大田县农村信用合作联社文件

田信联〔2019〕312号

关于印发《大田县农村信用合作联社客户信息保护管理办法》的通知

各分支机构、机关各部门:

为加强客户信息保护管理，降低客户信息被违法使用和传播的风险，经县联社同意，现将《大田县农村信用合作联社客户信息保护管理办法》印发给你们，请遵照执行，执行中遇到的问题及意见建议请及时反馈。

大田县农村信用合作联社

2019年10月25日

大田县农村信用合作联社客户信息保护管理办法

第一章 总 则

第一条 为加强大田县农村信用合作联社（以下简称联社）客户信息保护管理，降低客户信息被违法使用和传播的风险，根据《中华人民共和国商业银行法》《中华人民共和国消费者权益保护法》等法律法规，特制定本办法。

第二条 客户信息保护管理涵盖客户信息的产生、传输、存储、处理、销毁等各个环节。客户信息的载体包括“IT 系统数据”的电子信息和纸质的“实体介质档案”两种形式。

第三条 保护客户信息安全及其合法权益是联社应承担的企业社会责任，全体员工应严格遵守相关要求，保护客户信息安全，严禁泄露、交易和滥用客户信息。

第四条 客户信息安全管理应遵循“谁主管谁负责，谁使用谁负责”的原则。

第五条 各职能部门、各网点应当依照有关法律、法规、规章和金融监管部门政策规定，遵循以下原则，依法采集、传输、处理、使用、存储、查询、销毁客户信息。

（一）目的明确原则：客户信息的收集、处理或利用都必须依据明确的目的进行，不得收集与业务无关的信息。

（二）知情同意原则：客户信息的收集应该在客户知悉或同意的情况下进行，收集客户信息的手段必须合法。

（三）使用限制原则：对客户信息的使用不得超出收集目的范围。

（四）公开告知原则：必须以明确、易懂和适宜的方式如实向客户告知处理客户信息的目的、客户信息的收集和使用范围、客户信息保护措施等信息。

（五）信息保密原则：对收集到的客户信息，负有保密责任，应采取有效措施保障客户信息不被任何与处理目的无关的个人、组织和机构获知。

（六）数据质量原则：客户信息必须在利用目的范围内保持正确、完整及最新状况。

（七）分级保护原则：必须按照客户电子信息的敏感程度，采取与之对应级别的保护措施。

（八）安全保障原则：应采取必要、合理的管理和技术措施，防止未经授权的客户信息检索、使用、公开、修改，防范客户信息丢失、泄露、损毁等事件。

（九）责任落实原则：客户电子信息采集、传输、处理、使用、存储、查询、销毁等各个环节应明确管理责任，严格落实管理措施。

第二章 客户信息的内容

第六条 客户认证信息，包括密码、密钥、动态认证信息。

第七条 客户身份信息，包括客户名称、客户证件类别、客户证件号码及有效期限、客户联系方式、客户地址及照片。

第八条 客户财产信息，包括客户经营或收入状况、拥有的不动产状况、拥有的车辆状况、纳税额等。

第九条 客户账户信息，包括账号、账户开立时间、开户行、账户余额、账户交易情况等。

第十条 客户信用信息，包括授信或信用卡额度情况、贷款情况以及客户在经济活动中形成的，能够反映其信用状况的其他信息。

第十一条 客户金融交易信息，包括银行业金融机构在支付结算、理财、保险箱等中间业务过程中获取和保存的客户电子信息，以及客户通过银行业金融机构与保险公司、证券公司、基金公司、期货公司等第三方机构发生业务关系时产生的客户信息等。

第十二条 开展业务过程中获取、保存、形成的其他客户信息。

第十三条 客户信息按其敏感性分级，可以分为客户敏感信息和客户一般信息。敏感信息主要是指涉及个人隐私或商业秘密等银行客户不愿意对外披露，一旦披露可能会影响客户账务、资金安全的信息。客户敏感信息一般包括客户认证信息、客户身份信息、以及可以直接或间接识别出特定客户的其他类型的客户信息。客户一般信息是指除客户敏感信息之外的其他客户信息。

第三章 组织与职责

第十四条 联社将客户信息安全保护纳入全面风险管理体系，建立完善的客户信息安全保护管理机制，确保客户信息安全。

第十五条 全体员工有权利和义务制止对于任何可能危害客户信息安全的行为，并向上级领导或信息安全管理人员及时反映情况。

第十六条 各职能部门、各网点应负责各自主管的业务系统的客户信息安全保护，明确各业务系统的客户信息安全责任人，按照本规定落实业务系统的安全管理要求。

第十七条 涉及客户信息的职能管理部门职责:

（一） 负责规范本部门访问客户信息的业务人员岗位角色及其职责;

（二）负责主管的业务系统的客户敏感信息安全保护，建立落实管理制度和实施细则;

（三）负责业务层面客户信息安全的日常管理;

（四）负责受理客户信息泄密事件的投诉、上报;

（五） 制订对业务合作伙伴的信息泄露的惩罚措施;

（六） 协助完成客户信息泄密现象的市场调查;

（七）协助进行客户信息泄密事件的查处。

第十八条 信息科技部职责:

（一）负责所运维的涉及客户信息的系统和平台技术层面的客户信息安全保障和稽查工作;

（二）负责所主管系统的客户敏感信息安全保护，建立落实管理制度和实施细则；

（三）负责规范后台运行维护人员、开发测试人员、生产运行支撑人员的角色和职责；

（四）做好对第三方的管理，包括组织签订保密协议，加强操作管理等；

（五）负责规范所属系统和平台客户信息安全技术标准和访问流程；

（六）协助主管部门查处客户信息泄密事件。

第十九条 主管部门风险合规部的职责：

（一）制定客户信息安全保护管理制度；

（二）牵头组织客户信息安全管理专项检查；

（三）负责收集、汇总客户信息泄密事件；

（四）其他需要负责的事项。

第二十条 其他相关部门的职责：

（一）办公室：负责客户信息安全宣传、培训等工作，负责客户信息安全事件的对外解释口径；

（二）人力资源部：组织有关员工签订保密承诺书，及时发布人员岗位变动、离职的信息给帐号管理部门，参与对客户信息泄密人员的查处；

（三）监察审计部：负责相关管理规定的监察、违规行为的调查审核、违规人员的处罚；负责客户信息泄密事件的查处；负责开展客户信息风险的审计。

第四章　业务管理

第二十一条　联社各职能部门、各网点应全面梳理各业务流程中涉及客户信息的业务环节，明确各业务环节对客户信息的保护要求和管理责任，严格落实各项管理措施，防止未经授权的客户信息检索、使用、公开、修改，防范客户信息丢失、泄露、损毁等事件。

第二十二条　各职能部门、各网点在收集客户相关信息时，应当有效限定客户信息收集的目的和方式，确保目的明确、合法、有特定意义，确保收集方式安全、可靠。

第二十三条　各相关业务部门、各网点在收集客户相关信息时，应明确各类业务的收集范围，在业务活动中只收集与业务经营目的相关的最少信息，不超越目的范围，不收集与业务无关的信息，并明确信息的保存期限。

第二十四条　各职能部门、各网点收集客户信息前应征得客户的同意，包括默许同意或明示同意。收集客户一般信息时，可认为客户默许同意，如果客户明确反对，应停止收集或删除客户信息；收集客户敏感信息时，必须得到客户的明示同意。

第二十五条 各职能部门、各网点在收集客户相关信息时，应对客户尽到告知、说明和警示的义务，以明确、易懂和适宜的方式如实告知客户收集信息的目的、方式、使用范围、使用期限、信息保护措施、存在的风险以及投诉渠道等信息。

第二十六条 各职能部门、各网点应在客户信息采集目的范围内保持其信息准确、完整，并能反映客户在信息录入时的当前状况。

第二十七条 各职能部门、各网点应强化客户信息查询流程控制和记录控制，根据人员岗位职责，遵循最小授权原则，严格控制信息系统客户电子信息查询权限，确保查询记录可追溯。

第二十八条 针对自己建立的应用系统，应建立客户信息更新控制流程，用户更新信息系统中客户电子信息必须严格身份认证和权限控制，更新操作有可靠记录以备跟踪审计。

第二十九条 各职能部门，各网点在客户信息管理过程中应根据信息重要性和敏感性对信息进行识别和分级管理，针对敏感信息，应实行更高的权限控制，采取更严格的保护措施保障客户电子信息安全。

第三十条 客户拥有客户信息的主体权益，有权对大田联社相关部门、网点提出对其客户信息的补充、修改、删除要求。相关部门、网点应根据客户要求进行查验核对，在保证客户信息完整的前提下，补充或修改相关信息。客户有正当理由要求删除其客户信息时，大田联社相关业务条线部门、各网点应及时删除客

户信息，有可能会影响执法机构调查取证时，相关部门、网点应采取适当的存储和屏蔽措施。

第三十一条 各部门、网点在不损害客户合法权益的前提下，可以在产品营销、客户关系管理、产品研发、内部检查过程中合理使用客户信息。

（一）相关部门和网点应以提升客户服务水平、客户资产收益水平和客户满意度为目标进行客户电子信息挖掘和分析，不得损害客户利益和相关权益，不得将挖掘和分析结果用于非法用途；

（二）相关部门和网点利用客户电子信息进行金融产品营销时，应获得客户同意；在客户明确拒绝的情况下，应立即停止利用客户电子信息进行营销。

第三十二条 相关部门和网点不得将客户授权或同意将其客户信息用于营销、对外提供等作为与客户建立业务关系的先决条件。

第三十三条 相关部门和网点不得违背收集阶段的转移目的或超出告知的转移范围转移客户信息。在未经客户同意的情况下，不得将客户信息转移至大田联社系统外。

第三十四条 各部门、网点不得向境外转移在中国境内收集的客户电子信息，法律法规、行政管理、监管部门等另有规定的除外。大田联社相关业务条线部门、各网点应确保客户电子信息境外转移活动满足我国及转出、转入国（地区）法律法规要求。

第三十五条 各部门、网点在向司法部门、行政管理部门及其他有权机关提供客户电子信息时，应按照法律法规相关规定，履行相应的审批程序，规范协助查询及资料提供手续，审核对方真实身份和有关法律文书，切实保护客户电子信息。

第三十六条 建立有关客户信息的投诉受理渠道，客户信息收集阶段明确告知客户相关投诉渠道，明确投诉事件的处理流程，建立投诉事件跟踪处理机制，妥善处置有关客户信息的投诉事件。

第三十七条 相关部门应建立明确的客户电子信息失效、安全销毁策略，确保客户信息达到使用目的或超过留存期限后及时进行处理。

第五章 技术管理

第三十八条 电脑信息部应明确客户电子信息录入、传输、存储、处理、销毁等信息生命周期的安全保护技术要求。明确涉及客户电子信息系统的开发、测试和运维等系统生命周期的管理责任，严格落实各项管理措施。

第三十九条 电脑信息部应加强客户电子信息数据规划，强化源数据管理，逐步建立统一客户电子信息视图。

第四十条 各部门、网点应采用安全的传输方式和途径传输客户电子信息，应采取身份认证、访问控制、加密、监控和审计

等安全措施，防止信息泄露和篡改。严禁通过互联网、传真机、邮件系统等方式明文传输客户信息。

第四十一条 电脑信息部应制定客户信息安全存储规范，采取有效保护措施，确保客户信息在信息系统中存储安全。客户账户密码必须加密存储并严禁脱离生产环境。不得在办公终端、移动终端明文存储客户敏感电子信息，严禁在非可控区域存储客户敏感信息。

第四十二条 相关部门应根据省联社要求，建立严格的客户电子信息后台查询和修改控制流程，严控客户电子信息后台查询和修改权限，建立分级授权机制，确保查询和修改的记录可追溯。通过后台修改的客户电子信息必须进行审核校验。

第四十三条 电脑信息部应建立针对客户电子信息的安全设计与安全编码规范，禁止在交易节点存放磁道信息、密码等客户敏感信息，禁止用户界面的错误提示中泄露客户敏感信息，严禁在日志文件中记录客户敏感信息。

第四十四条 电脑信息部不得直接把客户信息用于开发和测试等活动，应建立客户电子信息的脱敏处理策略、流程与规则，并确保脱敏处理后的客户电子信息不可恢复。

第四十五条 对于脱离生命周期的客户电子数据，电脑信息部门应采取软件工具、消磁或物理销毁的方式及时进行销毁，确保其不可恢复。

第六章　第三方合作管理

第四十六条　各部门、网点应加强与第三方合作业务中的客户信息管理，做好事前尽职调查、合同或协议管理及事后风险监控工作。未经客户授权，不得以任何形式将客户敏感信息提供给第三方机构。

第四十七条　各部门、网点与第三方签订协议时应明确要求第三方承诺保障大田联社客户信息安全，非经客户和大田联社的授权同意，不得将获得的客户信息提供给其他第三方，法律法规另有规定的除外。

第四十八条　相关部门应对合作第三方的客户信息保护情况进行评估和检查。并把评估和检查报告上报联社。

第七章　外包管理

第四十九条　审慎控制涉及客户信息的外包活动范围。在开展外包活动前，必须对外包服务商客户信息安全保障情况进行全面的风险评估和尽职调查。

第五十条　外包合同或协议中要明确服务提供商在保护客户信息安全方面的责任，以及针对客户信息安全要求需采取的具体措施。并在外包合同或协议中约定服务提供商对客户信息安全和客户权利的保护条款、事故处理方式及违约赔偿条款。

第五十一条　加强外包服务人员管理。建立外包服务人员服务档案，签署书面保密协议。对外包服务人员服务过程中的客户

信息保护职责进行宣传、培训、监督和审查，严格限制外包服务人员权限，及时注销离场的外包服务人员用户。

第五十二条 外包人员参与的信息系统开发、测试等活动不得使用客户敏感电子信息。涉及客户电子信息的信息系统运维外包服务，联社必须掌握系统最高管理权限。

第五十三条 应对外包活动开展期间外包服务商的客户信息保护情况进行定期评估和检查。

第五十四条 终止与外包服务商合作时，应及时收回或销毁外包服务商因外包活动而获得的客户信息，销毁的信息在技术上应不可恢复。

第八章 风险管理

第五十五条 风险合规部应开展客户信息风险评估工作，评估范围应包括各业务流程涉及客户信息业务环节保护措施的有效性和相关岗位尽职情况。

第五十六条 各相关部门应分层次开展定期检查，通过建立检查计划、规范检查流程、明确检查标准和整改监督机制，对网点客户信息保护工作进行系统性检查，全面掌控客户信息保护的内控管理情况。

第五十七条 监察审计部应当定期开展客户信息管理审计工作。发生客户信息风险事件后应当及时开展专项审计。

第五十八条 电脑信息部应将批量处理客户电子信息、大量下载客户信息等操作列入重点复核检查的范围，确保客户电子信息的高危风险点在日常操作流程中得到有效管控。

第五十九条 各部门、网点针对可能影响客户资金安全的客户信息泄露事件，应及时通知客户，并采取有效技术措施，加强客户身份认证，确保客户资金安全。

第六十条 各部门、网点发生客户信息风险事件或发现第三方合作机构违反客户信息保护要求的行为，应在事件发生当日或合作机构违规行为之日起 7 个工作日内将相关情况及初步处理意见报告联社。

第九章 安全检查

第六十一条 各网点负责开展日常的安全检查，各业务条线部门负责专项安全检查、抽查。

第六十二条 各职能部门负责客户信息安全检查情况汇总，梳理存在问题，通报结果；针对发现重大安全隐患或违规行为，应向分管领导汇报。

第六十三条 各职能部门针对安全检查过程中发现的突出问题，牵头协调各部门提出改进方案，并要求相关部门落实解决，并对改进措施落实情况进行跟踪检查。

第六十四条 用于客户信息安全检查、稽核的原始日志必须单独保存，电脑信息部要制定数据存储备份管理制度，定期对原

始日志进行备份归档，所有客户敏感信息操作原始日志在线至少保留 1 年，离线至少保留 3 年。

第六十五条 联社有权根据国家的法律、法规和规章制度，对于发现的任何侵害客户信息安全的个人采取相应的处罚措施。

第十章 信息泄密处罚

第六十六条 发生客户信息泄密事件，由信息安全主管部门组织有关部门联合进行责任认定，按照省联社、大田联社具体处罚办法对相关直接责任人和负有领导责任的人进行处罚。

第六十七条 内部员工发生泄密事件，应根据信息安全事件造成的影响及相关责任主体的态度，作出如下处理:

1. 批评教育：包括责令责任主体检查、诫勉谈话等;

2. 书面检查：责令责任主体向联社作出书面检查;

3. 通报批评：在大田联社辖内对责任主体发文通报;

4. 绩效处分：降低或扣除责任主体绩效，纳入月度或年度考核;

5. 行政处分：追究信息安全事件发生负有领导责任的负责人的管理责任， 对相关责任人予以行政处分， 直至开除。

6. 法律责任：如涉嫌犯罪的，则移交司法机关处理。

第六十八条 对与联社有合作关系的单位或个人，若发生泄密事件，应根据合同和相关要求进行处罚，涉嫌犯罪的，依法移交司法机关处理。

第十一章　附　则

第六十九条　本办法是联社进行客户信息安全管理工作的基本依据。各部门和各网点和应做好客户信息安全管理工作。

第七十条　本办法适用于客户信息的使用人员、运维人员、开发测试人员、管理人员和安全审计人员等。

第七十一条　本办法由大田县农村信用合作联社负责解释和修订。

第七十二条　本办法自公布之日起执行。

抄　　送：省联社三明办事处，县人行、县监管组。

内部发送：县联社领导。

联系人：林廷瑜　　联系电话：0598-7225920

大田县农村信用合作联社办公室　　2019 年 10 月 25 日印发