Identitii Limited
ACN 603 107 044
ASX:ID8

Anti-Bribery & Anti-Corruption 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
Definitions 3
Objectives 4
Policy implementation **5**
Responsible parties involved in implementation 5
Communication and distribution 5
Policy change requests 7
Policy exception process 8
Policy requirements **10**
Requirements applicable to all staff 10
Requirements applicable to line managers 10
Principles 11
Prohibition against bribery and corruption 11
Interactions with officials and third parties must be compliant 12
Documentation and record-keeping 12
Prohibition on facilitation payments 12
Political or charitable contributions 12
Political contributions 12
Charitable donations 13
Compliance with local laws 13
Reporting violations and suspected misconduct 13
Protection 13
Policy compliance and enforcement **14**
Examples of non-compliance 14
Misconduct 14
Serious misconduct 14
Consequences for non-compliance 15
Policy monitoring and evaluation **15**
Monitoring and evaluation 15
Review 17
Conclusion **18**

Public

Introduction

Context

Identitii Limited operates in a global environment where anti-bribery and anti-corruption laws are stringent and varied across different jurisdictions. To ensure compliance and maintain high ethical standards, it is imperative for Identitii to adopt robust policies that prevent any form of bribery or corruption. This policy is aligned with international standards such as the United States Foreign Corrupt Practices Act (FCPA), the Criminal Code Act 1995 (Australia), and the Bribery Act 2010 (UK). The necessity of this policy is underscored by Identitii's commitment to conducting business legally and ethically, thereby protecting its reputation and avoiding severe legal penalties.

Purpose

The purpose of the Identitii Anti-Bribery & Anti-Corruption Policy is to provide clear guidelines and standards for all personnel in relation to interactions with officials and third parties. This policy aims to prevent bribery and corruption within Identitii's operations and to ensure full compliance with relevant anti-corruption legislation in all jurisdictions where Identitii operates. It serves to foster a culture of integrity and ethical business practices throughout the organisation.

Scope

Identitii Limited and its wholly owned subsidiaries require all personnel—including directors, temporary staff, contractors, and business associates—to comply with this policy, as well as with anti-corruption legislation and any applicable anti-corruption laws and regulations specific to the locations in which they operate.

Definitions

1. “Anti-Corruption Legislation” means the United States Foreign Corrupt Practices Act (the “FCPA”), the Criminal Code Act 1995 (Commonwealth of Australia), including Divisions 70 and 141, and the Bribery Act 2010 (United Kingdom).
2. “Bribery” means the offering or providing (or authorising the offer or provision) of any loan, gift, lavish trip or entertainment, donation, payment, or any other thing of value directly or indirectly, in cash or in kind, to or for the benefit of any official or third party to obtain or retain business or to secure any improper advantage for the Identitii.
3. “Business Associates” means the third-party companies and individuals (such as joint venture partners, consultants and agents) acting on behalf of the Identitii, whether directly or indirectly, by representing the Group’s interests in relation to business development or retention of business opportunities.
4. “Facilitation Payment” means payments of nominal amounts to persons in order to ensure or speed up the performance of a government official’s routine governmental duties or actions.

5. “Government Official” means anyone regardless of rank or title who is:
    a. engaged in public duty in a government agency whether elected or appointed, and at any level of government including national, state or local government entities;
    b. a member of any legislative, administrative or judicial body;
    c. an employee of a government agency, regardless of rank including an administrative and/or office worker;
    d. an officer or employee of a government-owned or government-controlled entity, including state-owned entities that operate in the commercial sector;
    e. an officer or employee of a public international organisation (such as the United Nations, the World Bank or the International Monetary Fund); or
    f. acting in an official capacity for a government, government agency, or state-owned enterprise.
6. “Item of Value” includes cash, travel, meals, gifts, and other tangible or intangible benefits.
7. “Official” means a government official, political party, official or officer of a political party or candidate for political office.
8. “Personnel” means all persons acting on behalf of the Identitii at all levels, including officers, directors, employees, temporary staff and contractors of the Group.
9. “Secure an improper advantage” includes obtaining any improper commercial or financial benefit.
10. “Third Party” means any individual or organisation other than officials, with whom personnel come into contact during the course of their employment or business relationships associated with Identitii.

Objectives

The primary objectives of this policy are to:

1. Establish and enforce standards that prohibit any form of bribery or corrupt activity within Identitii’s operations.
2. Guarantee adherence to all applicable anti-corruption laws and regulations in every country where Identitii operates.
3. Foster a corporate culture where high ethical standards and integrity are paramount in all business dealings.
4. Safeguard Identitii's reputation and legal standing by preventing activities that could lead to legal penalties or reputational damage.
5. Provide comprehensive training to ensure all personnel understand the policy and their responsibilities in preventing bribery and corruption.
6. Encourage vigilance and provide clear reporting mechanisms for any suspected violations of this policy.

Public

Policy implementation

Responsible parties involved in implementation

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

Role	Responsibilities
CEO	• Act as a point of contact for policy-related queries and reporting. • Ensure compliance with local anti-corruption laws and regulations.
Company Secretary	• Overall administration of the Anti-Bribery & Anti-Corruption Policy. • Monitor policy implementation and effectiveness. • Conduct regular audits of internal control systems. • Provide training on policy compliance.
Personnel (Employees, Directors, Temporary Staff, Contractors)	• Understand and comply with the Anti-Bribery & Anti-Corruption Policy. • Follow reporting requirements for any breaches or suspicious activity. • Maintain accurate and honest records of all business transactions. • Adhere to the policy's requirements in all business interactions.
Business Associates	• Adhere to the Anti-Bribery & Anti-Corruption Policy when representing Identitii's interests. • Report any suspected violations of the policy.

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.
7. Periodic policy review:

Public

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. Familiarise yourself with the Anti-Bribery & Anti-Corruption Policy and adhere to its guidelines and principles at all times.
2. Do not engage in offering, promising, giving, or accepting anything of value to secure an improper advantage or business gain.
3. Refrain from making facilitation payments to expedite routine governmental actions.
4. Ensure all interactions with officials and third parties are ethical and comply with this policy, avoiding any appearance of impropriety.
5. Maintain accurate and complete records of all business transactions, in line with legal requirements and Identitii's accounting and finance policies.
6. Do not make political contributions on behalf of Identitii. Personal political contributions are allowed but must not be linked to Identitii's business interests.
7. Obtain prior approval from a member of the Executive team before making charitable donations on behalf of Identitii.
8. Immediately report any suspected violations of this policy or any laws to the Company Secretary or through the Identitii Whistleblower Policy.
9. Fully cooperate with any audits or investigations related to bribery and corruption conducted by Identitii.
10. Do not use personal funds to engage in any interactions or transactions prohibited under this policy.
11. Seek guidance from the Company Secretary if unsure about the appropriateness of any actions, gifts, or entertainment.

Requirements applicable to line managers

1. Ensure that all team members understand and comply with the Anti-Bribery & Anti-Corruption Policy.
2. Regularly monitor and review team activities to ensure adherence to the policy and detect any potential breaches.
3. Create an environment where employees feel comfortable reporting any suspicious activities or violations of the policy without fear of retaliation.
4. Oversee and review records of business transactions to ensure accuracy and compliance with policy requirements.
5. Provide guidance to team members on ethical interactions with officials and third parties, and consult with the Company Secretary when necessary.
6. Promptly report any suspected violations or concerns related to bribery and corruption to the Company Secretary.
7. Demonstrate a high level of integrity and ethical behaviour in all business dealings, serving as a role model for team members.
8. Ensure proper documentation and record-keeping practices are followed within the team.
9. Integrate anti-bribery and anti-corruption principles into daily operations and decision-making processes.

Public

Principles

Prohibition against bribery and corruption

Identitii strictly prohibits personnel engaging in or tolerating bribery or any other form of corruption. Identitii's corporate values require that in all aspects of business all personnel act honestly, adhere to the highest ethical standards, and act in compliance with all relevant legal requirements.

The prohibition of bribery under this policy includes the provision or conveying of anything of value to any third party, official or family members of officials, whether directly or indirectly, to secure any improper advantage or to obtain or retain business.

This means that personnel must not:

1. Offer, promise or give an item of value with the intention of influencing an official or third party who is otherwise expected to act in good faith or in an impartial manner, to do or omit to do anything in the performance of their role or function, in order to provide Identitii with business or an improper advantage; or
2. Authorise the provision of an item of value to any other person, if it is known, or reasonably should have been known, that any portion of that item of value will be passed onto an official or third party to secure an improper advantage or obtain or retain business; or
3. Engage, or procure, another party to provide an item of value to an official or third party, (or to procure another person to make such provision), in order to secure an improper advantage or obtain or retain business.
4. The prohibition of bribery under this policy also includes the request or acceptance by any personnel of (or the agreement to accept) anything of value from an official or third party either:
    a. intending that, in consequence, a function or activity should be performed improperly (whether by the requestor/acceptor or another person); or
    b. where the request, agreement or acceptance itself constitutes the recipient's improper performance of a function or activity; or
    c. as a reward for the improper performance of a function or activity (whether by the recipient or another person).

Public

Interactions with officials and third parties must be compliant

All interactions with officials and third parties must comply with this policy, and Identitii personnel must not take any actions, whether direct or indirect, which create the appearance of impropriety regardless of whether there is any improper intent behind their actions.

Personnel have separately been provided with the Identitii Code of Conduct as part of the People & Culture Policy, which outlines the guidelines applicable to their business. A copy of the People & Culture Policy can be found on the Identitii website or obtained from the Company Secretary.

If, after considering the People & Culture Policy, you are still in any doubt as to the appropriateness of any gift or entertainment, you should consult the Company Secretary before it is given or accepted or otherwise as soon as possible.

Documentation and record-keeping

As part of Identitii's commitment to open and honest business practices, Identitii requires all of its businesses to maintain accurate books of accounts and records. Identitii and its subsidiaries must keep accurate and complete records of all business transactions:

1. in accordance with the law and generally accepted accounting principles and practices,
2. in accordance with the Identitii's accounting and finance policies, and
3. in a manner that reasonably reflects the underlying transactions and events.

Prohibition on facilitation payments

Identitii does not condone the making of facilitation payments and the making of facilitation payments by any personnel is prohibited.

Political or charitable contributions

Political contributions

Identitii prohibits personnel from making political contributions to candidates for any political office on behalf of any Identitii company. This Policy does not restrict an individual's freedom to make political contributions in their personal capacity.

The context of any other political contributions is key in determining their appropriateness. For instance, it is permissible for Identitii to make a payment to attend a political function in circumstances where such payment could not be construed as an attempt to influence the political party.

If you are in any doubt as to the appropriateness of any political contribution, you should consult with the Company Secretary before it is given or accepted, or otherwise as soon as possible.

Public

Charitable donations

Identitii is committed to the communities in which it does business and encourages and supports employees participating in local community development initiatives, making donations, and undertaking volunteer work. In addition, Identitii and its subsidiaries may support a number of nominated charitable organisations as determined by the local business.

Personnel should only make donations on behalf of Identitii with the prior approval of a member of the Executive team of Identitii or the local business. This Policy does not prevent an individual's freedom to make donations or undertake volunteer work in their personal capacity.

Compliance with local laws

If local laws, codes of conduct, or other regulations in a particular country or region are more restrictive than this policy, then any personnel, including any business associates operating in that country or region must fully comply with the more restrictive requirements.

Reporting violations and suspected misconduct

Any personnel or stakeholder who believes that a violation of this policy or any laws has been committed, is being committed, or is being planned, should report the matter immediately to the Company Secretary or review the guidelines set out in the Identitii Whistleblower Policy. A copy of the Identitii Whistleblower Policy can be found on the Identitii website or obtained from the Company Secretary.

If anyone is unsure whether a particular act constitutes bribery or a facilitation payment, or has any other queries, they should ask the Company Secretary.

Protection

Identitii prohibits retaliation against anyone reporting such suspicions. Personnel who wish to raise a concern or report another's wrongdoing, or who have refused pressure to either accept or offer a bribe, should not be worried about possible repercussions. Identitii encourages openness and will support any Personnel who raises genuine concerns in good faith, in line with the Whistleblower Policy.

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.

Bribery and the related improper conduct addressed by this policy are very serious offences. If Identitii or one of its subsidiaries is found to have taken part in bribery or any other related improper conduct addressed by this policy it could face a fine and suffer reputational harm.

Breach of this policy by personnel will be regarded as serious misconduct, leading to disciplinary action which may include termination of employment, and individuals may be subject to penalties or lengthy terms of imprisonment. Breach of this policy by a business associate will be regarded as a material breach for the purposes of termination of the agreement with the Business Associate.

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.

Public

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 financial audits, 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.

Public

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 HR, 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.

Public

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 Identitii Anti-Bribery & Anti-Corruption Policy is a comprehensive framework designed to ensure the company adheres to stringent global anti-corruption laws while fostering a culture of integrity and ethical business practices. Key aspects of the policy include clear definitions, the prohibition of bribery and corruption, and strict guidelines for interactions with officials and third parties. The policy mandates thorough documentation, regular training, and clear reporting mechanisms to detect and address violations promptly.

Public