Identitii Limited
ACN 603 107 044
ASX:ID8

Disclosure Policy

Public

Version	2.1
Publication date	2025-05-22
Owner	Disclosure Committee
Approver	Board of Directors
Classification	Public

Introduction **4**
Context 4
Purpose 4
Scope 4
Objectives 4
Policy implementation **5**
Responsible parties involved in implementation 5
Communication and distribution 6
Policy change requests 7
Policy exception process 8
Policy requirements **10**
Requirements applicable to all staff 10
Requirements applicable to line managers 10
Principles 10
Continuous disclosure obligations 10
Disclosure obligations 10
Material effect on price or value 10
Disclosure matters generally 11
Inform ASX first 11
Speculation and rumours 11
False market 11
Trading halts and voluntary suspension 11
Breaches 11
Market communication 11
Communication of information 11
Analysts and institutional investors 12
Analyst reports 12
Inadvertent disclosure or mistaken non-disclosure 12
Media relations and public statements 13
Investor relations and communication 13
Periodic reporting 13
The Company's website 13
Use of electronic communication and other technology 13
General meetings 13
Notices of meetings 14
Auditor to attend AGM 14
Shareholder privacy 14
Policy compliance and enforcement **14**
Examples of non-compliance 14
Misconduct 14
Serious misconduct 15
Consequences for non-compliance 15

Public

Policy monitoring and evaluation..... 16
Monitoring and evaluation..... 16
Review..... 17
Conclusion..... 18

Public

Introduction

Context

The policy is necessitated by the need for transparent, timely, and effective communication with shareholders. This is crucial in maintaining investor confidence and compliance with regulatory requirements, particularly the ASX Listing Rules and the Corporations Act 2001 (Cth). The company must ensure that all material information is disclosed to the market to prevent any false or misleading perceptions about its securities.

Purpose

The purpose of the policy is to establish clear guidelines and procedures for communicating with shareholders. It aims to ensure that all material information is disclosed in a manner that is timely, accessible, and clear. This is to ensure the company complies with continuous disclosure obligations and maintains transparency with its shareholders.

Scope

This policy applies to all directors, officers, employees, and consultants of Identitii Limited and its wholly owned subsidiaries (collectively referred to as personnel). It encompasses all aspects of the group's communication with shareholders, including disclosures required by the ASX Listing Rules and the Corporations Act 2001 (Cth). This includes all forms of communication, such as market announcements, media releases, and briefings with analysts and institutional investors.

Objectives

The policy's objectives and desired outcomes are to:

1. Ensure compliance with ASX Listing Rule 3.1 and the Corporations Act 2001 (Cth) by promptly disclosing any material information that could affect the price or value of the company's securities.
2. Establish a Disclosure Committee responsible for managing compliance with disclosure obligations.
3. Provide clear procedures for assessing and disclosing material price-sensitive information.
4. Ensure that information is first disclosed to the ASX before being released to the public or media.
5. Prevent and correct any false markets in the company's securities.
6. Facilitate effective and timely communication with shareholders, enhancing transparency and investor confidence.

Public

Policy implementation

Responsible parties involved in implementation

The Company has established a Disclosure Committee, initially composed of the CEO and the Company Secretary, though membership may vary over time. The role of the Disclosure Committee is to manage the Company's compliance with its disclosure obligations and this policy. Subject to any directions from the Board, its responsibilities include overseeing these compliance efforts. Additionally, the Company has appointed the Company Secretary as the person responsible for communication with ASX regarding listing rule matters and for the general administration of this policy.

Role	Responsibilities
Disclosure Committee	• Monitor the company's compliance with disclosure obligations and relevant procedures. • Assess the materiality of potentially price-sensitive information and escalate significant matters to the Chairperson and the Board. • Make decisions on information to be disclosed to the market. • Prepare timely company announcements that are not misleading and are clear, balanced, and objective. • Refer key significant announcements to the Board for consideration. • Review periodic disclosure documents and media announcements before their release to the market. • Monitor disclosure processes and reporting.
Company Secretary	• Ensure that ASX is immediately notified of any information that needs to be disclosed. • Review board papers and other referred information for potential disclosure obligations. • Approve routine administrative market releases.
Other officers and employees	• Understand and comply with the company’s legal obligations related to the disclosure of material price-sensitive information and confidentiality. • Participate in training organised by the Disclosure Committee to raise awareness of internal processes and controls. • Promote compliance with the policy and guidelines.

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, such as the CTO or the Head of Operations, assesses the proposed change and decides whether to approve, reject, or request further modifications.

Public

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.
    Monitoring and review:
    c. 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.
    d. If circumstances change, the exception may be modified, extended, or revoked based on the reassessment results.
7. 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. All staff must be aware of and understand the company's disclosure obligations and this policy. Periodic training will be provided to ensure comprehension and compliance.
2. Staff must promptly report any information that may be materially price-sensitive to their line manager or a member of the Disclosure Committee.
3. Staff must maintain the confidentiality of any potentially price-sensitive information until it is disclosed to the market.
4. All staff must comply with the procedures and guidelines set out in this policy to ensure timely and accurate disclosure of material information.

Requirements applicable to line managers

1. Line managers are responsible for monitoring the activities and information within their area of control to identify any potentially material price-sensitive information.
2. Line managers must immediately escalate any potentially material price-sensitive information to the Disclosure Committee.
3. Line managers should provide support and guidance to their team members to ensure they understand and comply with the disclosure requirements.
4. Line managers should facilitate and encourage participation in any training sessions organised by the Disclosure Committee to ensure their teams are informed about the company's disclosure obligations and processes.
5. Line managers should ensure clear and effective communication within their teams regarding the importance of compliance with the disclosure policy and procedures.

Principles

Continuous disclosure obligations

Disclosure obligations

The Company has adopted a set of procedures and guidelines in relation to its continuous disclosure obligations under the ASX Listing Rules and the Corporations Act 2001 (Cth). ASX Listing Rule 3.1 requires the Company to immediately disclose to the market any information concerning the Company that a reasonable person would expect to have a material effect on the price or value of the Company's securities. Disclosure is made by making an announcement to ASX.

Material effect on price or value

Information will be taken to have a material effect on the price or value of the Company's securities if it would be likely to influence investors in deciding whether to buy, hold or sell the Company's securities if the information became public. This type of information is referred to as "material price sensitive" information. Materiality is assessed using measures appropriate to the Company and having regard to the examples given by ASX in ASX Listing Rule 3.1.

Public

Disclosure matters generally

Inform ASX first

The Company will not release any information publicly that is required to be disclosed through ASX until the Company has received formal confirmation of its release to the market by ASX, unless otherwise permitted by the Listing Rules. Information must not be given to the media before it is given to ASX, even on an embargo basis.

Speculation and rumours

Generally, the Company will not respond to market speculation or rumours unless a response is required by law or ASX, including for the purposes of the "False market" section of this policy.

False market

If the ASX considers that there is, or is likely to be, a false market in the Company's securities and asks the Company to give it information to correct or prevent a false market, the Company must give the ASX the information needed to correct or prevent the false market.

Trading halts and voluntary suspension

If necessary, the Disclosure Committee may consider and are authorised to request a trading halt from ASX to prevent trading in the Company's securities on an uninformed basis, and to manage disclosure issues.

Breaches

Failure to comply with the disclosure obligations in this policy may lead to a breach of the Corporations Act or Listing Rules and to personal penalties for directors and officers. Breaches of this policy may lead to disciplinary action being taken.

Market communication

Communication of information

The Company will post on its website relevant announcements made to the market and related information, (which may include slides and presentations used in analyst or media briefings) after they have been given to ASX and following confirmation of release to the market by ASX.

Material price sensitive information will be posted as soon as reasonably practicable after its release to ASX following receipt of confirmation from ASX. Information may also be provided from time to time to the media on behalf of the Company but not before disclosure to ASX, even on an embargo basis.

Public

Analysts and institutional investors

The Company may conduct briefings for analysts and institutional investors from time to time to discuss matters concerning the Company. Only the directors, the Company Secretary or approved representatives of the Company are authorised to speak with analysts and institutional investors.

The Company's policy at these briefings is that:

1. the Company will not comment on material price sensitive issues not already disclosed to the market; and
2. any questions raised in relation to material price sensitive issues not already disclosed to the market will not be answered or will be taken on notice.

If a question can only be answered by disclosing material price sensitive information, the Company's policy is to decline to answer the question or alternatively, take it on notice. If a question is taken on notice and the answer would involve the release of material price sensitive information, the information must be released through ASX before responding.

A Company representative in attendance may make notes of meetings and briefings with investors or analysts. Alternatively, an event may be webcast or teleconferenced or a recording or transcript added to the Company's website. After briefings, a member of the Disclosure Committee will consider the matters discussed at the briefings to ascertain whether any material price sensitive information was inadvertently disclosed. If so, the information must be communicated to the market as set out in the "Inadvertent disclosure or mistaken non-disclosure" section of this policy.

Analyst reports

If requested, the Company may review analyst reports. The Company's policy is that it will only review these reports to clarify historical information and correct factual inaccuracies if this can be achieved using information that has been disclosed to the market generally.

No comment or feedback will be provided on financial forecasts, including profit forecasts prepared by the analyst, or on conclusions or recommendations set out in the report. The Company will communicate this policy whenever asked to review an analyst report.

Inadvertent disclosure or mistaken non-disclosure

If material price sensitive information is inadvertently disclosed, or a director or employee becomes aware of information which should be disclosed, a member of the Disclosure Committee must immediately be contacted so that appropriate action can be taken including, if required, announcing the information through ASX and then posting it on the Company's web site.

Public

Media relations and public statements

Media relations and communications are the responsibility of the Chairperson and CEO. On Board, corporate and governance matters, the Chairperson is generally the spokesperson and on general business and financial matters, the CEO is generally the spokesperson.

Other officers or senior employees may be authorised by the Board or the CEO to speak to the media on particular issues or matters. Any inquiry that refers to market share, financials or any matter which the recipient considers may be materially price sensitive must be referred to the Company Secretary.

No information is to be given to the media on matters which are of general public interest or which may be materially price sensitive without the approval of the Chair and CEO. The guidelines outlined above are subject to any directions given by the Board, either generally or in a particular instance.

Investor relations and communication

Periodic reporting

The Company produces half yearly and yearly financial reports and an annual report in accordance with the Corporations Act, the Listing Rules and applicable accounting standards.

The Company's website

The Company's website contains information about the Company, including shareholder communications, market releases and related information. Investor information is posted in a separate section on the website from other material about the Company.

Relevant media releases, the Company's financial data and its charters and public policies will also be available on the Company's website. The website also provides information to assist shareholders in directing relevant inquiries to the Company's share registry.

Use of electronic communication and other technology

Shareholders may elect to receive information electronically. The Company will communicate by post with shareholders who have not elected to receive information electronically. The Company may consider the use of other technologies as they become widely available.

General meetings

General meetings are used to communicate with shareholders and allow an opportunity for informed shareholder participation. Shareholders are encouraged to attend or, if unable to attend, to vote on the motions proposed by appointing a proxy or using any other means included in the notice of meeting. The Company conducts its general meetings in accordance with the Company's constitution, the Corporations Act and the Listing Rules. The Board will consider the use of technology and other means to facilitate shareholder participation as appropriate.

Public

Notices of meetings

Notices of meeting and accompanying explanatory notes aim to clearly, concisely and accurately set out the nature of the business to be considered at the meeting and comply with the Company's constitution, the Corporations Act and Listing Rules. The Company will place notices of general meetings and accompanying explanatory material on the Company's website.

Auditor to attend AGM

The external auditor will attend the annual general meeting and be available to answer questions about the conduct of the audit and the preparation and content of the auditor's report.

Shareholder privacy

The Company recognises that privacy is important and will not disclose registered shareholder details unless required by law. Shareholder details will only be used in accordance with applicable privacy laws.

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 corporate policies or codes of conduct. It typically involves violations of company policies, rules, or guidelines, which may result in minor breaches or disruptions in the workplace. Examples of misconduct include:

1. Minor policy violations:
    a. These can include tardiness, unauthorised personal use of company resources, or failure to adhere to dress code policies.
2. Insubordination:
    a. Disrespectful behaviour towards superiors or refusal to follow reasonable instructions falls under misconduct.
3. Non-compliance:
    a. Failure to adhere to specific procedures or protocols outlined by the organisation, such as timekeeping or reporting requirements.
4. Minor conflicts of interest:
    a. Engaging in activities that may compromise the employee's objectivity or create a conflict between personal and professional interests.

Public

Serious misconduct

Serious misconduct refers to actions or behaviour that significantly and detrimentally impact the organisation, its employees, clients, or stakeholders. It involves more severe violations that breach ethical standards, cause harm, or disrupt the workplace environment. Serious misconduct may have legal implications and can result in immediate termination of employment. Examples of serious misconduct include:

1. Theft or fraud:
    a. Engaging in fraudulent activities, embezzlement, misappropriation of company funds, or stealing company property.
2. Workplace violence or harassment:
    a. Physical assault, threats, intimidation, or any form of harassment that creates a hostile or unsafe work environment.
3. Gross negligence or recklessness:
    a. Engaging in actions that pose a significant risk to the safety of others or the company's operations, such as deliberate sabotage or deliberate violations of safety protocols.
    b. Failure to comply with disclosure obligations.
4. Discrimination:
    a. Treating others unfairly based on protected characteristics, such as race, gender, religion, or disability.
5. Breach of confidentiality:
    a. Unauthorised disclosure of confidential or sensitive information, including client data or trade secrets.

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

The Disclosure Committee will review this policy from time to time and report to the Board any changes it considers should be made. This policy may be amended by resolution of the Board. This policy is available on the Company's website and the key features, or a URL link to the webpage, are published in the annual report.

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

This Disclosure Policy ensures the Company's commitment to transparent, timely, and effective communication with shareholders, enhancing investor confidence and regulatory compliance, particularly with ASX Listing Rules and the Corporations Act 2001 (Cth). Compliance with this policy is mandatory for all personnel, with specific responsibilities assigned to line managers and the Disclosure Committee. The policy outlines clear guidelines and procedures for disclosing material information, designates responsible parties, and sets communication strategies to meet continuous disclosure obligations.

Public