PCA GLOBAL SERVICES LLP

CONFIDENTIALITY POLICY

Document No.	CB-POLICY-CONFIDENTIALITY-001
Version	1.0
Date	2025-04-23

REVISION HISTORY

SR NO.	DATE OF REVISION	VERSION	DESCRIPTION OF CHANGE	CHANGED BY	REVIEWED & APPROVED BY

TABLE OF CONTENTS

1. Policy Statement

PCA Global Services recognizes the importance of maintaining the confidentiality of information entrusted to us by our clients and stakeholders. We are committed to protecting all confidential information obtained or created during our certification activities, ensuring its security and preventing unauthorized access or disclosure.

This Confidentiality Policy establishes our commitment to:

- **Protect Client Information:** Safeguard all confidential information of our clients, including proprietary information, management systems documentation, audit findings, and certification status.
- **Legal and Contractual Obligations:** Comply with all applicable legal, regulatory, and contractual requirements related to confidentiality and data protection.
- **Data Security:** Implement and maintain appropriate security measures to protect confidential information from unauthorized access, use, disclosure, alteration, or destruction, whether in physical or electronic form.
- **Limited Disclosure:** Limit the disclosure of confidential information to only those individuals or entities who have a legitimate need to know and are bound by confidentiality obligations, or as required by law or accreditation requirements.
- **Maintain Trust:** Foster a culture of trust and confidence with our clients and stakeholders by demonstrating a strong commitment to confidentiality.

This policy applies to all personnel of PCA Global Services, including employees, auditors, technical experts, committee members, subcontractors, and any other individuals acting on our behalf.

2. Scope

This Confidentiality Policy applies to all information, in any form (verbal, written, electronic, visual), that is:

- **Client-Specific Information:** Information about a specific client organization, its management system, operations, products, services, processes, personnel, and any other proprietary or sensitive data disclosed to PCA Global Services during the application, audit, certification, surveillance, and recertification processes.
- **Audit Information:** Information generated during audits, including audit plans, audit findings, nonconformities, audit reports, and related working papers.
- **Certification Decision Information:** Information related to certification decisions, including the rationale for decisions and any deliberations of certification committees or decision-makers.
- **Complaint and Appeal Information:** Information related to complaints and appeals received from clients or other parties, including the details of the complaint/appeal, investigation findings, and resolution actions.
- **Stakeholder Confidential Information:** Confidential information received from other stakeholders, such as accreditation bodies, regulatory agencies, or partner organizations.

- **Personnel Confidential Information:** Confidential personal data of PCA Global Services' personnel, in accordance with applicable data protection laws.
- **Business Confidential Information:** PCA Global Services' own internal confidential business information, such as strategic plans, financial data, proprietary processes, and intellectual property.

3. Principles and Objectives

To support the effective implementation of this Confidentiality Policy, PCA Global Services commits to the following principles and objectives, ensuring the protection of all confidential information obtained or created during its certification activities:

Information Protection and Integrity

- Identify and classify all confidential information received from or related to clients, personnel, or third parties.
- Protect confidential information from unauthorized access, disclosure, alteration, or destruction.
- Ensure that information is used solely for its intended purpose and only by authorized individuals.
- Apply appropriate administrative, technical, and physical safeguards to secure sensitive data.

Personnel Awareness and Accountability

- Ensure that all personnel, including internal staff, auditors, technical experts, and contractors, are fully aware of their confidentiality obligations.
- Require all relevant personnel to sign confidentiality and non-disclosure agreements.
- Regularly train employees and contracted personnel on confidentiality requirements and data handling protocols.
- Hold personnel accountable for any breach or mishandling of confidential information.

Legal and Regulatory Compliance

- Comply with all applicable legal, regulatory, and contractual obligations relating to data confidentiality and information protection.
- Fulfill any data protection requirements in accordance with local and international regulations, including but not limited to GDPR, if applicable.
- Cooperate fully with authorities in cases where disclosure is legally required, while informing the client when permitted by law.

Secure Communication and Data Storage

- Utilize secure communication channels when transmitting sensitive information.
- Store confidential information using encrypted or access-controlled systems.
- Restrict physical and digital access to client data based on role and necessity.

- Ensure secure disposal or deletion of information once its retention period has expired or when it is no longer needed.

Third-Party and Subcontractor Controls

- Ensure that any third-party or subcontracted entity engaged by PCA Global Services adheres to equivalent confidentiality and data protection standards.
- Include confidentiality clauses in all third-party agreements and monitor compliance regularly.
- Prohibit unauthorized sharing or use of confidential information by external parties.

Client Transparency and Consent

- Inform clients about the confidentiality measures in place and how their data will be handled.
- Obtain explicit client consent when required, particularly for data use beyond the certification scope.
- Respond promptly to any client concerns or inquiries related to confidentiality.

Breach Prevention and Response

- Monitor systems and processes proactively to detect potential confidentiality breaches.
- Establish procedures for timely reporting, investigation, and resolution of confidentiality incidents.
- Take corrective and preventive actions to address root causes and prevent recurrence.
- Notify affected stakeholders where appropriate and in accordance with legal obligations.

Continual Improvement

- Periodically review and improve confidentiality policies, procedures, and controls.
- Conduct internal audits and management reviews to assess effectiveness.
- Integrate lessons learned from breaches, audits, and client feedback to strengthen the confidentiality framework.

4. Records

The following records shall be maintained in accordance with the PCA Global Services Record Management Procedure (CB-PROC-RECORD-MANAGE-001):

- Signed Confidentiality Agreements or Declarations for all personnel
- Records of Confidentiality Training provided to personnel
- Logs of access to sensitive confidential information
- Records of authorizations for disclosure of confidential information
- Documentation of any breaches of confidentiality, investigations, and corrective actions taken
- Records of review and updates to the Confidentiality Policy

5. Review and Communication

This Confidentiality Policy shall be:

- **Reviewed for continuing suitability** at least annually during management review, or more frequently, if necessary, to ensure it remains relevant and effective.
- **Communicated and made available** to all personnel within PCA Global Services and to relevant external stakeholders, including clients and the public.
- **Understood and implemented** by all personnel involved in certification activities.

[Signature of Top Management Representative]

[Name and Title of Top Management Representative]

[Date of Approval]

