**xxx银行**

信息科技风险管理办法（试行）

第一章 总 则

第一条 为加强xxx银行（以下简称“本行”）信息科技风险管理，实现风险识别、计量、监测和控制，依据《银行业金融机构全面风险管理指引》、《商业银行信息科技风险管理指引》（银监发〔2009〕19号）、《江苏省农村商业银行信息科技风险管理制度（试行）》及相关规定，制定本办法。

第二条 本办法所称的信息科技风险是指本行在信息科技运用过程中，由于自然因素、人为因素、技术漏洞和管理缺陷等原因，产生的操作、法律和声誉等风险。信息科技风险包括但不限于：

（一）决策风险。具体体现为IT战略不能保持与业务战略的一致性，选择了不适合的信息科技路线。

（二）安全风险。具体体现为信息安全事件造成信息资源或系统等机密性、完整性、可用性受损。

（三）外包风险。具体体现为外包方选择失误，对外包方服务水平控制不力，缺乏有效监督及外包应急机制等。

（四）业务连续性风险。具体体现为环境灾难事件、自然灾难事件、人为事件等导致系统故障或资产受损，造成服务中断或业务无法持续。

（五）质量风险。具体体现为项目建设管理不规范，人为疏忽、不尽责导致信息系统设计、实现、部署、测试过程存在缺陷。

（六）运行风险。具体体现为运行监控不到位、不规范，事件应急处置机制不成熟，运行事件造成服务、数据可用性受损。

（七）合规风险。具体体现为不符合国家和行业的信息科技管理要求。

第三条 本办法适用于总行及各营业网点的信息科技风险管理。

第二章 组织及职责

第四条 董事会是信息科技风险管理最高决策机构，法定代表人是信息科技风险管理的第一责任人。

第五条 风险管理部门牵头开展信息科技风险管理工作。组织制定信息科技风险管理工作报告，经业务连续性管理委员会、高级管理层审议后，提交董事会决策。

第六条 内部审计部门进行独立有效的信息科技风险管理审计，对审计报告进行确认并落实整改。

第三章 制度制订及维护

第七条 风险管理部门牵头组织制订本单位信息科技风险管理制度体系，包括策略、制度、流程及表单。该体系应通过业务连续性管理委员会审议，经高级管理层集体研究后报送董事会决策批准。

第八条 信息科技风险管理制度体系包括但不限于以下内容：

（一）科技治理。

（二）风险管理。

（三）安全管理。

（四）项目管理。

（五）运行管理。

（六）业务连续性管理。

（七）外包管理。

（八）审计。

第九条 本行每年对信息科技风险管理制度体系进行修订维护。

第四章 科技风险评估及处置

第十条 评估工作

（一）本行风险管理部门组织建立针对外部风险提示、重大项目的立项和投产环节的风险评估方法，并牵头实施。

（二）建立重大项目在设计和运维环节的风险评估方法，并牵头实施。

（三）建立信息科技风险管理体系的风险评估方法，并每年执行评估工作。

第十一条 处置工作

（一）风险管理部门基于风险评估及信息科技审计结果，牵头组织制订风险处置管理要求，实施处置工作。

（二）每年对信息科技风险管理体系评估所发现问题进行风险处置。

第五章 科技风险监测

第十二条 风险管理部门组织建立本行信息科技风险管理专项检查机制，并牵头实施检查工作。

第十三条 风险管理部门组织建立信息科技风险监测数据的采集和报送机制，以及信息科技风险监测指标体系和分析方法。

第十四条 定期实施信息科技风险数据的采集和分析。条件允许情况下可运用信息系统定期实施。监测范围至少包括：

（一）信息科技项目（含科技外包）实施情况。

（二）信息系统日常运行指标及状况。

（三）运行环境下的操作风险。

（四）信息安全事件。

（五）信息科技服务投诉和事件形成的风险点。

（六）内部审计、外部审计和监管发现问题及风险处置情况。

（七）外包服务商服务水平协议完成情况。

（八）新技术发展可能造成的影响和已使用软件面临的新威胁。

第六章 报告及培训

第十五条 风险管理部门牵头组织制订编写信息科技风险管理年度报告，提交业务连续性管理委员会和高级管理层审议后并入风险管理年度报告，提交董事会决策。根据管理要求，将年度报告报送行业管理机构。

第十六条 风险管理部门制订信息科技风险意识培训年度计划，每年组织实施面向不同层面的信息科技风险意识培训。

第七章 附 则

第十七条 本办法由xxx银行信息科技部负责解释和修订。

第十八条 本办法自发文之日起施行。