

Whistleblower Policy

Who can make a protected disclosure, what can be reported, who can receive it, how the discloser is protected and supported, and how disclosures are handled, investigated and reported. Ready to adapt for your organisation.

Version 1.0 · October 2026 · Free template from Risk Frameworks Australia (riskfa.com) · No membership or sign-up

How to use this industry policy. Adopt the structure, terms and protections as written: they follow the *Corporations Act 2001* and ASIC Regulatory Guide 270, so that your organisation speaks the same language as the rest of the industry and as the regulators. Fill in the text in [square brackets] with your organisation's details, including your eligible recipients and disclosure channels, add examples of wrongdoing that fit your business, and approve the Policy through your governance process. Legal requirements are summarised as at October 2026: confirm the current requirements that apply to your organisation before relying on them. This template is general information only, provided free of charge, and is used at your own risk (see the disclaimer at the end).

Document control

Item	Detail
Document	Whistleblower Policy
Organisation	[Organisation name] and its related bodies corporate [list]
Document owner	[General Counsel / Head of Compliance]
Approved by	[Board], on the recommendation of the [Board Audit Committee / Board Risk Committee]
Version / date approved	[1.0] / [date]
Review cycle	At least every [2 years] (RG 270.158), and after any change in the law or a significant matter
Where this Policy is published	[Intranet link] ; [external website link]

1. Purpose

[Organisation] wants to know about wrongdoing as early as possible, so that it can be stopped and fixed. This Policy:

- encourages people to speak up about misconduct or an improper state of affairs, and explains how;
- explains the legal protections available to whistleblowers and how [Organisation] will protect and support them;
- ensures disclosures are dealt with properly, confidentially and on time;
- ensures people mentioned in a disclosure are treated fairly;
- supports [Organisation]'s values, code of conduct and risk management framework; and
- meets [Organisation]'s legal obligations, including *Corporations Act 2001* s1317AI.

Speaking up is valued. No one at [Organisation] will be disadvantaged for raising a genuine concern under this Policy.

2. Legal framework and who must have this Policy

The *Corporations Act 2001* Part 9.4AAA (ss1317AA–1317AK) gives protection to whistleblowers who disclose misconduct about companies, banks, insurers, superannuation entities and other regulated entities (s1317AAB). The *Taxation Administration Act 1953* Part IVD (ss14ZZT–14ZZZE) gives similar protection for disclosures about tax affairs. The protections apply to any qualifying disclosure, whether or not the entity is required to have a policy (RG 270.4).

Entity	Requirement (s1317AI, as at October 2026)
Public company (including listed companies)	Must have a whistleblower policy with the s1317AI(5) content and make it available to officers and employees (s1317AI(1); RG 270.5).
Large proprietary company	Must do the same from 6 months after the end of the first financial year in which it is a large proprietary company (s1317AI(2); RG 270.8). A proprietary company is large if it meets at least two of: consolidated revenue of \$50 million or more, consolidated gross assets of \$25 million or more, or 100 or more employees (s45A(3); Corporations Regulations reg 1.0.02B).

Entity	Requirement (s1317AI, as at October 2026)
Proprietary company that is trustee of a registrable superannuation entity	Must have and make available the policy (s1317AI(3); RG 270.9).
Public company limited by guarantee, not-for-profit, not an RSE trustee, consolidated revenue under \$1 million	Relieved from s1317AI(1) (<i>ASIC Corporations (Whistleblower Policies) Instrument 2019/1146</i> ; RG 270.20).
Other entities	No policy required, but the protections still apply. This Policy is good practice (RG 270.10).

Failing to have and make available a required policy is an offence of strict liability (s1317AI(1)–(4), s1311(1); RG 270.24). In a claim for compensation, a court may consider the extent to which an employer gave effect to its whistleblower policy (s1317AE(3)(b); RG 270.27).

2.1 Where this Policy meets s1317AI(5)

s1317AI(5) requires information about	Section of this Policy
(a) the protections available to whistleblowers, including under Part 9.4AAA	4, 5, 6 and 9
(b) to whom qualifying disclosures may be made, and how	7 and 8; Appendix B
(c) how [Organisation] will support whistleblowers and protect them from detriment	10 and 11
(d) how [Organisation] will investigate qualifying disclosures	12 and 13; Appendices A and C
(e) how [Organisation] will ensure fair treatment of employees mentioned in, or the subject of, qualifying disclosures	14
(f) how this Policy is made available to officers and employees	18
(g) any matters prescribed by regulations	None prescribed as at October 2026

RG 270 also expects the Policy to cover the tax whistleblower protections in Part IVD of the *Taxation Administration Act 1953* (RG 270.12). They are included throughout.

3. Key definitions

Term	Meaning
Discloser	A person who makes, or may make, a disclosure under this Policy.
Eligible whistleblower	A person who can qualify for protection (section 4; s1317AAA; tax: s14ZZU).
Disclosable matter	Information about misconduct or an improper state of affairs that can qualify for protection (section 5; s1317AA(4)–(5)).
Eligible recipient	A person who can receive a disclosure that qualifies for protection (section 7; s1317AAC; tax: s14ZZV).
Qualifying disclosure	A disclosure that qualifies for protection under Part 9.4AAA or Part IVD.
Misconduct	Includes fraud, negligence, default, breach of trust and breach of duty (Corporations Act s9; RG 270.52).
Detriment	Includes dismissal, injury in employment, a disadvantageous change of position or duties, discrimination, harassment or intimidation, harm or injury including psychological harm, and damage to property, reputation, business or financial position, or any other damage (s1317ADA).
Personal work-related grievance	A grievance about the discloser's own employment that has implications for them personally, as defined in s1317AADA(2) (section 6).
Whistleblower Protection Officer (WPO)	The person responsible for protecting and supporting disclosers and the integrity of this Policy (RG 270.145(d)): [name / role] .
Whistleblower Investigation Officer (WIO)	The person responsible for arranging and overseeing investigations (RG 270.145(e)): [name / role] .
Senior manager	A person other than a director or secretary who makes, or participates in making, decisions that affect the whole or a substantial part of the business, or who has the capacity to significantly affect its financial standing (s9).

4. Who can make a protected disclosure

You are an **eligible whistleblower** if you are, **or have been**, any of the following in relation to **[Organisation]** (s1317AAA; RG 270.43):

- an officer (for example a director or company secretary) or an employee, including permanent, part-time, fixed-term and temporary staff, interns and secondees;
- an individual who supplies goods or services to **[Organisation]**, paid or unpaid (for example contractors, consultants, service providers), or an employee of such a supplier;
- an associate of **[Organisation]**; or
- a relative, dependant or spouse of any of the above, or a dependant of their spouse.

For a superannuation entity, eligible whistleblowers also include current and former trustees, custodians and investment managers of the entity, officers and employees of a corporate trustee, custodian or investment manager, their suppliers and suppliers' employees, and relatives and dependants of those people (s1317AAA(f)–(h); RG 270.44).

The tax whistleblower provisions cover a similar group: current and former officers, employees, suppliers and their employees, associates, and their spouses, children and dependants (*Taxation Administration Act 1953* s14ZZU).

A discloser qualifies for protection if they are an eligible whistleblower and they disclose a **disclosable matter** (section 5) to an **eligible recipient** (section 7), or to ASIC, APRA or another prescribed Commonwealth body; or they make a disclosure to a lawyer to get legal advice or representation about the whistleblower provisions; or they make a public interest or emergency disclosure that meets the legal conditions (s1317AA, 1317AAD; RG 270.45).

5. What can be reported: disclosable matters

A disclosable matter is information that you have **reasonable grounds to suspect** concerns misconduct, or an improper state of affairs or circumstances, in relation to **[Organisation]** or a related body corporate (s1317AA(4)). Without limiting that, it includes information that **[Organisation]** or a related body corporate, or any of their officers or employees, has engaged in conduct that (s1317AA(5)):

- is an offence against, or a contravention of, the *Corporations Act 2001*, *ASIC Act 2001*, *Banking Act 1959*, *Financial Accountability Regime Act 2023*, *Financial Sector (Collection of Data) Act 2001*, *Insurance Act 1973*, *Life Insurance Act 1995*, *National Consumer Credit Protection Act 2009* or *Superannuation Industry (Supervision) Act 1993*, or an instrument made under any of them;

- is an offence against any other Commonwealth law punishable by imprisonment for 12 months or more; or
- represents a danger to the public or the financial system.

Disclosable matters can include conduct that is not against a particular law, such as business practices that may cause consumer harm or a systemic issue a regulator should know about (RG 270.52, RG 270.56).

Type of wrongdoing	Examples relevant to [Organisation] (adapt to your business)
Fraud, theft, bribery or corruption	Misappropriation of customer or member money; offering or accepting bribes or secret commissions; falsifying records.
Customer harm and conduct	Selling products to customers they are not suitable for; charging fees for no service; misleading advertising or disclosure; hiding errors that have caused customer loss.
Regulatory breaches	Failing to report breaches, incidents or reportable situations to ASIC or APRA; breaches of licence conditions, prudential standards, AML/CTF obligations or privacy law.
Financial reporting and tax	Manipulating accounts, reserves, unit prices or performance figures; tax evasion or improper tax arrangements.
Risk and safety	Concealing a serious information security incident; conduct that is a danger to the public or the financial system.
Retaliation	Detriment, or threats of detriment, against someone who has made, or is thought to have made or be planning, a disclosure.

- 'Reasonable grounds to suspect' is an objective test. Your motive does not affect protection. You do not need proof, but a bare allegation with no supporting information is unlikely to meet the test (RG 270.53).
- **You are still protected if your disclosure turns out to be incorrect** (RG 270.57).
- Tax matters: a disclosure to an eligible recipient under the tax provisions is protected if you have reasonable grounds to suspect the information indicates misconduct or an improper state of affairs in the tax affairs of **[Organisation]** or an associate, and you consider it may assist the recipient in relation to those tax affairs (s14ZZT(2)). Disclosures to the Commissioner of Taxation or the Tax Practitioners Board are covered by s14ZZT(1) and (1A).
- **[Organisation]** discourages deliberately false reports, made knowing they are untrue. A

report you know to be untrue is unlikely to meet the 'reasonable grounds to suspect' test, and may lead to disciplinary action. This does not apply to a disclosure you genuinely suspect is true but cannot prove (RG 270 good practice tip 4).

6. What is not covered: personal work-related grievances

Disclosures that relate **solely** to a personal work-related grievance, and do not concern detriment or a threat of detriment to you, do not qualify for protection under the Corporations Act (s1317AADA(1); RG 270.58). A personal work-related grievance concerns your current or former employment and has implications for you personally, but does not have significant implications for [Organisation] beyond you and does not concern a disclosable matter in s1317AA(5) (s1317AADA(2)). Examples include:

- an interpersonal conflict between you and another employee;
- a decision about your engagement, transfer or promotion;
- a decision about the terms and conditions of your engagement; and
- a decision to suspend or terminate your engagement, or otherwise discipline you.

A grievance **may still be protected** if it is mixed with information about misconduct; if it concerns a breach of employment or other laws punishable by 12 months' imprisonment or more, a danger to the public, or misconduct beyond your own circumstances; if you suffer or are threatened with detriment for making a disclosure; or if you disclose it to a lawyer for advice about the whistleblower protections (RG 270.63; s1317AA(3)).

Personal work-related grievances should be raised under the [Grievance Policy] with [HR contact]. They may be protected under other laws, such as the *Fair Work Act 2009* (RG 270.49). Other concerns that are not disclosable matters can be raised with your manager or through [speak-up channel], but those reports do not attract the legal whistleblower protections.

7. Who can receive a disclosure

To qualify for protection you must make your disclosure **directly** to one of the people or bodies below (RG 270.67). [Organisation] encourages you to make disclosures to one of our internal or external eligible recipients first, so that we can act quickly, but you can go directly to a regulator and still be protected (RG 270 good practice tip 5). If you want more information before making a disclosure, contact the WPO at [contact] or an independent lawyer (RG 270.66).

7.1 Eligible recipients within [Organisation]

Eligible recipient (s1317AAC(1))	At [Organisation] (see Appendix B)
An officer or senior manager of [Organisation] or a related body corporate	Directors, the company secretary and members of the [executive team]
An auditor, or a member of an audit team, of [Organisation] or a related body corporate (internal or external, RG 270.68 note)	[External auditor firm and audit partner] ; [Head of Internal Audit]
An actuary of [Organisation] or a related body corporate	[Appointed Actuary]
A person authorised by [Organisation] to receive disclosures	The WPO; [nominated Whistleblower Disclosure Officers] ; [Independent whistleblower service provider: name, phone, web]

For a superannuation entity, eligible recipients are its officers, auditors and actuary, an individual trustee, a director of the corporate trustee, and a person authorised by the trustee (s1317AAC(2); RG 270.69).

For tax disclosures, eligible recipients include the auditor, a registered tax agent or BAS agent providing services to [Organisation], a director, secretary or senior manager, any employee or officer with functions or duties relating to [Organisation]'s tax affairs, a person authorised by [Organisation], and the Inspector-General of Taxation (s14ZZV; *Taxation Administration Regulations 2017* s13A).

7.2 Legal practitioners

A disclosure to a legal practitioner for the purpose of obtaining legal advice or legal representation about the whistleblower provisions is protected, even if the lawyer concludes it is not about a disclosable matter (s1317AA(3); s14ZZT(3); RG 270.72). Under the tax provisions only, a disclosure to a medical practitioner or psychologist for care, treatment or counselling is also protected (s14ZZT(3B)).

7.3 Regulators

You can disclose directly to **ASIC** or **APRA**, or another Commonwealth body prescribed by regulation (none was prescribed as at October 2026), and be protected (s1317AA(1); RG 270.73). Tax disclosures can be made to the **Commissioner of Taxation** (ATO) or, for matters within its functions, the **Tax Practitioners Board** (s14ZZT(1), (1A)). See ASIC Information Sheet 239 *How ASIC handles whistleblower reports* and the ATO's tax whistleblower guidance.

7.4 Public interest and emergency disclosures

In limited circumstances you can disclose to a member of the Commonwealth, a state or a territory parliament, or to a professional journalist (as defined in the Corporations Act), and be protected. **You must first have made a disclosure to ASIC, APRA or a prescribed body; disclosures to [Organisation] alone are not enough** (s1317AAD; RG 270.74–RG 270.77). [Organisation] strongly recommends you get independent legal advice before making one (RG 270.78).

Condition	Public interest disclosure (s1317AAD(1))	Emergency disclosure (s1317AAD(2))
Previous disclosure	Made to ASIC, APRA or a prescribed body and qualified for protection	Made to ASIC, APRA or a prescribed body and qualified for protection
Time	At least 90 days have passed since the previous disclosure	No waiting period
Your belief	No reasonable grounds to believe action is being, or has been, taken; and reasonable grounds to believe a further disclosure is in the public interest	Reasonable grounds to believe the information concerns a substantial and imminent danger to the health or safety of one or more people or to the natural environment
Written notice	After the 90 days, written notice to the body you disclosed to, identifying the previous disclosure and stating that you intend to make a public interest disclosure	Written notice to the body you disclosed to, identifying the previous disclosure and stating that you intend to make an emergency disclosure
Extent	No more information than necessary to inform the recipient of the misconduct or improper state of affairs	No more information than necessary to inform the recipient of the danger

8. How to make a disclosure

You can make a disclosure at any time, in person, by phone, in writing or online, during or outside business hours, and you can do so **anonymously** (RG 270.80, RG 270.83).

Channel	Details
Independent whistleblower service (24/7, anonymous option)	[Provider name] ; phone [number] ; web [link] ; email [address] . You can receive updates and answer questions while staying anonymous.
Whistleblower Protection Officer	[Name / role] ; phone [number] ; email [confidential address] ; post [marked 'Private and confidential — addressee only']
Other eligible recipients	As listed in Appendix B (for example a director, executive, the Head of Internal Audit, or the external auditor).
Regulators	ASIC [link] ; APRA [link] ; ATO tax whistleblowers [link]

- Include as much as you can: what happened, when and where, who was involved, how you know, and any documents or other evidence. You do not need to have all the details.
- **Anonymity:** you can remain anonymous when making the disclosure, during the investigation and afterwards, and you can refuse to answer questions that you think could reveal your identity. Anonymous disclosures are still protected (s1317AA(5) note; RG 270.83–RG 270.84). An anonymous email address or a pseudonym can be used. Keeping a two-way channel open (for example through the independent service) helps us ask follow-up questions and keep you informed.
- Do not investigate the matter yourself or collect information you are not entitled to access.

9. Legal protections for disclosers

These protections apply to qualifying disclosures made internally, to lawyers, to regulators, and to public interest and emergency disclosures made in line with the law (RG 270.89).

9.1 Identity protection (confidentiality)

- It is illegal for a person who obtained the information because of the disclosure to disclose your identity, or information likely to lead to your identification, unless an exception applies (s1317AAE(1); tax: s14ZZW). Under the Corporations Act this is an offence and a civil penalty provision; under the tax provisions it is an offence.
- The exceptions are disclosure to ASIC, APRA or a member of the Australian Federal Police; to a lawyer for advice or representation about the whistleblower provisions; to a person or body prescribed by regulation; or **with your consent** (s1317AAE(2)). For tax disclosures, the exceptions are disclosure to the Commissioner of Taxation, a member of the Australian Federal Police, a lawyer for advice or representation about the tax whistleblower provisions, the Inspector-General of Taxation, the Tax Practitioners Board or the ACNC Commissioner (prescribed), or with your consent (s14ZZW(2); *Taxation Administration Regulations 2017* s13B).
- Information that could identify you may be disclosed without your consent only if it does not include your identity, is reasonably necessary to investigate the matter, and all reasonable steps are taken to reduce the risk that you will be identified (s1317AAE(4); RG 270.93).
- You cannot generally be required to disclose your identity, or produce documents that identify you, to a court or tribunal (s1317AG).
- If you think your confidentiality has been breached, tell the WPO or **[Chair of the Board Audit Committee]**. You can also complain to ASIC, APRA or the ATO (RG 270.94).

9.2 Protection from detriment

- No person may cause, or threaten to cause, detriment to you or anyone else because they believe or suspect that a person has made, may have made, proposes to make or could make a qualifying disclosure (s1317AC(1)–(2); tax: s14ZZY). A threat can be express or implied, conditional or unconditional, and you do not need to have actually feared it would be carried out (s1317AC(4)–(5)).
- Officers and employees involved in a company's contravention also contravene the law (s1317AC(3)). These are offences and civil penalty provisions.
- Reasonable administrative action to protect you (for example moving you to another location to prevent detriment), and managing unsatisfactory performance in line with the **[Performance Management Policy]**, are not detrimental conduct. **[Organisation]** will explain the reasons for any such action (RG 270.100–RG 270.101).

9.3 Compensation and other remedies

- You, or any other person, can seek compensation and other remedies through the courts if you suffer loss, damage or injury because of detrimental conduct, including where [Organisation] failed to take reasonable precautions and exercise due diligence to prevent it (s1317AD, s1317AE; RG 270.102; tax: s14ZZZ, s14ZZZA).
- Courts can order compensation (from the person, the employer, or both), an injunction, an apology, reinstatement, exemplary damages or any other order the court thinks appropriate (s1317AE(1)).
- Once you point to evidence suggesting a reasonable possibility of detrimental conduct, the other party must prove the claim is not made out (s1317AD(2B)).
- You can be ordered to pay costs only if you brought the proceedings vexatiously or without reasonable cause, or your unreasonable act or omission caused the costs (s1317AH).
- [Organisation] encourages you to seek independent legal advice (RG 270.103).

9.4 Civil, criminal and administrative liability protection

- You are not subject to any civil, criminal or administrative liability (including disciplinary action) for making a qualifying disclosure, and no contractual or other remedy may be enforced against you on the basis of the disclosure (s1317AB(1)(a)–(b); tax: s14ZZX).
- You have qualified privilege in respect of the disclosure, and a contract you are party to cannot be terminated because the disclosure breaches it (s1317AB(2)).
- For disclosures to ASIC, APRA or a prescribed body, and public interest or emergency disclosures, the information is not admissible in evidence against you in criminal proceedings or proceedings for a penalty, other than about the falsity of the information (s1317AB(1)(c)). For tax disclosures, this applies to disclosures to the Commissioner of Taxation or the Tax Practitioners Board (s14ZZX(1)(c)).
- **These protections do not give immunity for any misconduct you were involved in that is revealed by your disclosure** (s1317AB(1) note; RG 270.105).

10. How [Organisation] protects confidentiality in practice

[Organisation] will (RG 270.108):

- redact your name, role and other identifying details from records and investigation documents, and refer to you in a gender-neutral way;
- where possible, check with you which parts of your disclosure could identify you;
- limit access to disclosure information to those directly involved in handling and

investigating it, and tell only a restricted number of people your identity (with your consent);

- store all paper and electronic records securely, in a restricted [case management system]; and not send documents to shared printers or email addresses others can access;
- remind everyone involved that unauthorised disclosure of your identity may be a criminal offence; and
- have disclosures handled and investigated by trained staff.

In practice, people may still guess your identity, for example if you have told others you were thinking of making a disclosure, if very few people had access to the information, or if the information was told to you privately (RG 270 good practice tip 8). The WPO will discuss this with you.

11. Support and protection from detriment in practice

- **Risk assessment:** as soon as possible after receiving a disclosure, the WPO assesses the risk of detriment to you and to others (for example colleagues who might be suspected of making it), by identifying who might have a motive, analysing likelihood and severity, putting controls in place, and monitoring the risk during and after the investigation. The assessment is recorded (RG 270.109; good practice tip 9).
- **Support:** access to the [Employee Assistance Program], counselling and other professional support, and a contact person for updates.
- **Practical protection:** where needed, working from another location, reassignment to another role at the same level, changes to how you work, or reassignment or relocation of other staff involved.
- **Managers:** managers are reminded of their duties to keep matters confidential, address risks of isolation or harassment, manage conflicts and ensure fairness when managing your performance.
- **If detriment occurs:** tell the WPO. A complaint about detriment is investigated as a separate matter by someone not involved in the original disclosure, and the findings are reported to the [Board Audit Committee]. Interventions may include disciplinary action against the person responsible, extended leave, a career development plan, or compensation or other remedies.
- You can also seek independent legal advice, or contact ASIC, APRA or the ATO, if you believe you have suffered detriment (RG 270.110).

12. Handling a disclosure

Step	What happens	Target timeframe
1. Receive	The eligible recipient records the disclosure with only the information needed, and passes it to the WPO with your consent to share your identity, or without identifying details . Recipients must not investigate or tell anyone else.	Passed to the WPO within [1 business day]
2. Acknowledge	The WPO acknowledges receipt (including through anonymous channels) and explains this Policy, confidentiality and support.	Within [2 business days]
3. Protect	Detriment risk assessment and support plan (section 11).	Within [5 business days]
4. Assess	The WPO assesses whether the disclosure qualifies for protection and whether a formal investigation is needed (RG 270.116). Where it is unclear, [Organisation] treats the discloser as protected (RG 270 good practice tip 11).	Within [10 business days]
5. Escalate and notify	Serious matters are escalated (below). Compliance assesses any regulatory notification obligations, for example a reportable situation to ASIC, an APRA notification or an AUSTRAC report, under the RiskFA Incident & Issues Management Standard. Notifications must not identify the discloser unless the law permits it.	Immediately for serious matters; reportability decision within the Standard's timeframes
6. Investigate or resolve	Investigation (section 13), or another appropriate response if an investigation is not needed, with reasons recorded.	Target completion within [60–90 days] of receipt
7. Close	Findings documented and reported; the discloser told the outcome where appropriate; issues and actions raised for any control failures; records secured.	Within [10 business days] of the findings

- **Escalation:** a disclosure about a director, the CEO, the Chair or a member of the executive is referred directly to the [Chair of the Board Audit Committee], not to management. A disclosure that may involve a serious offence, a danger to the public or the financial system, or a material risk to [Organisation] is reported to the [Chair of the Board Audit Committee] within [24 hours], without identifying the discloser.
- Focus on the substance of the disclosure, not the discloser's motive. Matters that appear personal may point to a wider problem, for example a culture of bullying (RG 270

good practice tip 11).

- A whistleblower disclosure is also recorded as an incident or issue in the register under the Incident & Issues Management Standard, with no information that could identify the discloser.

13. Investigating a disclosure

- **Scope and lead:** the WIO decides the nature and scope of the investigation, who will lead it (internal, external, or jointly with an external investigation firm), what technical, financial or legal advice is needed, and the timeframe (RG 270 good practice tips 12 and 13).
- **Independence:** investigations are objective, fair and independent of the discloser, the people who are the subject of the disclosure and the business unit involved. No one investigates a matter in which they have a conflict of interest.
- **Confidentiality:** information likely to identify the discloser is not shared without consent unless the s1317AAE(4) conditions are met (RG 270.118). Legal professional privilege is considered where [General Counsel] directs.
- **Anonymous disclosures:** [Organisation] will investigate as far as it can on the information provided. It may be unable to investigate fully if it cannot contact the discloser (RG 270.119–RG 270.120).
- **Evidence:** evidence is gathered and preserved properly; interviews are documented; findings are based on the balance of probabilities and the evidence.
- **Updates:** the discloser receives regular updates where they can be contacted, at least when the investigation starts, while it is in progress [every 4 weeks], and when it is finalised (RG 270.121–RG 270.122). Anonymity is protected when giving updates.
- **Findings:** the investigator reports findings in writing (Appendix C) to the WIO and, for serious matters, to the [Board Audit Committee], without identifying the discloser (RG 270.123). The discloser is told the outcome, although it may not always be appropriate to give full details, for example for privacy or legal reasons (RG 270.124).
- **Review:** a discloser who is not satisfied may ask for a review of whether this Policy was followed. The review is done by an officer not involved in the original handling, and the findings go to the [Board Audit Committee]. [Organisation] is not required to reopen an investigation if it was conducted properly and there is no new information that would change the findings (RG 270 good practice tip 14). The discloser can also complain to ASIC, APRA or the ATO.
- **Outcomes:** substantiated wrongdoing leads to action: disciplinary action under the RiskFA Consequence Management Framework, customer remediation under the RiskFA Customer Remediation Policy, fixing control weaknesses as issues under the Incident & Issues Management Standard, and regulatory notification where required.

14. Fair treatment of people mentioned in a disclosure

[Organisation] will ensure fair treatment of employees who are mentioned in a disclosure or who are its subject (s1317AI(5)(e); RG 270.125–RG 270.127). In particular:

- disclosures are handled confidentially, as far as practical;
- each disclosure is assessed and may be investigated; the purpose of an investigation is to find whether there is enough evidence to substantiate or refute the matters reported;
- investigations are objective, fair and independent, and no conclusion is reached before the evidence is assessed;
- an employee who is the subject of a disclosure is told about the matters raised, as required by natural justice and procedural fairness, and is given a chance to respond **before any adverse finding is made or action taken**. The timing may be later where telling them earlier could compromise the investigation (for example a risk of destroying evidence, or a referral to ASIC, APRA, the ATO or police);
- they may access the [Employee Assistance Program] and other support; and
- no action is taken against them on the basis of an unproven allegation.

15. Roles and responsibilities

Role	Responsibilities
Board	Ultimately responsible for this Policy as part of the risk management and governance framework; ensures trends and themes from disclosures are addressed (RG 270.14).
[Board Audit Committee / Board Risk Committee]	Recommends this Policy to the Board; receives reporting (section 17); receives serious matters and matters about senior executives directly; oversees investigations of detriment complaints and reviews.
Chair of the [Board Audit Committee]	Escalation point for disclosures about directors, the CEO or executives; the WPO and WIO can escalate directly to the Chair (RG 270.146).
CEO and executive team	Demonstrate commitment to speaking up: take disclosures seriously, act on them promptly and support disclosers (RG 270.141).
Whistleblower Protection Officer	Owns the protection and support of disclosers; first contact for advice; detriment risk assessments; confidentiality; monitors the discloser's welfare; independent of the business line concerned.
Whistleblower Investigation Officer	Assesses and arranges investigations; appoints investigators; ensures fairness, independence and timeliness; reports findings.
Eligible recipients (including all officers and senior managers)	Recognise a disclosure, receive it confidentially, pass it to the WPO as this Policy requires, and do not investigate or reveal the discloser's identity.
People and Culture (HR) and Legal	Assist with investigations, support measures, privilege and employment law; keep grievance processes separate.
Line managers	Promote a speak-up culture; refer any disclosure they receive; never ask who made a disclosure; prevent detriment.
All staff and contractors	Report suspected wrongdoing; cooperate with investigations; keep information confidential; never cause or threaten detriment.

16. Records, privacy and information security

- All disclosure records are kept in a secure, access-restricted [case management system], separate from general HR and incident records (RG 270.113, RG 270.147).
- Personal information is handled in line with the *Privacy Act 1988* and the Australian Privacy Principles; a breach of disclosure records is managed under the RiskFA Data Breach Response Plan (RG 270.148–RG 270.149).
- Records are kept for at least [7 years] after the matter is closed, or longer where required by law.
- Service providers that receive disclosures are bound by contract to the same confidentiality and security standards, and [Organisation] monitors them. [Organisation] remains responsible for outsourced functions (RG 270 good practice tip 6).

17. Reporting and monitoring effectiveness

The WPO reports to the [Board Audit Committee] at least [quarterly], without including anything likely to identify a discloser (RG 270.150–RG 270.157). Reports include:

- number of disclosures, by channel, type of matter, business unit and location, and the type of discloser (for example employee or supplier);
- status, action taken, outcome and time to finalise each disclosure, compared with the targets in section 12;
- time to acknowledge, assess and complete investigations, and frequency of communication with disclosers;
- detriment complaints and their outcomes, and breaches of confidentiality;
- themes, root causes and control weaknesses identified, and the actions taken; and
- the proportion of reports that are not disclosable matters (a high share suggests people are unsure what or where to report).

[Organisation] also checks staff understanding of this Policy through [annual survey questions / sample interviews] (RG 270.155–RG 270.156).

18. Availability of this Policy and training

- This Policy is available to all officers and employees on [the intranet], in the [employee handbook], and in induction packs, and is promoted in [staff briefings] at least [annually] (s1317AI(1)(b), (5)(f); RG 270.128–RG 270.130).
- It is published on [Organisation]'s external website so that former employees, suppliers and others can use it, with internal-only details (such as names and direct numbers of internal recipients) removed if appropriate (RG 270.138–RG 270.139).
- All employees complete training on this Policy at induction and [annually] (RG 270.131).
- Managers receive training on handling disclosures and preventing detriment (RG 270.133).
- Eligible recipients, the WPO and the WIO receive specialist training, including on confidentiality and the prohibition on detriment (RG 270.134). External eligible recipients (such as the auditor and actuary) are told about their obligations (RG 270.135).
- People in overseas operations receive appropriate training, because disclosures to overseas recipients, or about overseas entities, may qualify for protection (RG 270.136).
- Changes to this Policy are communicated to all staff and recipients, with targeted training where procedures change (RG 270.137).

19. Review of this Policy and law reform

- This Policy is reviewed at least every [2 years] (RG 270.158), considering whether its scope suits the business, whether it is easy to understand, whether it reflects current law and good practice, and whether handling, protection and support need to improve (RG 270.159). Staff feedback is sought (RG 270.160).
- **Law reform (as at October 2026):** s1317AK requires a review of the operation of Part 9.4AAA and Part IVD of the *Taxation Administration Act 1953*. Proposals for a Whistleblower Protection Authority had not been enacted. From 4 December 2026 the definition of 'journalist' for public interest and emergency disclosures moves from s1317AAD(3) to s9 of the Corporations Act, with the same wording (*Treasury Laws Amendment (Strengthening Financial Systems and Other Measures) Act 2025*). Check for changes before each review.

20. Compliance with this Policy

Causing or threatening detriment to a discloser, breaching confidentiality, or deliberately making a false disclosure are serious breaches of this Policy and may lead to disciplinary action, up to termination of employment or engagement, under the RiskFA Consequence Management Framework. They may also be offences or civil penalty contraventions. Breaches are reported to the [\[Board Audit Committee\]](#) and, where relevant, considered in remuneration outcomes under the RiskFA Remuneration Policy (CPS 511 where it applies). This Policy does not form part of any employment contract.

21. Related documents

- [\[Code of Conduct\]](#) , [\[Grievance Policy\]](#) , [\[Bullying, Harassment and Discrimination Policy\]](#) , the RiskFA Consequence Management Framework
- RiskFA Incident & Issues Management Standard, RiskFA Customer Remediation Policy, RiskFA Data Breach Response Plan
- [\[Fraud and Corruption Control Policy\]](#) , [\[AML/CTF Program\]](#) , [\[Privacy Policy\]](#)
- Legislation: *Corporations Act 2001* Part 9.4AAA; *Taxation Administration Act 1953* Part IVD; *Taxation Administration Regulations 2017* Division 3A; *ASIC Corporations (Whistleblower Policies) Instrument 2019/1146*
- ASIC: RG 270 *Whistleblower policies*; INFO 239 *How ASIC handles whistleblower reports*; ATO tax whistleblower guidance; APRA guidance on making a disclosure to APRA
- Standards: ISO 37002:2021 *Whistleblowing management systems — Guidelines*

Appendix A. Disclosure handling workflow

1. **Disclosure received** by an eligible recipient, the independent service or the WPO.
Record date, channel and the matters raised. Ask for consent to share identity with the WPO; if not given, pass on only non-identifying information.
2. **Acknowledge** within [2 business days], through the discloser's chosen channel.
Explain confidentiality, protections, support and next steps.
3. **Detriment risk assessment** by the WPO within [5 business days]; agree a support plan; monitor throughout.
4. **Triage** within [10 business days]: Does it qualify for protection (eligible whistleblower, disclosable matter, eligible recipient)? Is it a personal work-related grievance only? If unsure, treat as protected. Does it involve a director or executive (refer to the Board Audit Committee Chair)? Does it need urgent action or regulatory notification?
5. **Decide the response**: formal investigation, other action (for example a targeted review), referral to another process with consent (for example a grievance), or no further action with documented reasons. Tell the discloser.
6. **Investigate** under section 13: terms of reference, independent investigator, evidence, procedural fairness for people mentioned, updates to the discloser every [4 weeks].
7. **Findings** documented (Appendix C) and reported to the WIO and, for serious matters, the Board Audit Committee, without identifying the discloser.
8. **Act**: discipline, customer remediation, control fixes (issues raised under the Incident & Issues Management Standard), regulatory notifications.
9. **Close**: tell the discloser the outcome where appropriate; reassess detriment risk; secure records; include in reporting.
10. **Review on request**: independent review of whether this Policy was followed.

Appendix B. Eligible recipients list template

Publish internal details on the intranet. The external website version may omit internal names and direct numbers (RG 270.139).

Recipient	Name and role	Contact (phone, email, address)	Covers
Independent whistleblower service	[Provider]	[Phone 24/7]; [web]; [email]	All matters, including anonymous and tax

Recipient	Name and role	Contact (phone, email, address)	Covers
Whistleblower Protection Officer	[Name, role]	[Confidential phone and email]	All matters
Whistleblower Disclosure Officer(s)	[Names, roles, locations]	[Contacts]	All matters
Chair of the [Board Audit Committee]	[Name]	[Confidential email]	All matters; required route for matters about directors or executives
Directors, company secretary and senior managers	[As listed in the officer register]	[Contacts]	All matters
Head of Internal Audit	[Name]	[Contacts]	All matters
External auditor	[Firm, audit partner]	[Contacts]	All matters, including tax
Appointed Actuary	[Name, firm]	[Contacts]	All matters
Tax: registered tax agent / BAS agent; officers with tax functions	[Names]	[Contacts]	Tax matters
Regulators	ASIC; APRA; ATO; Tax Practitioners Board; Inspector-General of Taxation (tax)	[Links to each regulator's whistleblower page]	As described in section 7

Appendix C. Investigation report template

The report must not include the discloser's identity or information likely to identify them, unless the discloser has consented or the law permits.

Section	Content
---------	---------

Section	Content
1. Reference and classification	Case reference (not the discloser's name); date received; channel; confidentiality and privilege markings; distribution list.
2. Allegations	Each allegation stated as a separate, specific matter; whether each is a disclosable matter.
3. Terms of reference	Scope, questions to be answered, investigator and their independence, timeframe, approvals.
4. Protection measures	Confirmation that confidentiality and detriment protections were applied; any concerns raised during the investigation.
5. Method	Documents and data reviewed; people interviewed (by role); experts used; limitations (for example an anonymous discloser could not be contacted).
6. Procedural fairness	How and when people mentioned were told of the allegations and given a chance to respond; summary of responses.
7. Findings	For each allegation: substantiated, partly substantiated, not substantiated or unable to be determined, with the evidence and reasoning (on the balance of probabilities).
8. Root cause and control weaknesses	Why it happened and which controls failed, using the Incident & Issues Management Standard categories.
9. Recommendations	Disciplinary referrals; customer remediation; control and process changes; regulatory notifications; owners and due dates.
10. Communication to the discloser	What the discloser will be told, and by whom.
11. Sign-off	Investigator; WIO; date; date reported to the [Board Audit Committee] .

Free general information only, provided free of charge. Not legal, financial or other professional advice, and used at your own risk. [Read the full disclaimer.](#)