数据安全管理规程

1.目的

为规范本机构认证活动中的记录管理与数据安全保密工作，确保认证全过程的可追溯性、数据的完整性、保密性及合规性，严格遵循《中华人民共和国数据安全法》、《中华人民共和国网络安全法》及相关法规要求，特制定本规程。

2.适用范围

适用于本机构在中华人民共和国境内开展的所有认证活动中产生的一切记录和数据的生成、收集、存储、处理、传输、保存及处置的全过程管理。

3.职责

3.1 最高管理者（总经理）：负责提供建立和实施记录与数据安全管理体系所需的资源。

3.2 管理者代表：负责本规程的全面推行、监督和协调，并向最高管理者报告绩效。

3.3 各部门：负责本部门业务范围内认证记录的及时、真实、准确生成与初步整理，严格执行数据安全规定。

3.4 办公室：负责提供安全、合规的信息技术环境，确保存储在境内的电子数据得到有效保护，并负责实施数据安全技术措施。

4.工作程序

4.1 数据安全与保密管理

4.1.1 数据分类与识别：在认证活动中收集和产生的客户信息、认证决定、审核/检查报告、产品检测报告、合同协议等，凡能单独或组合识别特定企业或个人信息的数据，均被视为重要数据，必须纳入本规程管理范围。

4.1.2 数据存储本地化：所有在认证活动中收集和产生的重要数据，其物理服务器和存储设备必须设置在中华人民共和国境内。办公室需定期检查并确保数据存储的物理位置和逻辑位置符合境内存储的要求。

4.1.3 数据安全保护：OCD 应采取必要的技术措施（如加密、访问控制、防火墙、防病毒、备份等）和管理措施，确保信息和数据的保密性、完整性和可用性，防止数据泄露、篡改或丢失。

数据访问权限应遵循“最小必要原则”，仅授权给因工作需要必须接触该数据的员工。

4.1.4 数据出境严格管制：原则上，存储在境内的数据不得向境外任何组织或个人进行传输、提供或公开。如因业务合作等特殊情况确需出境的，必须由申请使用部门负责人发起申请，办

公室组织相关人员进行安全风险评估，并报国家网信部门等主管机构批准后方可执行。严禁未经批准擅自出境数据。

若其他法律、行政法规对数据出境有特别规定的，从其规定。

4.2 认证记录管理

4.2.1 认证记录的建立与内容：

认证过程中形成的记录也是需要保密管理的数据。

OCD 应建立覆盖认证全过程的记录保持制度，记录应包括但不限于：认证申请与合同评审记录；审核/检查报告计划；现场审核/检查记录；审核/检查报告；样品检测报告；认证决定审批表；认证证书；客户投诉与申诉处理记录等。

记录形式可包括纸质文件和电子数据。

4.2.2 认证记录的质量要求

——真实性：记录必须客观反映认证活动的实际情况，严禁伪造、篡改。

——准确性：记录内容应清晰、明确，无歧义，能够有效证实认证活动的符合性和有效性。

——语言要求：所有记录资料必须使用中文。如原始资料为外文，应附有经确认的中文翻译件。

4.2.3 认证记录的保存与保管：

保存期限：所有认证记录的保存期限自认证周期结束之日起计算，不得少于 5 年。

对于有长期保存价值的记录（如认证合同），可适当延长保存期。

保管要求：

——纸质记录：应存放于安全、干燥、防蛀、防火的专用档案室，由质保部统一管理。

——电子记录：应在 OCD 总部办公室的境内服务器上，并定期备份，并采取防丢失、防损坏的技术措施。

质保部应建立便捷的检索系统，确保记录易于查找和存取。

4.2.4 认证记录的使用与处置：

内部人员借阅或调用记录需办理审批登记手续。外部机构（如监管机构）调阅记录，需出示正式函件，经管理者代表批准后方可提供。

超过保存期限的记录，由质保部或是记录使用部门提出销毁申请，经相关部门鉴定并报数据管理者代表批准后，采用粉碎、消磁等不可恢复的方式统一销毁。销毁过程应留有记录。