Confidentiality Policy

1. Preamble

Abet Management Consulting Private Limited (the Company) is committed to delivering services of the highest standards. In order to achieve this, the responsible handling of information, especially sensitive or confidential information, is vital. In recognition of this, our organization has established this Confidentiality Policy to govern the management of all confidential information within the firm. The Company recognizes that employees and personnel, in the course of their duties, may have access to confidential information, which must be protected.

This policy outlines the principles and measures taken to ensure that all confidential information is handled with care, and that confidentiality is maintained in all aspects of the firm's operations. The firm is committed to meeting all legal and regulatory obligations concerning confidentiality, ensuring that the information handled within the organization. Additionally, our organization shall ensure confidentiality of information obtained in the course of its certification activities by implementing a suitable system that ensures the protection of such confidential data.

2. Purpose

Information is an asset which, like other important business assets, has value to an organisation and consequently needs to be suitably protected. Processing and transmission of personal data on individuals who can be identified from the information has legislative controls placed on them. The objective of this document is to provide management direction and support for data protection.

The term 'Data Protection Law' encompasses the Digital Personal Data Protection Act, 2023, the Indian Information Technology Act, 2000, and the Indian Aadhar Act, 2016. This policy outlines the Company’s compliance framework for processing information related to its workforce, clients, project beneficiaries, and stakeholders.

It ensures that the processing of any personal data, including special category personal data, complies with the Digital Personal Data Protection Act, 2023. The Company is committed to embedding robust data protection practices within the culture of our staff and organisation.

3. Confidential Information

Confidential information includes any information that is not publicly known and may relate to technology, business, finance, transactions, or other matters of the company. It includes commercially valuable information such as trade secrets, business information, and personal data.

Examples of confidential information include, but are not limited to:

- Any document, discovery, invention, improvement, patent specification, formulations, plans, ideas, books, accounts, data, reports, drafts of documents, correspondence, client information, lists and files, decisions, information about employees, strategies, drawings, recommendations, designs, office precedents, policies, and procedures.
- Budget and financial information in any form (physical, electronic, electromagnetic, etc.).

Confidential information relating to unpublished inventions is especially sensitive. Disclosing an invention before filing a patent application results in the irreversible loss of intellectual property rights. Even after a patent application is filed, care must be taken not to disclose improvements to the invention. Trade secret protection can also be compromised through unauthorized disclosure.

4. Guiding Principles

To maintain the highest standards of confidentiality, all employees, contractors, and personnel of The Company must adhere to the following core principles:

a. Integrity and Trustworthiness

Every individual must act with integrity when handling confidential information. Trust is the foundation of our relationships with clients, collaborators, and employees. All actions taken

regarding confidential information must reflect the commitment to protecting it from unauthorized access or disclosure.

b. Confidentiality in Certification Activities
In the course of its certification activities, The Company ensures that all confidential information obtained is treated with the highest level of care. A suitable system will be implemented to maintain confidentiality and protect sensitive information related to certification processes. This principle ensures that no confidential data is disclosed during or after the certification process, safeguarding both the firm and its clients.

c. Need-to-Know Basis
Confidential information should only be disclosed on a "need-to-know" basis. It must be shared exclusively with individuals who require access to the information to perform their specific job functions. Disclosures should be limited to the minimum amount of information necessary.

d. Responsible Handling of Information
Confidential information should be handled with due diligence, care, and professionalism. This includes ensuring that physical and digital files are secure, managing access to sensitive data, and using proper storage and transmission methods to avoid exposure.

e. Compliance with Legal and Regulatory Requirements
All employees and personnel are expected to comply with relevant legal and regulatory requirements concerning confidentiality, including data protection laws, intellectual property rights, and any other legal obligations related to sensitive information.

5. Applicability

This policy shall be applicable to all projects, departments, establishments, and associated networks of The Company We are reaffirming our organization commitment to safeguarding confidential information and ensuring its protection across all operations. This policy underscores the company's responsibility to uphold the highest standards of confidentiality, minimize the risk of unauthorized disclosure, and contribute to the sustainable and secure development of the organization, its people, and its clients. This Policy will be communicated to all Joint Ventures, Subsidiaries, and affiliates of The Company, ensuring its adoption and implementation. The policy will be adapted where necessary to fit the specific operational contexts, confidentiality-related challenges, and regulatory requirements of each entity within the organization.

6. Maintenance of Confidentiality

Abet Management Consulting Private Limited employees and personnel:

- Must keep all confidential information secure.
- May use confidential information only for the purpose of performing their duties.
- May only disclose confidential information to individuals who are aware of the need for confidentiality and who have a legitimate "need to know" (and only to the extent that each person needs to know).

Employees' and personnel's obligation to maintain confidentiality extends to all types of sensitive information, including information obtained during certification activities. Our organization ensures that a suitable system is in place to protect confidential information gained through certification processes, preventing any unauthorized access, disclosure, or misuse of such information. The duty of confidentiality and non-disclosure continues even after the end of employment or engagement. Any breach may result in disciplinary action, dismissal, or legal consequences.

7. Storage of Confidential Information

Confidential documents and data must never be left visible or accessible to unauthorized individuals. This includes but is not limited to telephone messages, printouts, letters, and other documents containing confidential information.

- All hardware (such as computers, storage devices, and servers) containing confidential information must be securely stored in compliance with organization policies and procedures.

- Confidentiality of information obtained during certification activities must also be safeguarded. Our organization ensures that appropriate systems are in place to protect any confidential data collected or generated during certification processes, minimizing risks of unauthorized disclosure, misuse, or access
- Physical storage of confidential documents must be conducted in a manner that ensures their protection from unauthorized access, including locked cabinets, secure filing systems, and access-controlled areas.
- Electronic data must be stored in secure environments with encryption and password protections to prevent unauthorized access, alteration, or loss of confidential information.

Data Protection

To ensure the protection of client and audit data, robust encryption protocols are implemented both when stored and in transmission:

- Data is encrypted using industry standards for transmission, safeguarding sensitive information from unauthorized access or interception.
- Additionally, data is stored in secure, access-controlled environments with strict identity and authentication mechanisms, including multi-factor authentication (MFA) and role-based access controls (RBAC), ensuring only authorized personnel can access critical information.
- Comprehensive disaster recovery and business continuity plans are in place to maintain data integrity and availability.
- Regular backups are performed and securely stored in geographically redundant locations.
- Recovery procedures are tested periodically to ensure rapid restoration in the event of system failure, cyberattack, or natural disaster, thereby minimizing downtime and ensuring continuity of services.

8. Confidentiality Agreement

All personnel, assessors, and contractors involved in accreditation and certification activities are required to sign Confidentiality agreement. These agreements are a key part of our organization commitment to maintaining the highest standards of confidentiality.

The confidentiality agreements:

- Reinforce the obligation of all individuals to maintain the confidentiality of sensitive information they may come across during their involvement in accreditation or certification activities.
- Clearly outline the consequences for breaches of confidentiality, including disciplinary actions, dismissal, or legal consequences, depending on the severity of the breach.
- Specifically address the confidentiality of information obtained during certification activities, ensuring that proper systems are in place to protect such information from unauthorized disclosure or misuse.
- Ensure that confidentiality is upheld during all stages of the certification process, from initial data collection to final reporting, and that sensitive data remains secure throughout the lifecycle of the certification activities.

9. Sharing of Information

Confidential information is only shared with individuals or entities directly involved in the accreditation and certification process. Sharing beyond this scope requires:

- Explicit consent from the affected parties involved.
- Or sharing in accordance with legal and regulatory requirements, as mandated by law or authorized authorities.

The sharing of confidential information obtained during certification activities is strictly controlled. A suitable system is implemented to ensure that such information is only shared with authorized parties and remains protected throughout the certification process.

10. Non-Disclosure to Third Parties:

The Company shall not disclose confidential information to third parties without the explicit written consent of the affected party, except when required by law or regulatory authorities. This includes:

- Information obtained during certification activities, which is treated with the utmost confidentiality.
- A suitable system is in place to ensure that any confidential information from certification processes is not disclosed to unauthorized third parties unless required by legal or regulatory obligations.

Confidentiality agreements and internal controls are in place to ensure that all parties involved in certification and accreditation activities adhere to this non-disclosure policy.

11. Reporting Breaches

Any suspected or actual breaches of confidentiality must be reported immediately to the designated individual or department responsible for managing breaches. The report should include details of the breach and any potential impact on confidentiality.

Upon receiving the report:

- An investigation will be conducted to determine the nature and scope of the breach.
- Corrective actions will be taken as necessary to address the breach and prevent further incidents.

This includes breaches related to the confidentiality of information obtained during certification activities. Our organization has implemented a suitable system to identify, report, and manage such breaches to ensure that any confidential information associated with certification activities remains protected. Any breach related to this information will be treated with the same level of seriousness as other confidentiality violations and will result in appropriate disciplinary or legal action, depending on the severity of the breach.

12. Roles and Responsibilities

a. Executive Team

- Provide strategic oversight of the confidentiality policy and ensure its alignment with the organization's overall business strategy and risk management processes.
- Approve and periodically review the confidentiality and non-disclosure objectives, ensuring that adequate systems and controls are in place to protect sensitive information.
- Ensure that confidentiality principles are integrated into all organizational functions, including accreditation activities, internal processes, and external collaborations.

b. All Employees

- Adhere to internal guidelines for maintaining confidentiality, including the secure handling, storage, and sharing of sensitive information.
- Participate in training programs related to confidentiality and data security, staying informed about the organization's policies and procedures.
- Actively contribute to the protection of confidential information by following best practices in daily work activities, including the appropriate handling of information obtained during certification activities and ensuring its confidentiality.

c. Suppliers and Collaborators

- Encourage and, where possible, require suppliers and collaborators to align with The Company's confidentiality objectives, particularly regarding information related to certification activities.
- Ensure that all third parties involved in certification or accreditation processes adhere to the same confidentiality standards, safeguarding sensitive information throughout their operations.
- Foster a collaborative approach in which all external parties contribute to maintaining the confidentiality of information and protect it from unauthorized disclosure.

13. Communication and Training

- Policy Awareness**:** This policy shall be communicated internally through orientation sessions, trainings, the company intranet, and other relevant channels. It will also be made publicly available on our website.
- Training**:** This training will also include specific guidance confidential data throughout the certification process and prevent any unauthorized disclosure on the confidentiality of information obtained during certification activities. Our organization ensures that all relevant individuals are trained on the suitable system designed to protect.

14. Review and Amendments

This Confidentiality Policy will be reviewed at least annually—or sooner, if necessary—to ensure it remains up-to-date, effective, and aligned with evolving legal, regulatory, and industry standards related to confidentiality and data protection**.** The policy will also take into consideration new developments in technology, best practices in data security, and emerging risks to confidential information, particularly in the context of certification and accreditation activities.

Whenever updates or modifications to the policy are made, the organization will ensure these changes are clearly communicated to all employees, subsidiaries, contractors, and relevant stakeholders to promote understanding, compliance, and ongoing commitment to maintaining confidentiality and protecting sensitive information.

15. Policy Breach

Breaching this Confidentiality Policy may result in disciplinary action for misconduct, including dismissal. Unauthorized access to, or disclosure of, confidential information in breach of The Company's confidentiality policy may also be treated as a serious offence**.** The company reserves the right to terminate its contractual relationship with employees, associates, and other stakeholders if they breach any of the terms and conditions outlined in this policy. Such actions may also lead to legal consequences, depending on the severity of the breach and the nature of the information involved.

16. Approval and Implementation

This policy has been reviewed and approved by the Company's executive management. It enters into effect as of the date indicated and shall remain in force until reviewed or amended.