Identitii Limited
ACN 603 107 044
ASX:ID8

Whistleblower Policy

Public

Version	2.1
Publication date	2025-05-22
Owner	Chief Executive Officer
Approver	Board of Directors
Classification	Public

Introduction **4**
Context 4
Purpose 4
Scope 4
Disclosable matters 4
Non-disclosable matters 5
Applicable persons 5
Exclusions 5
Objectives 6
Policy implementation **6**
Responsible parties involved in implementation 6
Communication and distribution 8
Policy change requests 9
Policy exception process 10
Policy requirements **12**
Requirements applicable to all staff 12
Requirements applicable to line managers 12
Principles 12
Making a whistleblower disclosure 12
Legal protections for whistleblowers 13
Eligibility 13
Legal rights and protections 13
Identity protection (confidentiality) 13
Protection from detrimental acts or omissions 13
Compensation and remedies for any detriment suffered 14
Protection from civil, criminal, and administrative liability 15
Support and practical protection for whistleblowers 15
Protecting your identity 15
Ensuring fair treatment 15
Support services 16
Investigation of a whistleblower disclosure 16
Receiving a whistleblower disclosure 16
Assessing whether a whistleblower disclosure should be investigated 17
What will happen if my concern is assessed as a whistleblower disclosure? 17
What will happen if my concern is assessed as not being a whistleblower disclosure? 17
Undertaking an investigation 17
Outcomes of investigations 17
Review and appeal 18
Policy compliance and enforcement **18**
Examples of non-compliance 18
Misconduct 18

Public

Serious misconduct..... 18
Consequences for non-compliance..... 18
Policy monitoring and evaluation..... 19
Monitoring and evaluation..... 19
Review..... 20
Conclusion..... 21
Schedule 1 - Criteria for protection as a whistleblower..... 22
Schedule 2 - Disclosure in the public interest..... 25
Schedule 3 - Emergency disclosure..... 26

Public

Introduction

Context

Identitii Limited ("We", "Us", "Identitii", "the Company") recognises the crucial role that whistleblowers play in maintaining transparency, integrity, and accountability within the organisation. The Australian Corporations Act 2001 provides a legal framework to encourage and protect whistleblowing and mandates protections and guidelines for whistleblowers (as defined in the criteria set out in Schedules 1, 2, and 3), ensuring they can report misconduct, illegal activities, or unethical behaviour without fear of retaliation.

Purpose

The purpose of this policy is to align with the legal requirements set out in the Australian Corporations Act 2001, outline the protections available to whistleblowers, the procedures for making and investigating whistleblower disclosures, and the measures in place to ensure the fair treatment of all employees involved.

Scope

Disclosable matters

This policy covers the reporting of various types of wrongdoing, known as disclosable matters, including but not limited to:

1. Dishonesty
2. Fraud
3. Corruption
4. Illegal activities (including theft, drug use/sale, violence, threatened violence, or criminal damage to company assets/property)
5. Discrimination, vilification, sexual harassment, harassment, bullying, and victimisation
6. Breaches of legislation or by-laws
7. Unethical behaviour
8. Unsafe work practices
9. Serious misconduct (including gross mismanagement, substantial waste of company resources, or repeated breaches of administrative procedures)
10. An improper state of affairs or circumstances
11. Any conduct that may cause financial or non-financial loss to the company or be detrimental to the interests or reputation of the company or its employees
12. The deliberate concealment of information related to any of the above matters

Public

Non-disclosable matters

The types of matters that are not covered by the policy include, but are not limited to:

1. Personal work-related grievances, such as:
    a. Interpersonal conflicts with other employees
    b. Decisions regarding employment, transfer, or promotion
    c. Decisions about the terms and conditions of employment
    d. Decisions to suspend or terminate employment or other disciplinary actions
    e. These types of grievances do not qualify for whistleblower protections and should be addressed through the company's standard grievance resolution procedures.
2. Complaints about company products or services
3. Issues related to customer service or support
4. Matters that are purely personal in nature and do not have broader implications for the company
5. Disputes with competitors or other businesses that do not involve misconduct by the company
6. Reports made with malicious intent or knowingly false allegations

Applicable persons

This Whistleblowing Policy applies to all current and former employees, directors, officers, contractors, suppliers, consultants, and any associates of Identitii Limited and its wholly owned subsidiaries. It also covers any relatives, dependents, or spouses of these individuals who may become aware of relevant misconduct. It encompasses all areas of the business and operations of the group.

Exclusions

There are certain exclusions from the whistleblower protections for people who may otherwise meet some of the eligibility criteria and who have observed or been affected by misconduct of the company. If you fall into one of the following categories, you may not be covered by the whistleblower protections. Accordingly, we encourage you to seek your own legal advice about any other rights or remedies that may be available to you. These categories include:

1. Individuals experiencing an employment dispute or a personal work-related grievance
2. Competitors
3. Customers and clients

Public

Objectives

The objectives of this policy are to:

1. Encourage the reporting of suspected or actual misconduct, illegal activities, or unethical behaviour within the Company.
2. Provide a secure and confidential process for individuals to report their concerns without fear of retaliation.
3. Ensure that all reported concerns are thoroughly investigated and addressed in a timely and appropriate manner.
4. Protect the rights and anonymity of whistleblowers, while ensuring compliance with the Australian Corporations Act 2001.
5. Foster a culture of transparency, integrity, and accountability within the organisation.
6. Outline the responsibilities of the Company in supporting and protecting whistleblowers, and in maintaining robust procedures for handling disclosures.

Policy implementation

Responsible parties involved in implementation

Roles and responsibilities incl. responsible authorities for monitoring and enforcement.

Role	Responsibilities
CEO	• Ensure implementation and compliance with the Whistleblower Policy. • Oversee and determine methods for investigations. • Report violations and actions to the Board. • Maintain confidentiality and protect whistleblower identity. • Communicate investigation outcomes to whistleblowers. • Assess if disclosures meet criteria for disclosable matters. • Nominate impartial investigators and ensure fair, best-practice investigations. • Review and approve final investigation reports and actions. • Review and update investigation procedures regularly. • Communicate policy updates to stakeholders.

Public

Investigators	• Conduct prompt, fair, and thorough investigations into reported malpractice or misconduct. • Securely hold all evidence, materials, documents, and records related to the investigation. • Prepare and submit a report of findings to the CEO at the conclusion of the investigation. • Recommend steps to remedy any harm or loss and disciplinary actions if necessary. • Maintain strict confidentiality throughout the investigation process. • Keep detailed records of all investigation steps, findings, and decisions, documenting the evidence collected.
Internal Recipients (e.g., Directors, Company Secretaries, Company Officers, Senior Managers, Auditors, and other authorised persons)	• Receive whistleblower disclosures. • Forward disclosures to the relevant authority for investigation. • Maintain confidentiality and support the whistleblowing process. • Report disclosures as soon as possible to the CEO or appropriate alternative in case of conflict of interest.

Public

Communication and distribution

To ensure effective communication of the policy to relevant stakeholders, the following steps can be taken:

1. Distribution and accessibility:
    a. The policy document should be made available to all relevant stakeholders in a centralised and easily accessible location. This could be achieved by publishing the policy on the organisation's intranet, document management system, or employee portal.
    b. Additionally, stakeholders should be notified about the availability of the policy and provided with instructions on how to access it.
2. Training and awareness programs:
    a. Conduct training sessions or workshops to educate stakeholders about the policy and its importance.
    b. These sessions can include presentations, interactive discussions, and practical examples to enhance understanding.
    c. Ensure that all employees, including executives, managers, and staff in different roles, attend the training sessions.
    d. It is also important to conduct periodic refresher training to reinforce key policy concepts.
3. Acknowledgement and acceptance:
    a. Require stakeholders to acknowledge their understanding and acceptance of the policy. This can be done through the implementation of an electronic or physical acknowledgement process where stakeholders sign or electronically acknowledge that they have read and understood the policy. This ensures that stakeholders are aware of their responsibilities and are accountable for complying with the policy.
4. Communication channels:
    a. Utilise various communication channels to reinforce the policy's message and updates.
    b. These channels can include internal newsletters, email communications, team meetings, and notice boards.
    c. Regularly communicate updates or changes to the policy, and emphasise the importance of adhering to the policy's guidelines.
5. Ongoing support and guidance:
    a. Establish a designated point of contact to address stakeholders' questions, provide guidance, and offer support related to the policy. This ensures that stakeholders have access to the necessary resources and assistance to comply with the policy.
6. Integration into onboarding process:
    a. Incorporate the policy into the onboarding process for new employees.
    b. During orientation, provide an overview of the policy, explain its relevance to their role, and highlight the expectations for compliance.
    c. Provide access to the policy document and ensure that new employees acknowledge their understanding and acceptance of the policy.

Public

7. Periodic policy review:
    a. Regularly review the policy to ensure its effectiveness and relevance in addressing evolving threats and technologies.
    b. Engage stakeholders in the review process by soliciting feedback and incorporating their insights and experiences into policy updates.
    c. Communicate any changes or revisions to the policy to all stakeholders in a timely manner.

Policy change requests

The process for requesting a change to the policy may typically involve the following steps:

1. Identify the need for change
    a. Any stakeholder who identifies the need for a change to the policy should carefully evaluate the rationale behind it. This may include new risks, regulatory changes, technological advancements, or feedback received from employees, auditors, or other relevant sources.
    b. It's important to clearly articulate the reasons for the proposed change.
2. Document the proposed change:
    a. The stakeholder requesting the change should document the proposed modifications to the policy. This includes detailing the specific sections or clauses that require revision, addition, or removal, along with a clear explanation of the desired changes and the expected outcomes.
3. Impact assessment:
    a. The proposed change should undergo an impact assessment to evaluate its potential consequences. This assessment may involve considering the impact on existing processes, procedures, technical controls, resources, and compliance requirements.
    b. It's crucial to assess both the positive and negative implications of the change.
4. Consultation and collaboration:
    a. The stakeholder should engage in consultation and collaboration with relevant parties to gather input and feedback. This may include discussions with members of the information security team, legal counsel, HR, risk management personnel, and other subject matter experts. Their expertise and perspectives can help evaluate the viability and effectiveness of the proposed change.
5. Review and approval process:
    a. The proposed change should undergo a formal review process, which may involve a designated committee or a specific individual responsible for policy management.
    b. The review process evaluates the proposed change in light of the organisation's goals, compliance requirements, and overall risk posture.
    c. The approval authority assesses the proposed change and decides whether to approve, reject, or request further modifications.

6. Communication and documentation:
    a. Once the change is approved, it should be communicated to all relevant stakeholders. This includes updating the policy document with the revised sections or incorporating an addendum to the existing policy.
    b. The updated policy should be made easily accessible to all stakeholders through the organisation's established communication channels.
7. Training and awareness:
    a. Conduct training or awareness sessions to educate employees about the revised policy. This ensures that all individuals affected by the change are aware of their new obligations and understand the reasons behind the modification.
    b. Training sessions may include explanations of the change, examples of its practical application, and clarification of any questions or concerns raised by employees.
8. Implementation and monitoring:
    a. The revised policy should be implemented and enforced across the organisation.
    b. Ongoing monitoring and compliance assessments should be conducted to ensure adherence to the updated policy
    c. Any deviations or non-compliance should be addressed through appropriate corrective actions.

Policy exception process

Implementing a policy exception requires a careful evaluation and approval process to ensure that exceptions are justified, properly managed, and do not compromise the organisation.

The process for implementing a policy exception typically involves the following steps:

1. Identify the need for an exception:
    a. A stakeholder or individual within the organisation identifies a situation or circumstance that warrants an exception to a specific policy.
    b. The need for the exception must be clearly defined and supported by valid reasons, such as business requirements, technical limitations, or legal or regulatory obligations.
2. Documentation of the exception request:
    a. The stakeholder requesting the exception should document the details of the exception request. This includes specifying the policy or control from which the exception is sought, describing the reason for the exception, and providing any supporting evidence or documentation.
3. Evaluation and risk assessment:
    a. The exception request undergoes an evaluation and risk assessment process. This involves assessing the potential impact of granting the exception on the organisation's security, compliance, and overall risk posture.
    b. The evaluation should consider the severity of the identified risk, available mitigating controls, and alternative solutions to address the situation.

Public

4. Review and approval process:
    a. The exception request is reviewed by the appropriate authority or committee responsible for policy governance and compliance. This may involve the information security team, HR, risk management personnel, legal counsel, or other relevant stakeholders.
    b. The review assesses the justification, feasibility, and acceptability of the requested exception.
    c. The approval authority makes a decision to approve, reject, or request further modifications to the exception request.
5. Documentation and tracking:
    a. Once the exception is approved, it should be properly documented, including the justification for the exception, the approval details, and any conditions or limitations associated with the exception. This documentation helps ensure transparency, accountability, and auditability.
    b. The exception request and its approval status should be tracked in a centralised repository or system for future reference and reporting.
6. Communication and awareness:
    a. The approved exception should be communicated to the relevant stakeholders who are affected by the exception. This includes notifying individuals responsible for implementing or enforcing the policy, as well as any other personnel who may be impacted by the exception.
    b. It's essential to ensure that all affected parties understand the scope, limitations, and duration of the exception.
7. Monitoring and review:
    a. The exception should be periodically reviewed to assess its ongoing relevance and validity. This includes monitoring the associated risks, evaluating any changes in the organisation's environment, and reassessing the need for the exception.
    b. If circumstances change, the exception may be modified, extended, or revoked based on the reassessment results.
8. Reporting and accountability:
    a. The exception process should include reporting mechanisms to ensure proper oversight and accountability. This may involve regular reporting to senior management, the board of directors, or other governing bodies to provide visibility into the exceptions granted and their associated risks.

Public

Policy requirements

Requirements applicable to all staff

1. Report any suspected malpractice, misconduct, or conflicts of interest in accordance with this policy.
2. Provide specific, adequate, and pertinent information to facilitate reasonable investigations.
3. Cooperate fully with investigators during the investigation process.
4. Refrain from making false reports deliberately, maliciously, or for personal gain, as such actions may lead to disciplinary measures.

Requirements applicable to line managers

1. Forward all received reports to the relevant authority, as appropriate.
2. Maintain confidentiality and support the whistleblowing process.

Principles

Making a whistleblower disclosure

Identitii encourages individuals to make whistleblower disclosures internally in the first instance, to allow the company to address concerns promptly and effectively. However, disclosures to external parties are also protected under the Corporations Act. Disclosures can be made confidentially and, if desired, anonymously. Any person who has reasonable grounds to suspect that a disclosable matter has occurred is encouraged to report that suspicion to any of the eligible recipients listed in the table below.

Type of recipient	Eligible recipients	Contact method
Internal recipients	• Directors • Company Secretaries • Company Officers • Senior Managers • Auditors • Other persons authorised by the Company to receive whistleblower disclosures.	• Directly via phone, email, or in writing. • By email to whistleblower@identitii.com • Through a whistleblower complaints service or hotline (if applicable)
External recipients	• Legal practitioners • Regulatory bodies • Journalists and Parliamentarians (subject to the criteria in Schedules 2 & 3)	• Directly via phone, email, or in writing. • By contacting ASIC (if applicable • By contacting APRA (if applicable) • By contacting the Commonwealth Ombudsman (if applicable)

Public

All reports of disclosable matters should provide specific, adequate and pertinent information with respect to, among other things, dates, places, persons/witnesses, amounts, and other relevant information, in order to allow for a reasonable investigation to be conducted. After making a report to an eligible internal recipient they will acknowledge receipt, and may initiate a follow-up meeting, if there is a means to contact you.

Legal protections for whistleblowers

Eligibility

To qualify for protection under the Corporations Act, a whistleblower must meet the criteria of an 'eligible whistleblower' as defined in Schedules 1, 2, & 3. Disclosures that are not about disclosable matters do not qualify for protection under the Corporations Act.

Legal rights and protections

These protections do not grant immunity to you for any misconduct that you were involved in that is revealed in the disclosure. Disclosures that are not disclosable matters do not qualify for protection under the Corporations Act, but may be protected under legislative instruments such as the Fair Work Act 2009.

Identity protection (confidentiality)

You can ask Identitii to keep your identity, or information that is likely to lead to your identification, confidential. Generally, we cannot disclose this identifying information without your consent. However, we may report the information to regulatory bodies, the Australian Federal Police, or to a lawyer for advice about the whistleblower protections. There may also be circumstances where we are required to disclose the information to a court or tribunal, where the court or tribunal considers it necessary in the interests of justice or to give effect to the whistleblower provisions in the Corporations Act.

It is illegal for a person to reveal the identity of a whistleblower, or information likely to lead to the identification of a whistleblower, outside of these circumstances. We will investigate allegations from a whistleblower that their confidentiality has been breached following their disclosure.

Protection from detrimental acts or omissions

Under the Corporations Act, it is illegal for anyone to cause or threaten detriment to you because they believe or suspect that you have made, may have made, propose to make, or could make a whistleblower disclosure. This protection applies even if you have not made a report, but the offender causes or threatens detriment to you because they believe or suspect you have or might make a disclosure.

Public

Detriment may include, but is not limited to:

1. Dismissal from your employment
2. Injury in your employment
3. Alteration of your position or duties to your disadvantage
4. Discrimination between you and other employees of the same employer
5. Harassment or intimidation
6. Harm or injury, including causing psychological harm
7. Damage to your property
8. Damage to your reputation
9. Damage to your business or financial position
10. Any other form of damage

The criminal offence and civil penalty require that the detriment be the result of an actual or suspected whistleblower disclosure. In some cases, particularly in private employment, there may be disputes about whether the conduct was victimisation due to the whistleblower disclosure or for another reason.

If the Company investigates allegations that someone has caused or threatened detriment to you, your assistance will be needed. If you believe you have suffered detriment, you may need to seek independent legal advice regarding compensation.

Compensation and remedies for any detriment suffered

If you suffer loss, damage, or injury as a result of making a whistleblower disclosure, you can seek compensation through the court. If you are or were an employee and experienced detriment at work for reporting misconduct, the court may order the person causing you detriment or your employer to compensate you.

Additionally, you can pursue other remedies, such as:

1. Reinstatement to your original position or a comparable position by your employer.
2. An injunction from the court to prevent or stop detrimental conduct.
3. An apology from the person, company, or organisation that caused you detriment or threatened you with detriment.

It is important to note that it is your responsibility to bring any such action for compensation. We strongly encourage you, if you believe you are a whistleblower, to seek independent legal advice about what remedies may be available to you if you suffer loss, damage, or injury. We are unable to give legal advice.

If you are unsuccessful in your claim for compensation for detriment against a person, company or organisation, you may be protected from having to pay their legal costs (unless a court finds your claim to be vexatious or you acted unreasonably).

Public

Protection from civil, criminal, and administrative liability

The Corporations Act protects a whistleblower against certain legal actions related to making the whistleblower disclosure, including:

1. Criminal prosecution (and the disclosure cannot be used against the whistleblower in a prosecution, unless the disclosure is false)
2. Civil litigation (such as for breach of an employment contract, duty of confidentiality, or other contractual obligation), or
3. Administrative action (including disciplinary action).

If you are the subject of an action for making a whistleblower disclosure, you may rely on this protection in your defence.

Support and practical protection for whistleblowers

Protecting your identity

The reasonable steps we will take to protect your identity and information in your whistleblower disclosure that is likely to identify you, may include:

1. Securely storing all paper and electronic documents and other materials relating to the disclosure.
2. Where possible, communicating with you to help identify the aspects of your concerns that could inadvertently identify you.
3. Potentially using a pseudonym to refer to you.
4. Providing training and awareness about the confidentiality requirements and consequences of breaching confidentiality to those involved in receiving, handling and investigating disclosures.

While we will take all reasonable steps to protect your identity, it may be difficult if your concern relates to information that only a few people know about, or was told to you confidentially.

Ensuring fair treatment

Identitii prohibits detrimental acts as a result of reporting, or proposing to report, a disclosable matter, or because you have been involved in the investigation of a disclosable matter. Any form of harassment, discrimination, or adverse action against whistleblowers is strictly prohibited, and will result in disciplinary measures.

We will take all reasonable steps to ensure fair treatment in relation to disclosable matters including, but not limited to:

1. Assessing and monitoring any risk of detrimental acts occurring.
2. Taking reasonable steps to protect you from those risks.
3. Ensuring the investigation will be conducted in a fair, impartial, and objective manner.
4. Providing any employee mentioned in a whistleblower disclosure with an opportunity to respond to any allegations made against them.
5. Informing relevant parties of the investigation findings (subject to confidentiality requirements).

Public

Not all conduct will amount to detrimental acts, such as managing poor work performance in line with the Identitii's performance management procedures, disciplinary action in response to unrelated misconduct, when you intentionally make a whistleblower disclosure that you know isn't true or is misleading, or action that is reasonable to protect you from detrimental acts.

Support services

Identitii will assist employees mentioned in whistleblower disclosures in maintaining their wellbeing. This may include providing strategies to minimise and manage stress, referring you to counselling and/or the employee assistance program. This support will be available during and after the investigation process.

Investigation of a whistleblower disclosure

Identitii Limited is dedicated to conducting investigations that adhere to best practice standards. When a whistleblower disclosure is deemed to require further investigation, the company will:

1. Assign independent and impartial investigators with no conflicts of interest. The use of internal or external experts is permitted, as necessary.
2. Establish clear procedures and defined timelines for each stage of the investigation to ensure timely completion.
3. Collect all relevant evidence and conduct a comprehensive examination of the disclosure.
4. Maintain strict confidentiality throughout the investigation process, disclosing information only on a need-to-know basis.
5. Keep detailed records of all investigation steps, findings, and decisions, documenting the evidence collected.
6. Provide individuals mentioned in the disclosure with an opportunity to respond to allegations and ensure all parties are treated fairly.
7. Keep the whistleblower and other relevant parties informed about the progress of the investigation while maintaining confidentiality.
8. Establish a process for reviewing and appealing investigation findings if any party believes the investigation was flawed or unfair.
9. Regularly review and update investigation procedures to incorporate lessons learned and best practices.

Receiving a whistleblower disclosure

The person receiving the whistleblower disclosure must report it as soon as possible to the CEO, who will then determine if the allegation constitutes a disclosable matter. If there is a conflict of interest, the determination will be made by an appropriate alternative from the list of eligible internal recipients.

Public

Assessing whether a whistleblower disclosure should be investigated

Your concern will be assessed as an eligible whistleblower disclosure (i.e. a concern that is being treated by the Company as a whistleblowing matter under this policy) if:

1. You meet the eligibility criteria defined in Schedule 1.
2. You have reasonable grounds to suspect that the information you are disclosing constitutes a disclosable matter.
3. You reported your concern to an eligible internal recipient.

What will happen if my concern is assessed as a whistleblower disclosure?

If your concern is assessed as a whistleblower disclosure, Identitii will nominate an independent and impartial investigator with no conflicts of interest. The use of internal or external experts is permitted, as necessary.

The investigator will review the disclosure to decide whether any of the allegations raised should be investigated. For example, sometimes we may decide not to investigate a disclosure (or part of it) if we have previously investigated the allegations in the disclosure and there is no new material. We will inform you whether or not an investigation will be undertaken (if you can be contacted).

What will happen if my concern is assessed as not being a whistleblower disclosure?

If your concern is assessed as not being a whistleblower disclosure, Identitii will refer the concern to the most appropriate area for management (e.g. the business unit the subject of the concern).

Undertaking an investigation

If the investigator decides that your whistleblower disclosure will be investigated, they will conduct or commission an investigation with the support of internal or external resources as appropriate. Investigations will be conducted promptly and fairly with due regard for the nature of the allegation and the rights of the persons involved in the investigation, ensuring independence from both you and the individuals involved in the disclosure. Evidence, including any materials, documents or records shall be held securely by the investigator. We will seek to conduct the investigation as quickly as the circumstances allow. The investigator will update you on the progress of the investigation (if you can be contacted).

Outcomes of investigations

At the conclusion of the investigation, the investigator will prepare a report of the findings for the CEO, or in the event of a conflict of interest, another governance committee. Where the final report indicates that a disclosable matter has occurred, the final report will include recommendations for steps to be taken to remedy any harm or loss arising from the disclosable matter, including disciplinary proceedings against the person responsible for the conduct, and the referral of the matter to appropriate authorities

Depending on the circumstances of the whistleblower disclosure and any privacy or confidentiality concerns, you and/or the person subject to the disclosure will be informed of the findings. However, neither you nor the person subject to the disclosure will receive a copy of the investigation report.

Public

Review and appeal

If you want to escalate an issue, you must put this in writing and ask an eligible internal recipient or the investigator to send it to the CEO or another governance committee.

You can escalate your issues to CEO or other appropriate governance committee if you:

1. Are not satisfied with a decision of the CEO or eligible internal recipient to not conduct an investigation.
2. Are not satisfied with the findings of the investigation.
3. Consider that the investigator has not appropriately escalated the concerns that you raised with them.
4. Believe that this policy has not been complied with in full.

Policy compliance and enforcement

Examples of non-compliance

Misconduct

Misconduct refers to actions or behaviour by an employee that deviates from the expected standards of conduct outlined in this policy. Examples of misconduct include:

1. Providing false information or omitting important information intentionally.
2. Not following established procedures or guidelines for investigating whistleblower disclosures.
3. Submitting whistleblower reports with minor inaccuracies that fundamentally misrepresent the situation.

Serious misconduct

Serious misconduct refers to actions or behaviour that significantly and detrimentally impact the organisation, its employees, clients, or stakeholders in breach of this policy. Serious misconduct may have legal implications and can result in immediate termination of employment. Examples of serious misconduct include:

1. Deliberate deception or falsification of information in a whistleblower report to secure personal gain or harm others.
2. Deliberately hiding information or obstructing investigations related to serious misconduct reported through whistleblowing.
3. Taking adverse actions against employees who have made protected disclosures.

Consequences for non-compliance

While misconduct is considered a breach of company policies, it is typically addressed through disciplinary measures or corrective actions, such as verbal warnings, written warnings, counselling, or performance improvement plans.

Due to the severe nature of serious misconduct, immediate and decisive action is often taken, including disciplinary proceedings, investigations, termination, and potential legal consequences.

Public

Policy monitoring and evaluation

Monitoring and evaluation

Monitoring and evaluating the progress and effectiveness of the policy is crucial to ensure its continuous improvement and alignment with organisational goals. Monitoring and evaluation may be conducted through internal audit, external audit, and manual audits of controls:

1. Internal audit:
    a. Internal audit teams or personnel, independent from the areas being audited, can assess the implementation and compliance of the policy.
    b. Internal audits can include a review of controls, processes, and procedures to determine their effectiveness and identify any gaps or weaknesses.
    c. Internal auditors can conduct regular audits based on an audit plan, which outlines the areas to be audited and the frequency of audits.
    d. The internal audit function can evaluate the organisation's adherence to the policy's requirements, identify areas of non-compliance, and provide recommendations for improvement.
    e. The internal audit team may also assess the effectiveness of processes, risk management practices, and awareness and training programs.
2. External audit:
    a. External audit firms or independent assessors can be engaged to evaluate the organisation's compliance with relevant standards, regulations, or industry best practices.
    b. External audits provide an objective assessment of the organisation's controls and compliance with external requirements.
    c. External auditors may review the organisation's policies, procedures, and controls, and assess their effectiveness in achieving the desired objectives.
    d. External audits can also provide an independent assessment of the organisation's data privacy and protection practices, including compliance with applicable privacy laws and regulations.
3. Manual audits of controls:
    a. Manual audits of controls involve conducting specific assessments of individual controls and processes.
    b. These audits can be performed by designated individuals or teams responsible for managing specific controls, such as access control, financial audits, network security, or data privacy.
    c. Manual audits assess the adequacy and effectiveness of controls, identify any deviations or non-compliance, and recommend corrective actions.
    d. The audits can be conducted through interviews, documentation review, observations, and testing of control effectiveness.
    e. Manual audits help ensure that controls are properly implemented, monitored, and aligned with the policy's requirements.

Public

4. Key considerations:
    a. Monitoring and evaluation efforts should be based on a well-defined audit plan or schedule to ensure regular assessments of different aspects of the policy.
    b. The results of audits, both internal and external, should be documented and shared with relevant stakeholders, such as senior management.
    c. Identified gaps or non-compliance should be addressed through corrective actions and follow-up audits to verify the effectiveness of remedial measures.
    d. Monitoring and evaluation processes should be adaptable to changes in the organisation's environment, emerging threats, and evolving requirements.
    e. It is important to ensure that auditors and assessors possess the necessary expertise and knowledge to effectively evaluate the policy and associated controls.

Review

To ensure the policy remains up-to-date, effective, and aligned with organisational goals, feedback, review, and periodic revisions should be incorporated into the policy management process. Here are mechanisms that can be implemented for these purposes:

1. Feedback mechanisms:
    a. Establish a designated point of contact to receive feedback and suggestions regarding the policy.
    b. Encourage stakeholders to provide feedback through various channels, such as a designated email address, feedback forms, or an anonymous reporting system.
    c. Conduct surveys or focus group discussions to gather insights and perspectives from employees, management, and other stakeholders.
    d. Establish a culture of open communication and encourage stakeholders to proactively raise concerns or provide suggestions related to the policy.
2. Periodic review:
    a. Define a timeline or schedule for conducting periodic reviews of the policy. The frequency may vary depending on the organisation's needs, but typically ranges from annually to biennially.
    b. Form a review committee consisting of representatives from relevant departments, such as information security, HR, technology, legal, compliance, and risk management, to conduct the policy review.
    c. During the review, assess the policy's alignment with emerging threats, changes in regulatory requirements, technological advancements, and lessons learned from incidents or audits.
    d. Solicit feedback from stakeholders during the review process to gather insights on the policy's strengths, weaknesses, and areas for improvement.
    e. Evaluate the policy against industry best practices, standards, and guidelines to ensure its relevance and effectiveness.

Public

3. Revisions and updates:
    a. Based on the feedback and findings from the review process, initiate the necessary revisions and updates to the policy.
    b. Clearly document all changes made to the policy, including the rationale and considerations behind each revision.
    c. Ensure that the revised policy reflects the latest best practices, addresses identified gaps or weaknesses, and incorporates new legal or regulatory requirements.
    d. Communicate the revisions to all stakeholders through appropriate channels, such as internal newsletters, email communications, or training sessions.
    e. Ensure that stakeholders have access to the updated policy document and are aware of the changes made.
4. Training and awareness:
    a. Conduct training sessions or awareness programs to educate employees and stakeholders about the revised policy and its implications.
    b. Highlight the changes made, the reasons behind the revisions, and any new responsibilities or requirements resulting from the updated policy.
    c. Reinforce the importance of adhering to the policy and provide guidance on how to comply with the revised guidelines.
    d. Offer refresher training periodically to reinforce key policy concepts and maintain awareness among stakeholders.

Conclusion

The Whistleblower Policy is a critical component of Identitii's commitment to maintaining transparency, integrity, and accountability. This policy ensures a secure and confidential mechanism for reporting misconduct, illegal activities, or unethical behaviour, which fosters an environment where employees and stakeholders feel safe to voice their concerns without fear of retaliation.

We recognise the invaluable role that whistleblowers play in upholding our corporate governance and ethical standards and ensure that all disclosures are taken seriously, investigated thoroughly, and addressed promptly. We are dedicated to protecting the rights and anonymity of whistleblowers, ensuring fair treatment for all individuals involved, and maintaining compliance with the Australian Corporations Act 2001.

Public

Schedule 1 - Criteria for protection as a whistleblower

These criteria seek to include most people with a connection to a company who may be in a position to observe or be affected by misconduct and may face reprisals for reporting it. These people can access the rights and protections in the law from when they report misconduct. The protections also extend to the spouses and relatives of these people. Whistleblowers can provide their name, role, and contact details when they report, or they may also report anonymously. There is no formal registration process for whistleblowers; the protections apply to anyone who meets the criteria.

Criteria	The law requires
Your role	You must be a current or former: • Employee of the company or organisation your disclosure is about, or a related company or organisation • Officer (usually that means a director or company secretary) of the company or organisation your disclosure is about, or a related company or organisation • Person (or employee of a person or entity) who has supplied goods or services to the company or organisation your disclosure is about, or a related company or organisation – this can be either paid or unpaid, and can include volunteers • Associate of the company or organisation, usually a person with whom the company or organisation acts in concert • Trustee, custodian or investment manager of a superannuation entity, or an officer, employee or goods or service provider to a trustee, custodian or investment manager, or • Spouse, relative or dependant of one of the people referred to above, or a dependant of such an individual's spouse.

Public

Who you make the disclosure to	You must make your disclosure to: ● A director, company secretary, company officer, or senior manager of the company or organisation, or a related company or organisation ● An auditor, or a member of the audit team, of the company or organisation, or a related company or organisation ● An actuary of the company or organisation, or a related company or organisation ● A person authorised by the company or organisation to receive whistleblower disclosures ● ASIC or the Australian Prudential Regulation Authority (APRA), or ● Your lawyer, if disclosing to obtain legal advice or representation under the whistleblower provisions of the Corporations Act. While you must make your disclosure to one of these people or organisations, you can raise your concerns anonymously. The Corporations Act also includes limited protections for disclosures to journalists or parliamentarians, in certain circumstances, as set out in Schedule 2.

Public

Subject of your disclosure	You must have reasonable grounds to suspect that the information you are disclosing about the company concerns: ● misconduct, or ● an improper state of affairs or circumstances. This information can be about the company, or an officer or employee of the company or organisation, engaging in conduct that: ● breaches the Corporations Act ● breaches other financial sector laws enforced by ASIC or APRA ● breaches an offence against any other law of the Commonwealth that is punishable by imprisonment for a period of 12 months, or ● represents a danger to the public or the financial system. 'Reasonable grounds' means that a reasonable person in your position would also suspect the information indicates misconduct or a breach of the law. The Corporations Act also includes limited protections if your concerns relate to matters in the public interest or an emergency (see Schedule 2 or Schedule 3).

Public

Schedule 2 - Disclosure in the public interest

Whistleblower protections can also apply to you if you make a whistleblower report in the public interest. However, this is only in certain limited circumstances which are set out below. If you disclose your concerns to the public in another way, these protections do not apply.

Criteria	The law requires
Previous report	You must have previously made a report to ASIC or APRA that satisfies the criteria in Schedule 1.
90 days	At least 90 days have passed since you reported your concerns to ASIC or APRA, and you **do not** have reasonable grounds to believe that action to address your concerns is being or has been taken.
Public interest	You have reasonable grounds to believe that reporting your concerns to a journalist or parliamentarian would be in the public interest.
Written notice to ASIC or APRA	After 90 days from when you reported to ASIC or APRA, you give ASIC or APRA a written notice that includes sufficient information to identify your earlier report and states your intention to make a public interest disclosure. This could be by contacting the ASIC officer who considered your concerns and quoting the reference number of your case.
Journalist or parliamentarian	You report your concerns about misconduct or an improper state of affairs or circumstances or a breach of the law to a journalist or a parliamentarian. The extent of the information disclosed is no greater than is necessary to inform the recipient about your concerns.

Public

Schedule 3 - Emergency disclosure

Whistleblower protections can also apply to you if you make a whistleblower report to a journalist or parliamentarian in the event of an emergency. However, this is only in certain limited circumstances which are set out below. If you disclose your concerns to the public in another way, these protections do not apply.

Criteria	The law requires
Previous report	You must have previously made a report to ASIC or APRA that satisfies the criteria in Schedule 1.
Emergency	You have reasonable grounds to believe that the information in your report concerns substantial and imminent danger to the health or safety of one or more people or to the natural environment.
Written notice to ASIC or APRA	You give ASIC or APRA a written notice that includes sufficient information to identify your earlier report and states your intention to make an emergency disclosure. Please quote the reference number of your previous report to ASIC.
Journalist or parliamentarian	You report your concerns about the substantial or imminent danger to a journalist or parliamentarian. The extent of the information disclosed is no greater than is necessary to inform the recipient about the substantial and imminent danger.

Public