CONFIDENTIALITY POLICY

1. **Purpose:**

   This Confidentiality Policy outlines the commitment of NIHA to maintain the confidentiality and security of information related to its certification activities, in accordance with relevant requirements.

2. **Scope:**

   This policy applies to all personnel, including employees, contractors, and external parties, involved in any aspect of the certification process within the organization.

3. **Confidential Information:**
   a. Definition:
      - Confidential information includes, but is not limited to, client data, certification documents, audit reports, and any information obtained during the certification process.

   b. Handling:
      - All confidential information shall be handled with the utmost care and discretion.

4. **Responsibilities:**
   a. Management:
      - Senior management is responsible for overseeing the implementation of confidentiality measures and ensuring compliance with all relevant requirements.

   b. Employees and Contractors:
      - All personnel involved in the certification process are responsible for protecting the confidentiality of information and reporting any breaches.

5. **Confidentiality Measures:**
   a. Access Control:
      - Limit access to confidential information to authorized personnel only.
      - Implement secure login credentials, role-based access, and physical security measures.

   b. Training:
      - Provide training to personnel on the importance of confidentiality and their responsibilities.
      - Ensure awareness of legal and contractual obligations related to confidentiality.

6. **Non-Disclosure Agreements:**
   a. Client Agreements:
      - Include confidentiality clauses in agreements with clients to emphasize the importance of information security.

   b. Contractors and External Parties:

- Ensure that contractors and external parties sign non-disclosure agreements before engaging in any certification-related activities.

7. **Information Handling Procedures:**
   a. Secure Storage:
      - Store physical and electronic documents containing confidential information in secure and locked facilities.
      - Implement encryption and access controls for electronic storage.
   b. Data Transmission:
      - Utilize secure communication channels when transmitting confidential information.
      - Avoid discussing sensitive matters over non-secure communication platforms.

8. **Incident Reporting:**
   a. Breach Reporting:
      - Establish a clear process for reporting any suspected or actual breaches of confidentiality.
      - Investigate and take corrective actions in the event of a breach.

9. **Confidentiality Duration:**
   a. Post-Certification:
      - Maintain confidentiality beyond the certification period.
      - Dispose of confidential information securely, in compliance with applicable legal and regulatory requirements.

10. **Legal and Regulatory Compliance:**
    a. Compliance Review:
       - Regularly review and update confidentiality practices to ensure compliance with all relevant standards, as well as relevant legal and regulatory requirements.

11. **Continuous Improvement:**
    - Regularly review and update this policy to ensure alignment with relevant requirements and the continuous improvement of confidentiality measures.

12. **Communication:**
    - Communicate this confidentiality policy to all personnel involved in the certification process and ensure their understanding and adherence.

13. By following this Confidentiality Policy, NIHA aims to maintain the trust and confidence of its clients, uphold the integrity of the certification process, and comply with all relevant standards and other applicable legal and regulatory requirements.