厦门广信隆技术服务有限公司

Al-Baqara Certification

保密政策

Confidentiality Policy

文件编号:（Document No.）	ABC-PD-008
版本号:（Version No.）	A0
编制:（Compiled by）	韩锐
审核:（Reviewed by）	评审组 Review Group
批准:（Approved by）	沙忠虎
修订日期:（Revision Date）	

发布日期（Issuance Date）**:** **2026.4.5**	**实施日期**（Implementation Date）**:** **2026.4.5**

修订次数（Revision Times）	修订日期（Revision Date）	修改内容/原因 （Modification Content/Reason）	更改人（Modifier）	审核人（Reviewer）	批准人（Approver）

保密政策
Confidentiality Policy

1. 目的 / Purpose

为保护客户商业秘密、技术信息及认证过程相关未公开信息，防范信息泄露，依据 ISO/IEC 17065:2012 第 4.5 条及相关法律法规，建立保密机制、明确保密程序、制定本政策。

To protect clients’ trade secrets, technical information and non-public information related to certification activities, prevent information leakage, and establish confidentiality mechanisms, define confidentiality procedures and formulate this policy in accordance with Clause 4.5 of ISO/IEC 17065:2012 and relevant laws and regulations.

2. 适用范围 / Scope

适用于厦门广信隆技术服务有限公司（AL-BAQARA CERTIFICATION，简称 ABC）全体人员（含员工、审核员、技术专家、评审员、管理人员、外包人员、实习生），以及认证活动全过程中接触、处理、存储、传输、销毁客户信息与机构涉密信息的所有环节。

Applicable to all personnel of Xiamen Guangxinlong Technical Service Co., Ltd. (AL-BAQARA CERTIFICATION, hereinafter referred to as ABC), including employees, auditors, technical experts, reviewers, management staff, outsourced personnel and interns; and all stages of certification activities involving access, processing, storage, transmission and destruction of client information and confidential information of ABC.

3. 保密原则 / Confidentiality Principles

3.1 全程保密：从申请受理、合同评审、现场审核、技术评审、认证决定、发证、监督至证书暂停/撤销，全流程严格保密。

Full-process confidentiality: Strict confidentiality throughout application acceptance, contract review, on-site audit, technical review, certification decision, certification issuance, surveillance, suspension or withdrawal.

3.2 授权披露：仅在法律法规要求、客户书面授权、法定监管机构核查三种情形下可披露涉密信息。

Authorized disclosure: Confidential information may only be disclosed under three circumstances: legal requirements, written client authorization, or inspection by statutory regulatory authorities.

3.3 最小知悉：涉密信息仅限工作必需人员知悉，严禁无关人员接触。

Need-to-know: Confidential information is accessible only to personnel with job necessity; access by irrelevant personnel is strictly prohibited.

3.4 终身责任：保密义务不因离职、外包关系终止而失效，终身有效。

Lifetime obligation: Confidentiality obligations survive termination of employment or outsourcing relationship and remain permanently effective.

4. 保密信息范围 / Scope of Confidential Information

- 客户商业信息：配方、工艺、图纸、成本、报价、客户名单、销售数据、财务信息；
- Client business information: Formulas, processes, drawings, costs, quotations,

customer lists, sales data, financial information;
- 客户技术信息：生产技术、检验方法、质量控制文件、未公开标准；
- Client technical information: Production technologies, testing methods, quality control documents, non-public standards;
- 认证过程信息：审核报告、不符合项、评审意见、认证决定草案、涉密沟通记录；
- Certification process information: Audit reports, non-conformities, review comments, draft certification decisions, confidential communication records;
- 机构涉密信息：内部管理制度、评审规则、人员信息、收费明细、未公开政策。
- ABC confidential information: Internal management systems, review rules, personnel information, fee details, non-public policies.

5. 保密机制 / Confidentiality Mechanisms

5.1 人员保密承诺：所有人员入职/上岗前签署《保密承诺书》，明确保密责任与违约后果。
Personnel confidentiality commitment: All personnel sign a Confidentiality Commitment before employment/assignment, clarifying confidentiality responsibilities and breach consequences.

5.2 权限分级管控：信息系统按岗位设置访问权限，分级授权、全程留痕、操作可追溯。
Hierarchical access control: Information systems adopt role-based access permissions with hierarchical authorization, full-process logging and traceable operations.

5.3 物理安全防护：涉密文件专柜上锁存放；办公区域门禁管理；审核资料专人保管、专柜存放。
Physical security protection: Confidential documents stored in locked cabinets; office areas with access control; audit materials kept by designated personnel in secure storage.

5.4 信息系统安全：电脑设置强密码、定期更换；禁用外接设备（U 盘、移动硬盘）；涉密文件加密存储；网络传输加密；定期安全审计。
Information system security: Strong passwords with regular updates; external devices (USB, hard drives) restricted; confidential files encrypted; network transmission encrypted; regular security audits.

5.5 外包保密约束：与外包方签署《保密协议》，明确责任、违约赔偿及终身保密义务。
Outsourcing confidentiality binding: Sign Confidentiality Agreements with outsourced parties, defining responsibilities, compensation for breaches and lifelong confidentiality obligations.

6. 保密程序 / Confidentiality Procedures

6.1 信息收集与接收 / Information Collection & Receipt
- 仅收集认证必需信息，不额外索取无关涉密内容；
- Collect only information necessary for certification; no additional irrelevant confidential data shall be requested;
- 接收涉密资料时登记台账，注明来源、日期、用途、保管人。
- Register confidential materials upon receipt, recording source, date, purpose and

custodian.
6.2 信息存储与保管 / Information Storage & Retention
- 电子文件：加密存储于机构专用服务器，定期备份、异地存档；
- Electronic files: Encrypted storage on dedicated ABC servers with regular backups and off-site archiving;
- 纸质文件：分类编号、专柜上锁、专人管理、借阅登记、限时归还；
- Paper documents: Classified, numbered, stored in locked cabinets, managed by designated personnel, checked out with registration and returned on time;
- 禁止私自复印、拍照、摘抄、外传涉密信息。
- Unauthorized copying, photographing, excerpting or external distribution of confidential information is prohibited.
6.3 信息传输与共享 / Information Transmission & Sharing
- 内部共享：仅限授权人员，通过加密系统传输；
- Internal sharing: Limited to authorized personnel via encrypted systems;
- 对外传输：客户信息仅发送至客户指定授权联系人，全程加密；
- External transmission: Client information sent only to client-designated authorized contacts with full encryption;
- 严禁通过微信、QQ、私人邮箱、公共网盘传输涉密信息。
- Transmission of confidential information via WeChat, QQ, personal email or public cloud drives is strictly prohibited.
6.4 信息销毁 / Information Destruction
- 纸质文件：使用专用碎纸机彻底销毁，销毁记录存档；
- Paper documents: Shredded completely using dedicated shredders; destruction records archived;
- 电子文件：彻底删除+磁盘粉碎，不留备份痕迹；
- Electronic files: Permanent deletion + disk wiping with no residual backups;
- 废弃载体（U 盘、硬盘）：专业物理销毁，防止数据恢复。
- Obsolete media (USB, hard drives): Professional physical destruction to prevent data recovery.
6.5 离职/外包终止处理 / Termination Handling
- 离职/终止时，立即收回所有涉密资料、设备、系统权限；
- Upon termination, all confidential materials, equipment and system access rights are immediately revoked;
- 签署《离职保密承诺书》，重申终身保密义务；
- Sign a Post-Termination Confidentiality Commitment reaffirming lifelong obligations;
- 定期回访，核查保密遵守情况。
- Conduct regular follow-up reviews of confidentiality compliance.
7. 信息披露审批 / Disclosure Approval
任何涉密信息对外披露，须提交《信息披露申请表》，经部门负责人→管理者代表→总经理逐级审批，书面留存审批记录，方可按批准范围、方式、对象披露。
Any external disclosure of confidential information requires submission of an Information Disclosure Application Form, with written approval recorded through

Department Head → Management Representative → General Manager; disclosure may only proceed within the approved scope, method and recipients.

8. 违规责任 / Breach Liability

8.1 违反本政策者，视情节轻重给予警告、罚款、降职、辞退；
Violations of this policy shall result in warning, fine, demotion or dismissal depending on severity;

8.2 造成经济损失或声誉损害的，依法追究民事赔偿责任；
Those causing economic or reputational damage shall be held liable for civil compensation in accordance with the law;

8.3 涉嫌违法犯罪的，移交司法机关处理，追究刑事责任。
Suspected criminal offenses shall be referred to judicial authorities for criminal liability.

9. 监督与改进 / Supervision & Improvement

由管理者代表负责监督本政策实施，定期开展保密检查、风险评估、内部审核，持续完善保密机制与程序，确保有效执行。

The Management Representative oversees implementation of this policy, conducting regular confidentiality inspections, risk assessments and internal audits to continuously improve confidentiality mechanisms and procedures and ensure effective implementation.

10. 生效 / Effectiveness

本文件自发布之日起生效，ABC 全体人员须严格遵守。

This document shall take effect as of the issuance date and shall be strictly complied with by all ABC personnel.