be aware that if you do not consent to the limited sharing of your identity as needed, this may limit the Group's ability to progress your report and take any action in respect of it.

6 What if the information in my report is incorrect?

When making a report you will be expected to have reasonable grounds to believe the information you are disclosing is true, but you will not be penalised even if the information turns out to be incorrect. Your motive is irrelevant to whether your report is covered by this Policy. However, you obviously must not make a report that you know is not true or is misleading.

Where it is found that a person has knowingly made a false report, this may be a breach of the Group's Code of Conduct and this Policy, and will be considered a serious matter that may result in disciplinary action, up to and including termination of employment or engagement.

7 Can I make an anonymous report?

You can make an anonymous report if you want.

The Group encourages the reporting of Potential Misconduct, however we appreciate that doing so can be difficult.

We encourage you to provide your name because it will make it easier to investigate and address your report. However, you are not required to do so, and may choose to remain anonymous when making a disclosure, over the course of any investigation and after any investigation is finalised.

If you do not provide your name, any investigation will be conducted as best as possible in the circumstances. The Group will assess the content and merit of your disclosure in the same way as if you had revealed your identity. However, an investigation may not be possible unless sufficient information is provided, and it may make it difficult to offer you the same level of practical support if we do not know your identity.

If you do provide your name, it will only be disclosed in accordance with this Policy. If you have concerns about this, you can discuss this with the Recipient.

8 How will the Group respond to a report?

If you make a report under this Policy:

- It will be treated sensitively and seriously, and will be dealt with promptly, fairly and objectively.
- The Group will apply protections in accordance with this Policy, including section 10 below and/or any applicable Annexure.
- The Group's response to a report will vary depending on the nature of the report and the amount of information provided. Your report may be addressed and resolved informally or through formal investigation.
- Recipients will endeavour to contact you within 3 business days of receiving your report, where appropriate and you have provided a means of contact.
- If appropriate, you will be told how the Group has decided to respond to your disclosure, including whether an investigation will be conducted. This may not occur until after an investigation has been concluded. However, it may not always be appropriate to provide disclosers with this information, and may not be possible unless contact details are provided.
- While making a report does not guarantee a formal investigation, all reports will be properly assessed and considered by the Group and a decision made as to whether they should be formally investigated or internally resolved.
- Any investigations commenced will be conducted in a timely manner and will be fair and independent from any persons to whom the report relates. While timeframes will vary depending on the particular investigation, the Group endeavours to conclude investigations within 4 weeks of commencing the investigation.
- Where practicable, the Group will aim to update you about the general progress of any investigation on a monthly basis until it is finalised.
- Investigations will generally be overseen by the Chief Legal and Risk Officer, subject to any potential conflicts of interest or concerns. Other people, including employees or external advisers, may also be asked to assist or run the investigation.
- All employees and contractors must cooperate fully with any investigations.
- Unless there are confidentiality or other reasons not to do so, persons to whom a report relates will be provided with details of the report relevant to them (not the entire report or the results of the report) at an appropriate time (to the extent permitted by law) and be given an opportunity to respond to the details/allegations relevant to them.

9 What happens after an investigation?

The results of any investigation will be recorded in writing in a formal internal report that will be confidential and is the property of the Group. The outcome of any investigation will be reported to the Board in accordance with section 11 below.

The formal report recording the results of an investigation will not be provided to a discloser or any other person subject to or implicated in an investigation.

Where an investigation identifies a breach of the Group's Code of Conduct or internal policies or procedures, appropriate disciplinary action may be taken. This may include but is not limited to terminating or suspending the employment or engagement of a person(s) involved in any misconduct.

10 What protections exist if I make a report under the Policy?

The Group is committed to protecting people who report Potential Misconduct under this Policy. This section outlines the Group's policy on protecting those who make a report to which this Policy applies.

10.1 Protecting your identity

The Group will protect the identities of people who report Potential Misconduct. Your identity (and any information the Group has because of your report that someone could likely use to work out your identity) will only be disclosed if:

- you give your consent to the Group to disclose that information;
- the disclosure is allowed or required by law (for example, the disclosure is by the Group to certain regulators or to a lawyer in order to get legal advice); or
- in the case of information likely to identify you, it is reasonably necessary to disclose the information for the purposes of an investigation, but all reasonable steps are taken to prevent someone from working out your identity.

Measures which the Group will adopt to protect your identity may include some or all of the following, as appropriate and necessary in the circumstances:

- using a pseudonym in place of your name;
- if you choose to remain anonymous and have made your report via Safecall, communicating with you through the anonymous avenues available through that channel;
- redacting personal information or references to you;
- referring to you in a gender-neutral context;
- where possible, consulting with you to help identify the aspects of your disclosure that could inadvertently identify you;
- ensuring paper and electronic documents and other materials relating to your disclosure are stored securely;
- limiting access to all information relating to a report to those directly involved in managing and investigating the report;
- only disclosing your identity or information that is likely to lead to your identification in accordance with section 11 below and to a restricted number of people who are directly involved in handling and investigating the disclosure; and
- reminding each person who is involved in handling and investigating a disclosure about the confidentiality requirements, including the consequences of an unauthorised disclosure.

10.2 Protecting you from detriment

The Group and any other person must not victimise or cause detriment to you (or threaten to do so) because of a belief that you have, will or could report Potential Misconduct. Examples of detriment include discrimination, harassment, intimidation, retaliation, causing physical or psychological harm, damaging property, varying an employee's role or duties, or demoting or dismissing the person.

You are encouraged to tell a Recipient listed in section 4 if you are or someone else is being or has been subject to detrimental conduct, or if you are concerned that you may be subject to detrimental conduct. Preferably, this will be the Recipient to whom you made your initial disclosure, but can be to any Recipient. The Group will treat this very seriously.

Any person found to be involved in detrimental conduct will be subject to disciplinary action, up to and including termination of employment or engagement. The Group may also refer any person that has engaged in detrimental conduct to law enforcement authorities for further investigation.

The protections that will be offered by the Group to protect you from detriment will depend on things such as the Potential Misconduct and people involved. Protections may include the following, in the Group's discretion and as appropriate and necessary in the circumstances:

- monitoring and managing the behaviour of other employees;
- relocating employees (which may include the people alleged to have been involved in the Potential Misconduct) to a different division, group or office;
- offering you a leave of absence or flexible workplace arrangements while a matter is investigated;
- if you are an employee, providing you with access to the Group's Employee Assistance Program and/or additional support from counselling or other support services; and/or
- rectifying any detriment that you have suffered.

The Group will look for ways to support all people who make a report, but it will not be able to provide non-employees with the same type and level of support that it provides to employees. Where an aspect of this Policy cannot be applied to non-employees (for example, because the Group cannot itself offer flexible working arrangements to a supplier), the Group will still seek to offer as much support as practicable.

11 Reporting

All whistleblower reports will be promptly notified to the CEO and Managing Director by the Chief Legal and Risk Officer. Where there is a high degree of certainty that a whistleblower reports relates to Potential Misconduct, the report will also be promptly escalated to the Chair of the Board Audit and Risk Committee.

All incidents will be included in the periodic reporting to the Board Audit and Risk Committee.

The Board Audit & Risk Committee will be provided additional information about any material incidents raised.

12 Availability of this Policy and training

The Group will seek to ensure that officers and employees (including new officers and employees) are informed about and understand this Policy. Each officer and employee will receive a copy of this Policy and be provided with training about the Policy and their rights and obligations under it. Key officers and employees, including Recipients, will receive regular training, including in relation to how to respond to disclosures.

A copy of this Policy will also be available on the Group's public website at https://www.aubgroup.com.au/corporate-governance/.

13 Further information

Any questions about this Policy or making a report can be referred to the Chief Legal and Risk Officer (see Section 4 for contact details). Questions can be asked at any time, including before or after you have made a report under this Policy.

This Policy will be reviewed from time to time and amended as required.

This Policy does not form part of your terms of employment and may be amended from time to time.

Annexure 1 – Australia

Under Australian law, including the *Corporations Act 2001* (Cth) (the **Corporations Act**) and the *Taxation Administration Act 1953* (the **Tax Act**), legislative protections are available to Eligible Whistleblowers who make a 'protected disclosure' to certain people.

While you are encouraged to make a disclosure as set out under the Policy, the law will offer protections if you make a 'protected disclosure' in accordance with this Annexure (for example, you can report Potential Misconduct to people other than Recipients). A disclosure can qualify for legal protection even if it is made anonymously or turns out to be incorrect.

Protected disclosures

To be a '**protected disclosure'** qualifying for protection under the Corporations Act or Tax Act (as applicable), the Eligible Whistleblower must objectively have reasonable grounds to suspect that the disclosure concerns a '**disclosable matter**' and must make the disclosure to an '**eligible recipient**' who is able to receive such disclosures under the law. The Eligible Whistleblower's motive in making the disclosure is irrelevant. A matter that is disclosed under the Policy but which does not meet these criteria will not qualify for legal protection.

Types of 'disclosable matters' and 'eligible recipients' are outlined in the following table.

Disclosable matter	Eligible recipients

General disclosable matters
• Information about actual or suspected misconduct, or an improper state of affairs or circumstances in relation to the Group
• Information that the Group, or any officer or employee of the Group, has engaged in conduct that:
  ○ contravenes or constitutes an offence against certain legislation including the Corporations Act; *Australian Securities and Investments Commission Act 2001* (Cth); *Banking Act 1959* (Cth); *Financial Sector (Collection of Data) Act 2001* (Cth); *Insurance Act 1973* (Cth); *Life Insurance Act 1995* (Cth); *National Consumer Credit Protection Act 2009* (Cth); *Superannuation Industry (Supervision) Act 1993* (Cth); or an instrument made under any of the above;
  ○ represents a danger to the public or the financial system; or
  ○ constitutes an offence against any law of the Commonwealth that is
	Eligible recipients for any general disclosable matters
	• A person authorised by the Group to receive protected disclosures – i.e. Recipients under this Policy (see section 4);
	• An officer of the Group;
	• A senior manager of the Group, which the Group considers to include the Group's CEO and Managing Director, Chief Financial Officer, Chief Legal and Risk Officer;
	• An auditor, or a member of an audit team conducting an audit, of the Group;
	• An actuary of the Group;
	• ASIC, APRA or another Commonwealth body prescribed by regulation;
	• A legal practitioner for the purposes of obtaining legal advice or legal representation (even if the legal practitioner concludes the disclosure does not relate to a disclosable matter); or

Disclosable matter	Eligible recipients
punishable by imprisonment for a period of 12 months or more. Note that 'personal work-related grievances' are **not** 'disclosable matters', except in limited circumstances including as set out in Section 3 of the Policy above.	• Journalists or parliamentarians under certain circumstances allowing emergency and public interest disclosures. It is important for you to understand the criteria for making a public interest or emergency disclosure before doing so. You should contact an independent legal adviser before making a public interest or emergency disclosure.
Tax-related disclosable matters • Information about misconduct, or an improper state of affairs or circumstances, in relation to the tax affairs of the Company or an associate (as defined in the *Income Tax Assessment Act 1936* (Cth)), which the employee considers may assist the Eligible Recipient to perform functions or duties in relation to the tax affairs of the Company or an associate	**Eligible Recipients for any tax-related disclosable matters** • A person authorised by the Group to receive reports of tax-related disclosable matters – i.e. Recipients under this Policy (see section 4) • An auditor, or a member of an audit team conducting an audit, of the Group • A registered tax agent or BAS agent who provides tax services or BAS services to the Group • A director, secretary or senior manager of the Group • An employee or officer of the Group who has functions or duties that relate to the tax affairs of the Group • A legal practitioner for the purpose of obtaining legal advice or legal representation (even if the legal practitioner concludes the disclosure does not relate to a disclosable matter)
Further tax-related information Information that may assist the Commissioner of Taxation to perform his or her functions or duties under a taxation law in relation to the Company or an associate (as defined in the *Income Tax Assessment Act 1936* (Cth))	**Eligible Recipients for any further tax-related information** • Commissioner of Taxation • A legal practitioner for the purpose of obtaining legal advice or legal representation (even if the legal practitioner concludes the disclosure does not relate to a disclosable matter)

Specific protections and remedies

Legislative protections are available for disclosures qualifying for protection under the law, including but not limited to:

- it is illegal for a person to identify you, or disclose information that is likely to lead to your identification, except in certain circumstances including:
  - those referred to in section 10.1 of the Policy; and
  - if the disclosure is to the Australian Securities and Investments Commission, the Australian Prudential Regulation Authority, Australian Taxation Office, Australian Federal Police, a Commonwealth, State or Territory authority for the purposes of assisting the authority in the performance of its functions or duties, or to any other body which may be prescribed by legislation from time to time; and
- you are protected from detrimental acts or omissions, or the threat of detrimental acts or omissions, in relation to making (or because you will or can make) the disclosure and can seek compensation and other remedies through the Courts if you suffer loss, damage or injury because of a disclosure and the Group has failed to take reasonable precautions and exercise due diligence to prevent the detrimental conduct.

If your report qualifies for legal protection as described above and a person makes an unauthorised disclosure of your identity and/or causes or threatens to cause detriment to you because you have, will, or could report Potential Misconduct, the person will commit an offence under the law and you may be able to seek legal recourse. The person may also be liable for civil and/or criminal penalties.

You are also protected from the following in relation to a protected disclosure you make:

- civil liability (e.g. any legal action against you for breach of an employment contract, duty of confidentiality or another contractual obligation);
- criminal liability (e.g. attempted prosecution of you for unlawfully releasing information, or other use of the disclosure against you in a prosecution (other than for knowingly making a false disclosure)); and
- administrative liability (e.g. disciplinary action for making the disclosure).

However, you will not have immunity for any misconduct you have engaged in that is revealed in a disclosure.

Annexure 2 – Belgium

This annex provides the country specific procedure and legislative protection for Belgium and is drafted taking into account the provisions of the Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law (the **Directive**) and the Belgian transposing Law of November 28, 2022 on the Protection of Reporters of Breaches of Union or National Law (the **Whistleblower Act**).

Under the Whistleblower Act legislative protections are available to Eligible Whistleblowers (personal scope of application) who make a Protected Disclosure (see hereunder) concerning Disclosable matter(s) within the material scope of the Whistleblower Act (material scope of application).

This Annexure applies to all Eligible Whistleblowers (see below) associated with the Belgian entity of AUB, Tysers Belgium NV (**TBNV**).

Protected disclosures

To be a '**protected disclosure'** qualifying for protection under the Whistleblower Act, you must have a reason to believe that the reported information on infringements was correct at the time of reporting and the information has to fall within the material scope of the Act (i.e. be a disclosable matter, set out in the table below).

Second, you have to follow the legal procedure for internal or external reporting or disclosure (see below under 'reporting channels').

Types of 'Disclosable Matters' and 'Eligible Whistleblowers' are outlined in the following table.

Disclosable matter	Eligible Whistleblowers
The breaches in the following fields of law (domains) fall under the material scope of the Whistleblower Act and constitute protected disclosures: • public procurement; • financial services, products and markets and the prevention of money laundering and terrorist financing; • product safety and compliance; • transport safety; • environmental protection; • radiation and nuclear safety; • food and feed safety, animal health and welfare; • public health; • consumer protection;	Protection shall apply to reporting persons working in the private or public sector who acquired information on breaches in a work-related context including, at least, the following: • persons having the status of worker, within the meaning of Article 45(1) TFEU, including civil servants; • persons having self-employed status, within the meaning of Article 49 TFEU; • shareholders and persons belonging to the administrative, management or supervisory body of an undertaking, including non-executive members, as well as volunteers and paid or unpaid trainees; and • any persons working under the supervision and direction of contractors, subcontractors and suppliers.

Disclosable matter	Eligible Whistleblowers
• protection of privacy and personal data and security of networks and information systems; • combating tax fraud; and • combating social fraud (this includes (non-exhaustively) all breaches of the Social Penal Code and all breaches of the statute of independent workers).	Protection shall also apply to reporting persons where they report or publicly disclose information on breaches acquired in a work-based relationship which has since ended. Protection shall also apply to reporting persons whose work-based relationship is yet to begin in cases where information on breaches has been acquired during the recruitment process or other pre-contractual negotiations. The measures for the protection of reporting persons set out in Chapter VI of the Whistleblower Act shall also apply, where relevant, to: (a) facilitators; (b) third persons who are connected with the reporting persons and who could suffer retaliation in a work-related context, such as colleagues or relatives of the reporting persons; and (c) legal entities that the reporting persons own, work for or are otherwise connected with in a work-related context For disclosures concerning breaches related to financial services, products and markets, breaches related to the prevention of money laundering and terrorist financing, the reporting person is not required to prove the information was obtained in a work related context. The following are **not** Eligible Persons: • persons paid to report infringements to enforcement authorities in so far as they are listed as informants on the basis of their informed consent or registered as such in databases managed by authorities designated at national level; and • persons reporting or disclosing on the basis of an obligation stipulated in sector-specific Union acts.

Reporting channels

To be a '**protected disclosure'** qualifying for protection under the Whistleblower Act, you must follow the legal procedure for reporting. The Whistleblower Act provides in three legal reporting possibilities:

(a) internal reporting;

(b) external reporting; and

(c) disclosure.

A. Internal reporting procedure

The following internal procedure for reporting will apply, in addition to the group-level channel as provided in this Policy.

(1) Who should I tell?

You are encouraged to report Potential Misconduct to one of the following **Recipients**:

Recipient Name (Reporting Manager)	Contact Details
Justin Engelbrecht	Justin.Engelbrecht@tysers.com

The role of Recipients is to ensure that the information is heard by TBNV and proper follow-up occurs, as well as to ensure that you feel supported and protected. You can make your disclosure to a Recipient by using any listed method you prefer.

People must not discourage you from making a report under this Policy, and to do so will itself breach this Policy. If you are told not to raise or pursue a concern, even by your manager or a person in authority, you are encouraged to raise the concern with a Recipient.

(2) What information should I provide?

You should provide as much information as possible in your report, including details of the Potential Misconduct, people involved, dates, locations and if any more evidence may exist.

You are encouraged to feel supported and safe in providing information, and to consent to the limited sharing of your identity. This will assist TBNV to protect and support you in relation to your report and facilitate TBNV in investigating, reporting on and taking action arising as a result of your report.

Please be aware that if you do not consent to the limited sharing of your identity as needed, this may limit TBNV's ability to progress your report and take any action in respect of it.

(3) How will TBNV respond to a report?

If you make a report under this Policy:

- It will be treated sensitively and seriously, and will be dealt with promptly, fairly and objectively.
- TBNV will apply protections in accordance with this Annexure.
- Receipt of the report will be acknowledged within 7 days from the day of the report.
- The report received is accurately recorded in a secure report register. This register contains information such as the date and time of the report, the nature

of the (alleged) breach and other relevant details. This register is kept in a secure folder with access only for authorized persons.

- The Reporting Manager is responsible for following up the report carefully and verifies the accuracy of the allegations made in the report and addresses the reported breach, if necessary, including through measures such as an internal preliminary investigation, an inquiry, prosecution, recovery of funds or termination of proceedings.

(4) What happens after an investigation?

- The Reporting Manager will conduct an initial review to confirm whether it is a valid report within the scope and, if necessary, will evaluate and assess the received report in a completely independent manner and determine what action should be taken. In this regard, you may be contacted for additional information.
- Upon receipt of the report, the Reporting Manager shall initiate an investigation into the alleged breach and, in that capacity, is authorized to conduct an investigation independently. The purpose of the investigation is to establish the facts, identify possible violations and propose appropriate actions. If necessary for conducting a thorough and confidential investigation, the team of Reporting Manager(s) may be augmented by (external) experts, who support whistleblower investigations. If an external third party is authorized to (co)receive/investigate reports of breaches on behalf of the legal entity, such third party will provide appropriate safeguards regarding respect for independence, confidentiality and secrecy.
- The Reporting Manager will provide feedback on the report, in particular on the actions planned or taken as follow-up and on the reasons for such follow-up, within a reasonable period of not more than 3 months from the receipt of the report.
- If the breach is deemed proven based on the investigation results, appropriate and proportionate follow-up actions will be taken. This may range from disciplinary action against those involved to taking corrective action to improve compliance and prevent future breaches.
- Upon completion of the investigation, you will be informed of the results and any actions taken. If desired, information on the general progress of the report process may also be provided without revealing confidential information.

(5) Confidentiality

Ensuring confidentiality is essential to protect you and to promote a safe environment in which reports can be made. TBNV is committed to respecting and protecting your confidentiality.

In principle, your identity shall not be disclosed to anyone other than the authorised personnel responsible for receiving or following up reports without your free and express consent. This also applies to any other information from which your identity can be directly or indirectly deduced.

Notwithstanding the above, your identity and any other information from which your identity can be directly or indirectly inferred may be disclosed if it is a necessary and proportionate obligation under special legislation in the context of investigations by national authorities or judicial proceedings, including to safeguard the rights of defence of the data subject.

The Reporting Manager(s) and all other persons acting in the investigation of the report will keep your identity confidential during the proceedings, unless investigations by national authorities or legal proceedings require immediate disclosure.

B. External reporting

You also have the right to report (alleged) breaches directly externally to the relevant competent authority. However, the Group encourages each Reporter to first report a (suspected) breach internally before going to the authorities.

The authorities competent to receive reports, provide feedback and follow up on reports are as follows:

- the Federal Public Service Economy, SMEs, Self-Employed and Energy;
- the Federal Public Service Finance;
- the Federal Public Service Health, Food Chain Safety and Environment;
- the Federal Public Service Mobility and Transport;
- the Federal Public Service Employment, Labor and Social Dialogue;
- the Programming Public Service Social Integration, Poverty Reduction, So-cial Economy and Metropolitan Policy;
- the Federal Agency for Nuclear Control;
- the Federal Agency for Medicines and Health Products;
- the Federal Agency for the Safety of the Food Chain;
- the Belgian Competition Authority;
- the Data Protection Authority;
- the Financial Services and Markets Authority;
- the National Bank of Belgium;
- the College of Supervision of Auditors;
- the authorities reported in article 85 of the law of September 18, 2017 on the prevention of money laundering and the financing of terrorism and on the restriction of the use of cash;
- the National Committee for the Security of Drinking Water Supply and Distribution;
- the Belgian Institute of Postal Services and Telecommunications;
- the National Institute for Health and Disability Insurance;
- the National Institute for the Social Insurance of the Self-Employed;
- the National Employment Service;
- the State Social Security Administration;
- the Social Intelligence and Investigation Service;
- the Autonomous Anti-Fraud Coordination Service (CAF); and
- the Shipping Inspectorate.

In the absence of designation or if no authority considers itself competent to receive a report, the Federal Ombudsman act as the competent authority for the application of the Whistleblower Act.

More information can be consulted through the websites of the respective competent authorities, as well as through the Federal Ombudsman's website which can be accessed at www.federaalombudsman.be/nl/klokkenluiders.

C. Disclosure

A person who makes the information about the breaches publicly available ("Disclosure") cannot qualify for protection under this Policy, Annexure and/or the Whistleblower Act unless one of the following conditions are met:

- the person first made an internal and external disclosure, or immediately made an external disclosure, but no appropriate action was taken as a result of that disclosure within the timeframe provided; or
- the person has reasonable grounds to believe that:
  - (1) the breach may represent an imminent or real danger to the public interest; or
  - (2) in the case of an external report, there is a risk of reprisals, or it is unlikely that the breach will be effectively repaired because of the particular circumstances of the case (e.g. because evidence may be withheld or destroyed, or an authority may collude with the perpetrator of the breach or is involved in the breach).

Specific (legal) protections and remedies

TBNV shall ensure that you, when you report in accordance with this Policy and this Annexure in good faith an (alleged) breach, whether internal or external, will not suffer retaliation, nor threats or attempts of retaliation. You shall not lose the benefit of this protection on the sole ground that the report made in good faith is found to be false or unfounded.

TBNV further warrants that it will not discriminate against, nor tolerate discrimination or (threats or attempts to) retaliate, against you, facilitators or against third persons associated with you who could retaliate in a work-related context (such as your colleagues or family members), and legal entities that you own, work for or are otherwise associated with in a work-related context.

Retaliation shall mean ‘any direct or indirect act or omission in response to an internal or external report or disclosure, and which results or may result in unwarranted prejudice’.

The protections provided for in this Policy, Annexure and the Whistleblower Act do not prevent adverse action against you for legitimate, non-retaliatory reasons, even if you are involved in protected activities, as long as the adverse action is not directly related to the report or participation in the investigation.

Annexure 3 – Dubai (Dubai International Financial Centre only)

This Policy must be considered in conjunction with relevant local laws applicable in the Dubai International Financial Centre (**DIFC**). If this Policy and local laws are inconsistent, local law obligations will prevail over this Policy.

Under DIFC law, including the *DIFC Operating Law (DIFC Law No. 7 of 2018) (as amended by DIFC Law No. 2 of 2022)* (**Ops Law**) and the *DIFC Regulatory Law (DIFC Law No. 1 of 2004) (as amended)* (**Regulatory Law**), legislative protections are available to Eligible Whistleblowers who make a **'protected disclosure'** to certain people.

However, it is important to bear in mind that certain criminal Federal UAE laws apply both outside and inside the DIFC and these should be considered carefully when considering whether to make a disclosure.

You are encouraged to seek independent legal advice if you are unsure about your rights and obligations under DIFC law.

Protected disclosures

To receive protection under DIFC law, disclosures must be made in good faith, otherwise a fine may be payable.

Under the Ops Law, the disclosures must include your identity (so cannot be anonymous) and relate to a reasonable suspicion that Tysers Insurance Brokers Limited (**TIBL**) has or may have contravened a provision of law.

To receive protection under the Regulatory Law, the disclosures must relate to a reasonable suspicion that TIBL or one of its employees has or may have engaged in money laundering, fraud or other financial crime, or contravened the Regulatory Law or DFSA rules or legislation. Unlike the Ops Law, anonymous disclosures under the Regulatory Law receive can protection.

Eligible persons

Disclosures under the Ops Law may be made to the DIFC Registrar of Companies, TIBL's auditor or a member of the audit team, a director or other officer of TIBL.

Disclosures under the Regulatory Law may be made to the DFSA, a UAE criminal law enforcement agency, TIBL, TIBL's auditor, a director or other officer of TIBL.

Specific protections and remedies

If you make a qualifying disclosure, you will not be subject to any contractual, or legal or civil liability (under the Ops Law or Regulatory Law respectively). You also shall not be dismissed from your employment with TIBL, or otherwise be subject to any action by TIBL, the Company or the Group, which is reasonably likely to cause detriment to you, for making the disclosure.

In addition if you make a disclosure under the Ops Law:

1 the DIFC Registrar of Companies will not disclose your identity unless required to do so for a regulatory purpose or by a Court; and

2 no contractual, civil, or other remedy or right shall be enforced against you by another person for making that disclosure, or any consequence resulting from such disclosure.

If you make a disclosure in accordance with the Regulatory Law no contractual, civil or other remedy or right shall be enforced against you by another person for making that disclosure.

Other considerations under DIFC law

In relation to making a disclosure under the Policy, it is important to consider:

- **General duty to report crimes**: Under Federal Decree Law No. 31 of 2021 (**UAE Penal Code**) there is a general duty to report crimes. This obligation applies even in circumstances where you would not be protected as a whistleblower under UAE law.
- **Defamatory disclosures**: Defamation is a criminal offence in the UAE. You must take care not to make disclosures which could be deemed to be defamatory in nature, as this could breach UAE law. Such disclosures may also be an offence under *Federal Law No. 34 of 2021* if made by electronic means (including by email). In particular (i) limit the persons to whom you communicate a disclosure to those who strictly need to receive it and (ii) ensure the content of the disclosure is limited to facts known to you.
- **Confidentiality obligations**: there are strict confidentiality obligations under the UAE Penal Code, including in relation to the disclosure of information obtained by virtue of employment. Breach of these obligations can lead to imprisonment and/or fines. By making a disclosure under the Policy of information in relation to TIBL, the Company or the Group, you will not be deemed to have breached any confidentiality requirements in relation to TIBL, the Company or the Group. However, where disclosures could relate to confidential information belonging to third parties, the Group is unable to give this assurance. You should seek independent legal advice before disclosing under the Policy confidential information in relation to other persons or businesses as this could breach UAE law.

Annexure 4 – Ireland

The *Protected Disclosures Act* 2014, as amended by the *Protected Disclosures (Amendment) Act 2022* (the **2014 Act**), gives legal protection to certain persons who make disclosures, including protections against dismissal or penalisation by their employer. These certain persons include employees, independent contractors, agency workers, volunteers, unpaid trainees, board members, shareholders, members of administrative, management or supervisory bodies and job applicants and all individuals who acquire information on relevant wrongdoings in a work-related context.

A disclosure under the 2014 Act is a disclosure of information which, in the reasonable belief of the individual making the disclosure, tends to show one or more of the following wrongdoings has been, is being or is likely to be committed:

(a) a criminal offence;

(b) a failure to comply with any legal obligation other than one arising under the contract of employment of the person making the disclosure;

(c) a miscarriage of justice;

(d) the endangering of the health and safety of any individual;

(e) damage to the environment;

(f) unlawful or improper use of funds or resources of a public body;

(g) an act or omission by or on behalf of a public body which is oppressive, discriminatory, grossly negligent or constitutes gross mismanagement;

(h) an act or omission that is unlawful or that defeats the object or purpose of certain rules of the European Union in the following areas:

  (1) public procurement;

  (2) financial services, products and markets, and the prevention of money laundering and terrorist financing;

  (3) product safety and compliance;

  (4) transport safety;

  (5) protection of the environment;

  (6) radiation protection and nuclear safety;

  (7) food and feed safety and animal health and welfare;

  (8) public health;

  (9) consumer protection;

  (10) protection of privacy and personal data, and security of network and information systems;

  or affects the financial interests of the European Union or the internal market; or

(i) the deliberate concealment of any of the above matters.

As stated in the Policy at Section 10.1, the Company will not disclose the reporting person's identity without their consent. The 2014 Act prohibits a person to whom a report is made or transmitted, without the explicit consent of the reporting person, from disclosing to another person the identity of the reporting person or any information from which the identity of the reporting person may be directly or indirectly deduced, other than such persons as the first-mentioned person reasonably considers may be necessary for the purposes of the receipt or transmission of, or follow-up on, reports as required under

the 2014 Act. However, the 2014 Act outlines scenarios where the identity of a reporting person may need to be disclosed:

(a) where the disclosure is a necessary and proportionate obligation imposed by law in the context of investigations or judicial proceedings, including with a view to safeguarding the rights of defence of others;

(b) where the person to whom the report was made took all reasonable steps to avoid disclosing the identity of the reporting person or reasonably believes that disclosing the identity of the reporting person or any such information is necessary for the prevention of serious risk to the security of the State, public health, public safety or the environment; or

(c) where the disclosure is required by law.

In these circumstances, the reporting person has a right to be notified, in writing, before their identity is disclosed, unless such notification would jeopardise:

(a) the effective investigation of the disclosure;

(b) the prevention of serious risk to security of the State, public health, public safety or the environment; or

(c) the prevention or prosecution of a crime.

As stated in the Policy at Section 7, the Company encourages you to identify yourself when making a protected disclosure, as proper investigation is likely to be more difficult or impossible if we cannot obtain further information from the reporting person. The Company will determine if anonymous reports will be investigated on a case by case basis. However, where a reporting person who makes a disclosure under this Policy by way of an anonymous report is subsequently identified, the reporting person will be afforded the protections under the 2014 Act, as amended.

How to Raise a Concern Internally

The persons authorised by the Group to receive reports are listed at Section 4 of the Policy. Under The 2014 Act, persons also have the option to make a report internally to their employing entity in Ireland, which can be done under this annexure by making a report internally in writing to the Group Head of Risk & Audit. This annexure sets out the internal reporting channels and procedures for the purposes of Section 6 of the 2014 Act.

The Group Head of Risk & Audit will acknowledge, in writing to the reporting person, the disclosure not more than 7 days after receipt of the disclosure.

Initial Assessment

Once a reporting person has made a report internally to their employing entity in Ireland, the Group Head of Risk & Audit will carry out an initial assessment to determine whether there is evidence that a relevant wrongdoing may have occurred. If necessary to make an initial assessment, the Group Head of Risk & Audit will seek further information from the reporting person.

If, having carried out the initial assessment, the Group Head of Risk & Audit decides that there is no evidence that a relevant wrongdoing may have occurred, the Group Head of Risk & Audit will close this procedure or, if it is clear that the concern falls more appropriately within a different policy or procedure of the Company, the reporting person will be informed that it should progress in accordance with that procedure. The Group Head of Risk & Audit will inform the reporting person, in writing, as soon as practicable, of the decision and the reasons for it.

Investigation and Outcome

If, having carried out an initial assessment, the Group Head of Risk & Audit decides that there is evidence that a relevant wrongdoing may have occurred, the Group Head of Risk & Audit may then appoint such person or persons (either internal or external to the Company) who is or are most appropriately placed to investigate the particular disclosure in question (the **Investigator(s)**). The scope and terms of reference of any investigation may be determined by the Company prior to any investigation being carried out.

The Group Head of Risk & Audit will provide feedback to the reporting person within a reasonable time, being not more than 3 months from the date the acknowledgement of receipt of the report was set to the reporting person. Feedback should include information on the progress of the investigation and its likely timescale. However, sometimes the need for confidentiality may prevent the Company from giving the reporting person specific details of the investigation or any action taken as a result. The reporting person should treat any information about the investigation as strictly confidential. Any breach of this confidentiality may result in disciplinary action up to and including dismissal.

Where the reporting person so requests in writing, the Group Head of Risk & Audit will provide further feedback at intervals of 3 months until such time as the procedure concerned is closed.

Other appropriate action that may be taken by the Company includes, but is not limited to, the following:

(a) changes to the way the Company conducts its operations;

(b) a decision to commence disciplinary proceedings under the Company's Disciplinary Procedure;

(c) referral of the matter for consideration under another of the Company's policies or procedures; and/or

(d) the making of a report to an appropriate third party, such as a regulatory body, State agency or An Garda Síochána.

It should be noted that fair and due process requires that any person accused of wrongdoing should be made aware of and given the opportunity to respond to any allegations made against them.

External Reporting Channels

A reporting person may make a disclosure to one of the prescribed persons listed in *Protected Disclosures Act 2014 (Disclosure to Prescribed Persons) Order* 2020. In general, prescribed persons have regulatory functions in the area which are the subject of the allegations. Examples are the Central Bank, The Health and Safety Authority and the Data Protection Commission. A full list of prescribed persons by sector is available on gov.ie.

A reporting person may make a disclosure to a prescribed person if the reporting person reasonably believes that the relevant wrongdoing is within the remit of the prescribed person and the information the reporting person discloses and any allegations in it are substantially true.

A reporting person may also make a disclosure to the Protected Disclosures Commissioner if the reporting person reasonably believes that the relevant wrongdoing falls within the description of matters in respect of which the prescribed person by reason of the nature of their responsibilities or functions appear appropriate to be the recipient of the disclosure and that the information disclosed, and any allegation contained in it, are substantially true. A reporting person may make a disclosure to a prescribed person or the Protected Disclosures Commissioner if the reporting person reasonably believes that the information disclosed, and any allegation contained in it, are substantially true.

Protection and Support for Persons Making a Disclosure

If a reporting person makes a protected disclosure, they are protected by Irish law against dismissal or any form of detrimental treatment or penalisation as a result of raising a concern.

Annexure 5 – New Zealand

Under New Zealand law, including the *Protected Disclosures (Protection of Whistleblowers) Act 2022* (NZ) (the **Act**), legislative protections are available to '**disclosers**' who make a '**protected disclosure'** of '**serious wrongdoing**'.

Disclosers who have protections under the Act include current and former employees, homeworkers (defined in the *Employment Relations Act 2000* (NZ)), secondees, contractors, persons concerned in the management of the Group and volunteers.

Protected disclosures

To be a '**protected disclosure'** qualifying for protection under the Act, the discloser must:

- believe on reasonable grounds that there is, or has been, serious wrongdoing in or by the Group; and
- disclose information about that in accordance with the Act; and
- not disclose information in bad faith.

'**Serious wrongdoing**' includes any act, omission, or course of conduct in (or by) any organisation that is one or more of the following:

- an offence;
- a serious risk to:
  - public health;
  - public safety;
  - the health or safety of any individual; or
  - the environment;
- an unlawful, corrupt, irregular or grossly negligent use of public funds or public resources;
- a serious risk to the maintenance of law, including:
  - the prevention, investigation and detection of offences; or
  - the right to a fair trial;
- oppressive, unlawfully discriminatory, grossly negligent, or that constitutes gross mismanagement, and is done (or is an omission) by:
  - an employee (if the organisation is a public sector organisation); or
  - a person performing (or purporting to perform) a function or duty or exercising (or purporting to exercise) a power on behalf of a public sector organisation or the Government.

Annexure 6 – United Kingdom

Under UK law, namely the *Employment Rights Act 1996* (the **ERA**) as amended by the *Public Interest Disclosure Act 1998*, there is legislative protection for workers who make protected disclosures.

Who does this Policy apply to?

The protections in the ERA apply to 'workers', which is a concept defined in the ERA. This means, in addition to the categories of individuals listed under "Who does this Policy apply to?" in the main body of the Policy, the legislative protections apply to all workers within the Group, including interns, casual workers and agency workers.

Personnel responsible for this Policy

The firm has a Whistleblowers' Champion with responsibility for ensuring and overseeing the integrity, independence and effectiveness of the firm's policies and procedures on whistleblowing, who can be contacted at Justin.Engelbrecht@tysers.com. The Whistleblowers' Champion will review this policy from a legal and operational perspective from time to time and at least once a year will prepare reports to the board of the Tysers Insurance Brokers Limited, and provide reporting support to the Company, on the operation and effectiveness of the firm's whistleblowing systems and controls. The Whistleblowers' Champion is not responsible for the day-to-day operation of the policy.

All staff are responsible for the success of this policy and should ensure that they use it to disclose any suspected danger or wrongdoing. Staff are invited to comment on this policy and suggest ways in which it might be improved. Comments, suggestions and queries should be addressed to the Head of Legal, Tysers.

Protection from detriment

An individual who makes a 'protected disclosure' (as explained below) must not suffer any detrimental treatment as a result of doing so. Detrimental treatment includes dismissal, disciplinary action, threats or other unfavourable treatment or omission connected with making a protected disclosure.

Protected disclosure

To be a **'protected disclosure'** qualifying for protection under the ERA, the Eligible Whistleblower must make a 'qualifying disclosure' to one of the of the categories of people prescribed by sections 43C – 43H of the ERA. Depending on the category of person to which the 'qualifying disclosure' is made, there may be certain additional requirements in order for the Eligible Whistleblower to be protected.

Where the Eligible Whistleblower is a worker of the Group and the disclosure is made to the worker's employer, the disclosure will be a 'protected disclosure' if it is a report of information made in the reasonable belief that it is in the public interest, which the Eligible Whistleblower reasonably believes tends to show one or more of the following:

(e) that a criminal offence has been committed, is being committed or is likely to be committed;

(f) that a person has failed, is failing or is likely to fail to comply with any legal obligation to which they are subject;

(g) that a miscarriage of justice has occurred, is occurring or is likely to occur;

(h) that the health or safety of any individual has been, is being or is likely to be endangered;

(i) that the environment has been, is being or is likely to be damaged; or

(j) that information tending to show any matter falling within any one of the proceedings categories above has been, or is likely to be, deliberately concealed.

There is no need for there to be proof that a breach or failure has occurred or is likely to occur. A reasonable suspicion will suffice.

You should make a report if you have a suspicion that any misconduct set out above has taken place, is taking place, or is about to take place. You do not need to be certain of this to report it and should not normally investigate it yourself, but you must have a genuine suspicion with a factual basis and must report it honestly.

The requirement for the report to be in the public interest means that complaints relating to your own personal circumstances may not be a qualifying disclosure. In those cases, you should speak to your line manager or the Human Resources team or raise the issue using the Grievance Procedure. It may be appropriate to use this policy after such alternative routes have been exhausted, in relation to the effectiveness or efficiency of those routes. If you are uncertain whether something is within the scope of this Policy, you should contact the Head of Legal, Tysers.

External whistleblowing

We strongly encourage you to report concerns internally first, in line with this Policy. However, this Policy does not affect your right to raise 'reportable concerns' directly with the relevant UK regulator, the Financial Conduct Authority (the **FCA**) or raise 'qualifying disclosures' in accordance with the ERA.

A 'reportable concern' is a concern held by any person in relation to the activities of a firm, including:

(k) anything that would be the subject-matter of a protected disclosure (as defined above);

(l) a breach of relevant policies and procedures; and

(m) behaviour that harms or is likely to harm the reputation or financial well-being of the relevant UK entities regulated by the FCA.

You can raise reporting concerns without first making an internal report under this Policy, and disclosures to the FCA can be in addition to reporting under this Policy either simultaneously or consecutively. It is not necessary for a disclosure to be made to the Group in the first instance. Details for contacting the FCA are as follows:

Financial Conduct Authority (FCA)	Telephone: +44 (0)20 7066 9200 Email: whistle@fca.org.uk Address: Intelligence Department (Ref PIDA) Financial Conduct Authority, 12 Endeavour Square, London, E20 1JN Website: fca.org.uk/firms/whistleblowing

Please be aware that a wider range of disclosures can be made under this Policy than are 'protected disclosures' under employment legislation or are 'reportable concerns' for the purpose of the FCA. Therefore, not all reportable concerns or disclosures will be

protected disclosures under UK employment legislation. If you are uncertain whether something is within the scope of this Policy or within the protection provided by UK employment legislation, you can seek guidance from Head of Legal, Tysers or Protect, a leading independent charity providing information and advice, which operates a confidential helpline. Protect's contact details are as follows:

Whistleblowing Advice Line – 020 3117 2520

UK advice line – info@protect-advice.org.uk

Investigation and outcome

Sometimes the need for confidentiality may prevent us giving you specific details of the investigation or the outcome (including any disciplinary action taken as a result). You should treat any information about the investigation or any outcome as confidential.

While we cannot always guarantee the outcome you are seeking, we will try to deal with your concern fairly and in an appropriate way. By using this Policy you can help us to achieve this. If you are not happy with the way in which your concern has been handled, you can raise it with an alternative Recipient. Alternatively you may contact the Whistleblowing Champion.