AMENDMENT RECORD

DCRF	PAGE NO.	REVISION NO.	DATE REVISED	CHANGES
	03	00	01/01/2022	Minor changes in the 'applicability' section
	04	01	12/03/2025	Addition of requirement to enhanced confidentiality and security measures.

Prepared By
Ms. Injela Akhtar
Manager Operations /MR
Last Reviewed Dated: 12/3/2025

Approved By
Mr. Zeeshan Abdul Aziz
CEO
Last Reviewed Dated: 12/3/2025

Table of Contents

1. Introduction 3

2. Applicability 3

3. Procedure 3

4. Related Documents 5

1. Introduction

This procedure describes the measures taken by Acerta Certification & Inspection Private Limited (ACI) to ensure that information obtained in the course of client certifications is held appropriately confidentially at all levels of the organization, including sub-contractors as required by following standards & guidelines:

- ISO/IEC 17065:2012, Conformity assessment- Requirements for bodies certifying products, processes and services.
- ISO/IEC 17021-1-2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems.
- ISO/IEC 17021-2:2016, Conformity assessment— Requirements for bodies providing audit and certification of management systems Part 2: Competence requirements for auditing & certification of environmental management systems.
- ISO/IEC 17021-3:2017, Conformity assessment— Requirements for bodies providing audit and certification of management systems Part 3: Competence requirements for auditing & certification of quality management systems.
- ISO/IEC 17021-10:2018, Conformity assessment— Requirements for bodies providing audit and certification of management systems Part 3: Competence requirements for auditing & certification of Occupational Health & Safety Management systems.
- ISO 22003-1-2022, Food Safety- Part 1: Requirements for Bodies Providing audit & certification of food safety management systems.
- G-02/19-Rev 07, PNAC Guidelines of Accreditation Conditions for Certification Bodies.

2. Applicability

This procedure applies to all Acerta Certification & Inspection Private Limited (ACI) employees and subcontractors in ongoing activities undertaken to avoid conflicts of interest, and confidentiality management during certification of management systems.

3. Procedure

3.1 ACI personnel are exposed to a significant amount of proprietary information regarding client products, facilities, organization, and procedures in the conduct of certification programs.

3.2 Ensuring that this information is kept confidential is a major concern to ACI. Measures to preserve confidentiality are implemented in informing personnel and in the administrative and procedural structures of the certification systems. The following measures are implemented:

3.3 ACI has through legally enforceable agreements, has a policy and arrangements to safeguard the confidentiality of the information obtained or created during the performance of certification activities at all levels of its structure, including committees and external bodies or individuals acting on its behalf.

3.4 ACI informs the client, in advance, of the information it intends to place in the public domain. Confidential treatment of client processes and procedures is discussed with client

management at the opening meeting. All other information, except for information that is made publicly accessible by the client, shall be considered confidential.

3.5 Except as required in ISO 17021-1-2015 & ISO+IEC 17065:2012 Standards - PNAC guidelines, information about a particular client or individual shall not be disclosed to a third party without the written consent of the client or individual concerned.

3.6 Where the ACI is required by law to release confidential information to a third party, the client or individual concerned shall, unless regulated by law, be notified in advance of the information provided.

3.7 Information about the client from sources other than the client (e.g. Complainant, regulators) is treated as confidential, consistent with the certification body's policy.

3.8 Personnel, including any committee members, contractors, personnel of external bodies or Individuals acting on the certification body's behalf, would keep confidential all information obtained or created during the performance of the ACI ‘s activities.

3.9 ACI uses equipment and facilities that ensure the secure handling of confidential information (e.g. Documents, records).

3.10 When confidential information is made available to other bodies (e.g. An accreditation body), the certification body shall inform its client of this action.

3.11 The employment agreement signed by each employee contains a declaration of confidentiality of third party and company information.

3.12 Subcontracted auditors are required to sign a Non-Disclosure Agreement that indicates that they will hold all client information in the strictest confidentiality.

3.13 Client documents submitted to and retained by ACI are safeguarded in electronic format as well as in Hard copy in respective clients’ files.

3.14 ACI’s working documents containing proprietary client information are handled with discretion and maintained in electronic files.

3.15 Records pertaining to client certification programs are safeguarded for at least 5 years during with limited access by ACI personnel.

3.16 Special arrangements regarding confidentiality may be submitted by the client.

3.17 Clients are informed that certification files held by ACI are subject to review by industry and accreditation agencies.

4.00 Enhanced Confidentiality and Security Measures

To ensure the highest level of confidentiality and security, IHC has made it mandatory to restrict access to all devices and systems using password authentication and security protocols, ensuring only authorized personnel have clearance. Wi-Fi networks must be secured and encrypted to prevent unauthorized access and data breaches. Shared office resources, including printers, must not be used for confidential documents; instead, dedicated printers must be configured before printing. Sensitive discussions must take place only in designated meeting rooms to prevent eavesdropping or information leaks. No confidential files may be stored in shared spaces, and all sensitive information must be stored in designated, secure locations with proper lock and key mechanisms. Additionally, all employees must undergo regular training on handling confidential information, following best practices, and reporting security risks to maintain compliance with confidentiality procedures. Failure to adhere to these mandatory requirements may result in corrective actions to uphold IHC’s commitment to security and

privacy.

4. Related Documents

1. Confidentiality Policy (ACI-CP-001)
2. Non-Disclosure Agreement (ACI-F034)