Identitii Limited
ACN 603 107 044
ASX:ID8

Anti-Terrorism Policy

Public

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

Introduction **3**
Context 3
Purpose 3
Scope 3
Objectives 3
Policy implementation **4**
Responsible parties involved in implementation 4
Communication and distribution 4
Policy change requests 6
Policy exception process 7
Policy requirements **8**
Requirements applicable to all staff 8
Requirements applicable to line managers 9
Principles 9
Compliance with legislation 9
Personnel verification 9
Prohibition on terrorism financing 9
Reporting suspicious activities or transactions 9
Policy compliance and enforcement **10**
Examples of non-compliance 10
Misconduct 10
Serious misconduct 10
Consequences for non-compliance 11
Policy monitoring and evaluation **11**
Monitoring and evaluation 11
Review 12
Conclusion **14**

Public

Introduction

Context

The necessity of this policy arises from the growing global threat of terrorism and the legal obligations imposed by Australian Government legislation. Organisations, including Identitii, must ensure they are not inadvertently supporting or engaging with terrorist entities.

Purpose

The purpose of this policy is to outline Identitii's commitment to preventing terrorism by ensuring that its resources are not used to support terrorist activities. This policy establishes the procedures and measures Identitii will adopt to comply with Australian Government legislation related to terrorism.

Scope

This policy applies to all employees, contractors, and stakeholders of Identitii Limited and its wholly owned subsidiaries. It covers all financial transactions, support activities, and partnerships involving individuals or organisations, both domestic and international. The scope of this policy is aligned with relevant standards, including:

- Part 5.3 of the Criminal Code Act 1995 (‘the Criminal Code’)
- Part 4 of the Charter of the United Nations Act 1945 (‘the UN Charter Act’)."

Objectives

The objectives of this policy are:

1. To ensure compliance with Australian Government legislation prohibiting dealings with listed terrorist organisations and proscribed persons or entities.
2. To implement measures for verifying the identity, credentials, and standing of individuals and organisations that Identitii supports or transacts with.
3. To prevent the remittance of funds to known or suspected terrorist organisations or individuals.
4. To establish a clear reporting mechanism for any suspected links to terrorism, ensuring prompt action and communication with relevant national authorities.

Public

Policy implementation

Responsible parties involved in implementation

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

Role	Responsibilities
Board of Directors	• Ensure overall compliance with the anti-terrorism policy and related legislation. • Approve and oversee the implementation of the policy.
CEO	• Lead the development and enforcement of the anti-terrorism policy. • Ensure that all relevant measures are in place and that staff are aware of their obligations.
Head of Operations	• Maintain up-to-date knowledge of relevant laws and regulations. • Conduct due diligence checks on individuals and organisations. • Ensure that all employees are trained and aware of the anti-terrorism policy. • Incorporate compliance requirements into employee onboarding and ongoing training programs.
Finance Department	• Ensure that no funds are remitted to known or suspected terrorist organisations or individuals. • Conduct financial transactions in compliance with the policy. • Report any suspicious activity.
All Employees and Contractors	• Adhere to the anti-terrorism policy in all activities. • Report any suspicions or breaches of the policy. • Participate in training and awareness programs.

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 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 legal, 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 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 comply with the anti-terrorism policy and relevant legislation at all times.
2. Participate in training programs to understand the policy and the legal requirements associated with anti-terrorism.
3. Promptly report any known or suspected links to terrorism.
4. Exercise due diligence in all activities, ensuring that individuals and organisations are verified and not associated with terrorism.
5. Maintain confidentiality regarding any investigations or reports related to terrorism.

Requirements applicable to line managers

1. Ensure that all team members are aware of and adhere to the anti-terrorism policy.
2. Facilitate and monitor the participation of their team members in mandatory training programs.
3. Regularly monitor activities within their department to ensure compliance with the policy.
4. Report any suspicions or breaches of the policy and assist in any subsequent investigations.
5. Provide support and guidance to staff on policy-related matters and ensure that any concerns or queries are addressed promptly.

Principles

Compliance with legislation

Identitii acknowledges that Australian Government legislation prohibits dealing with listed terrorist organizations and/or proscribed persons or entities. Identitii will at all times adopt measures intended to facilitate compliance with this legislation.

Personnel verification

Identitii will confirm the identity, credentials and good standing of the people or organisations it supports and will check that these people or organisations are not on the lists maintained by the Australian Government.

Prohibition on terrorism financing

Identitii will not knowingly remit any funds to known or suspected terrorist organisations or individuals.

Reporting suspicious activities or transactions

Identitii will report any known or suspected terrorist links to the relevant national authority.

Public

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.

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.
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.

Public

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.

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.

Public

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.
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.

Public

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 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.
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.

Public

Conclusion

This policy underscores Identitii's unwavering commitment to combating terrorism and complying with Australian Government legislation. By adopting rigorous measures to verify the identity and credentials of individuals and organisations, Identitii aims to prevent any inadvertent support for terrorist activities. The policy outlines clear responsibilities for all employees, from the Board of Directors to line managers and staff, ensuring a unified and proactive approach to anti-terrorism compliance.

Public