**xxx银行**

信息科技外包管理办法

第一章 总 则

第一条 为规范xxx银行（以下简称“本行”）信息科技外包活动，加强信息科技风险管理，依据银监会颁布的《商业银行信息科技风险管理指引》、《银行业金融机构信息科技外包风险监管指引》及省联社相关制度，特制定本办法。

第二条 信息科技外包是指农商行将原本由自身负责处理的信息科技活动委托给服务提供商进行处理的行为，包含项目外包、人力资源外包等形式。

本办法适用于以下信息科技外包：

1.基础设施类外包，指外包服务商提供机房、线路及配套等基础设施服务；

2.系统服务类外包，指外包服务商提供信息系统日常运行和维护等服务工作；

3.软件开发类外包，指外包服务商提供专业技术人员协助本行完成指定功能应用或管理系统的开发工作；

4.电子设备服务类外包，指外包服务商提供 ATM 等自助设备的布放和运维、监控设备和终端设备运维等服务工作；

5.其他信息科技外包。

第三条 外包应以满足需求、保证质量、提高效率、风险可控、成本可控为基本原则。

第四条 本行信息科技的战略管理、核心管理以及内部审计等职能不宜外包。

第二章 组织架构及职责

第五条 本行外包管理的组织架构包括信息科技管理委员会及下设信息科技外包管理责任小组，其中信息科技外包管理责任小组组成成员主要包括信息科技部、风险管理部、合规管理部、审计部、办公室等部门。

第六条 信息科技管理委员会以及下设信息科技外包管理责任小组的职责按《关于成立xxx银行信息科技外包管理责任小组的通知》（xxx银行行办[2016]128 号）执行。

第七条 信息科技部的职责主要包括以下方面：

1.信息科技部门建立外包执行团队，执行团队包括内控管理岗、信息科技外包项目经理、信息安全管理岗。

2.根据本行发展规划或外包服务需求，结合本行的建设情况，确立外包项目的范围和内容，制定外包年度计划及外包阶段性计划；

3.配合完成外包活动的合同签署以及外包服务技术指标的制定等工作；

4.负责外包服务商在本部门工作的日常管理，包括现场管理、合同履约、合同验收及风险防控，定期提交外包管理工作报告；

5.负责对外包服务商履约情况及遵守现场工作秩序情况进行监督检查，对发现的问题提出风险警示；

6.根据本行要求提出外包管理的优化和改进方案；

7.在发现外包服务商的业务活动存在缺陷时，采取及时有效的措施；

8.信息科技管理委员会确定的其他职责。

第八条 风险管理部的职责主要包括以下方面：

1.负责外包风险状况的监督及风险管理；

2.向信息科技管理委员会提出有关外包活动发展和风险管控的意见和建议；

3.根据信息科技部提交的外包项目情况报告，及时发现信息科技外包风险，并进行风险提示；

4.定期向信息科技管理委员会提交外包风险评估报告；

5.信息科技管理委员会确定的其他职责。

第九条 合规管理部的职责主要包括以下方面：

1.负责外包合同签署前的审查与核对；

2.信息科技管理委员会确定的其他职责。

第十条 审计部的职责主要包括以下方面：

1.负责对外包服务商的资质进行尽职调查，定期安排内部审计，确保审计范围涵盖所有外包安排；

2.信息科技管理委员会确定的其他职责。

第十一条 办公室的职责主要包括以下方面：

负责做好外包人员的食宿安排及行为管理；信息科技管理委员会确定的其他职责。

第三章 外包服务商资质评审

第十二条 外包服务商的资质评审由本行信息科技管理委员会负责统一组织，原则上每年评审一次，特殊情况可根据实际需要安排评审。

第十三条 提供外包服务的外包服务商必须符合资质要求，不符合资质要求的外包服务商不准参与外包服务。

第十四条 开展外包服务商资质评审前必须对外包服务商进行尽职调查，并形成尽职调查报告。对外包服务商的尽职调查主要包括以下内容：

1.管理能力和行业地位；

2.财务稳健性；

3.经营声誉和企业文化；

4.技术实力和服务质量；

5.突发事件应对能力；

6.对银行业的熟悉程度；

7.对其他银行业金融机构提供服务的情况；

8.本行认为重要的其他事项。

如果外包活动涉及多个外包服务商时，应当对这些外包服务商进行关联关系的调查。

第十五条 外包服务商资质评审活动由信息科技部牵头实施，风险管理部、合规管理部、审计部配合落实。

第四章 外包合同

第十六条 本行信息科技外包项目立项前，必须实施风险评估，明确双方的权利义务。评估结果为风险可控后方可签订合同或协议，应当包括但不限于以下内容：

1.外包服务的范围和标准；

2.外包服务的保密性和安全性的安排；

3.外包服务的业务连续性的安排以及外包服务商提供专属资源的承诺；

4.外包服务的监督、检查和考核；

5.外包争端的解决机制；

6.合同或协议变更或终止的过渡安排；

7.担保和损失赔偿以及违约责任。

第十七条 签订外包合同时外包服务商须承诺以下事项：

1.定期通报外包活动的有关事项；

2.及时通报外包活动的突发性事件；

3.配合本行接受银行业监督管理机构的检查；

4.保障客户信息的安全性，当客户信息不安全或客户权利受到影响时，本行有权随时终止外包合同；

5.遵守本行有关信息科技风险管理制度和流程；

6.第三方供应商出现问题时，保证软硬件持续可用的相关措施；

7.不得以本行的名义开展活动；

8.本行认为应当承诺的其他事项。

第十八条 本行外包合同由信息科技部上报合规管理部法务审查岗审核，合规管理部总经理核对，分管行长审查，行长批准，办公室用印。

第五章 风险管理

第十九条 信息科技外包管理责任小组要切实加强信息科技相关外包管理工作，确保本行客户资料等敏感信息的安全，应采取包括但不限于以下风险管控措施：

1.本行应按“必需知道”和“最小授权”原则对外包服务商相关人员的系统登陆权限、操作权限、文件读写权限等进行严格控制，授权管理工作要求及流程要制定成文，授权的书面审批或电子审批过程应当保持原始记载，并由专人负责收集、归档、管理；

2.应当采取技术手段实现研发数据（含客户资料，下同）与外包服务商自带数据的有效隔离，外包人员未经批准不得将 U 盘、移动硬盘等带有存储功能的介质接入开发测试环境，严禁外包服务商下载、复制或截取本行的相关数据资料；

3.本行在批准外包服务商使用本行客户资料等数据时，应当先对数据进行技术处理和过滤，严禁将“裸数据”交由外包服务商进行开发测试；

4.外包服务商应保证其相关人员遵守本行信息科技风险的相关管理制度和保密规定；

5.将涉及本行客户资料的外包作为重要外包；

6.严格禁止外包服务商对外转包，采取足够措施确保相关信息的安全；

7.信息科技外包项目文档全面详实，并由外包执行团队负责审查后归档；

8.信息科技外包项目文档由专人规范管理，调阅有审批记录；

9.信息科技部应对外包开发商提供的软件源代码进行安全检查。

第二十条 关注外包服务商分包风险，若外包活动存在分包情况的，须在合同中明确以下事项：

1.外包服务商分包的规则；

2.分包服务提供商应当严格遵守主服务提供商与本行确定的外包合同或协议中的相关条款；

3.主服务提供商应当确认在业务分包后继续保证对服务水平和系统控制负总责；

4.不得将外包活动的主要业务分包；

5.不得将外包活动转包或变相转包。

第二十一条 信息科技部负责制定和建立外包突发事件应急预案和机制，以应对外包服务商在服务中可能出现的重大缺失。尤其是需要考虑外包服务商的重大资源损失、重大财物损失和重要人员的变动，以及外包合同或协议的意外终止等情况。通过采取替代方案、寻求合同项下的保险安排等措施，确保业务活动的正常经营。

第二十二条 风险管理部负责对外包活动进行全面风险评估，审计部负责对外包活动进行审计。

第二十三条 本行在开展外包活动时如遇到对本行业务经营、客户信息安全、声誉等产生重大影响事件，应及时向监管部门报告。本行在实施重要外包(如数据中心和信息科技基础设施等）应格外谨慎，在准备实施重要外包时应以书面材料正式报告省联社及监管部门。

第六章 外包人员管理

第二十四条 外包服务商需要明确一名项目经理（或项目负责人）负责协调项目相关重要事项。

第二十五条 本行对于外包人员的管理方式以管理外包服务商项目经理为主，也可以根据实际需要直接管理和调配外包人员。

第二十六条 外包人员在本行服务期间，应严格遵守本行作息考勤制度以及其他工作规范。

第二十七条 信息科技部负责对外包人员使用环境和权限配置管理，对使用环境中的系统权限、文件读写权限必须严格控制，以满足工作需要为前提，遵循权限最小化原则，不得授予与工作无关的权限。

第二十八条 对于向外包人员提供本行内部资料必须严格审核，严禁未经授权提供。

第二十九条 外包单位人员应经信息科技部向办公室申请登记后，在正常工作时间访问办公区域及办公电脑。

第三十条 外包单位人员访问受控区域或设备须提出书面申请，批准后由信息科技部专人全程陪同，并登记备案，受控区域为本行机房及其它重要区域。

第三十一条 除已发生事故外，外包人员严禁在生产时间进行可能影响对外服务的变更维护操作。

第七章 外包服务的交付

第三十二条 外包人员应按外包合同要求交付服务工作成果。

第三十三条 开发类外包人员的交付物必须经过在测试环境下的严格测试，验收合格后才可以投产试用。

第三十四条 对于外包交付物验收不合格的，应要求外包服务商重新提供产品，并重新组织验收，直到验收通过，并纳入外包服务商考核评价指标。

第三十五条 由于外包服务商原因导致未按计划完成或完成项目质量不高，并造成一定影响的，作为不良合作记录登记，对未完成服务由外包服务商继续完成，并不再追加任何费用。

第八章 外包交付物管理

第三十六条 对于外包人员提交的源代码，须经信息科技部人员审核编译。所产生的执行程序，须经本行相关人员测试通过后，按规定流程投入生产系统。

第三十七条 对于外包开发人员提交的关键代码（涉及业务系统核心处理流程、记账或有关安全加密、认证的代码等），信息科技部须对源代码进行重点抽查，并记录抽查结果，存档保留。

第三十八条 对于外包测试人员提交的测试方案和测试案例，信息科技部须组织人员进行复核确认；外包测试人员编写的测试脚本和测试用程序必须满足项目测试性能要求。

第三十九条 外包咨询人员应及时对本行的咨询要求做出响应，按时协助解决问题，或提供符合要求的咨询建议或报告。

第四十条 外包维护人员必须及时响应业务需求，并按本行要求提供服务。

第九章 外包评价与审计

第四十一条 信息科技部负责组织制定对外包服务商考核评价的量化指标，根据量化的考核指标，每半年进行一次对外包服务提供商进行安全检查和服务评价，获取服务提供商自评估或行方评估报告，由信息科技部及审计部评审外包方提供的服务报告，对外包方履职情况进行审计。

第四十二条 考核评价结果将作为外包服务商资质评审的重要依据。外包服务商如存在考核不合格的情况，未来三年内不得参与本行外包服务。

第四十三条 审计部负责定期对信息科技外包活动进行审计。

第四十四条 在外包服务过程中，依据服务水平设定的目标，对外包服务提供商的服务水平进行持续监控，监控中发现问题，外包服务提供商能及时进行整改，若不能及时整改则扣减相应考核指标分数。

第十章 外包商准入

第四十五条 外包商的准入条件：

1.外包方公司管理完善，财务、科技实力雄厚，诚信良好，有稳定的售后服务；

2.网络、服务器等硬件系统外包方须持有相关设备的金牌代理或相应级别资质；

3.外包方及相关项目经理须实施过银行系统内同等规模不少于3 个成功项目，杜绝借壳投标情况，通过合同明确特定的项目经理在项目施工时的驻场时间；

4.外包方需具备较强的发展能力，在行业内有一定的市场份额；

5.外包方需具备较强的故障、意外事件和突发事件的担当能力，对因外包没有履行职责造成的损失具有经济承担能力；

6.外包方所开发的软件应符合相关法律、法规和软件开发规范，未侵犯他人的著作权，应提供相关专属资源的承诺；

7.外包方提供的软件中涉密部分必须有国家要求的相关资质。

第四十六条 外包商需提交相关的资质资料，所有资料需加盖单位公章并保证真实有效。资质资料包括以下几项：

1.营业执照副本；

2.企业法人代表或委托授权人有效证件；

3.外包商的专业资质、技术实力及其从业人员的履历和专业技能资料；

4.其他能证明外包商实力的资信文件。

以上资料审核通过后，由本行信息科技外包管理责任小组进行综合评定，选择经营状况、财务实力、诚信历史、安全资质、技术服务能力和责任承担能力比较强的外包商，进入合格外包商名单

第十一章 外包商退出

第四十七条 根据外包商的外包服务水平、竞争力及供需双方的依赖程度,将外包商分为:A 级外包商、B 级外包商、C 级外包商。

1.A 级外包商：能够长期稳定的提供安全的信息技术服务，对需求方的工作具有全局性或局部战略需求的影响，生产资源优势明显。

2.B 级外包商：在信息技术服务方面能够达到基本满足。

3.C 级外包商：能够满足合同约定的当前运作要求，在信息技术服务方面偶尔会出现小的波动或不稳定的情况。

第四十八条 根据外包商 ABC 三级管理。凡出现以下情况考虑退出：

1．连续两年被评定为 C 级外包商的，信息科技外包管理责任小组应积极寻找更好的外包商逐一替代。对确因资源紧张不得不使用的Ｃ级外包商，要通过制定纠正预防措施，改进信息技术服务质量；

2．信息技术服务中出现问题,整改措施屡次得不到实施,且信息技术服务质量得不到提高,不能满足本行技术和安全要求的；

3．凡发生欺诈、违约、失信等不法行为，造成影响恶劣，且行为得不到纠正的。

第十二章 附 则

第四十九条 本办法由xxx银行信息科技部负责解释和修订。

第五十条 本办法自发文之日起施行。