**xxx银行**

计算机系统运行管理办法

第一章　总　则

第一条　为规范xxx银行（以下简称“本行”）计算机系统的运行管理，规范操作，依据《中华人民共和国计算机信息系统安全保护条例》、省联社《信息科技运行管理制度》等规定，制定本办法。

第二条概念释义

（一）本办法中计算机系统运行管理包括：中心机房、设备运行、主机系统、网络系统、操作权限与口令管理等。

（二）中心机房是指容纳并集中运行计算机业务处理、管理信息或网络通信系统等的专用物理场所

（三）设备运行管理是指对运行中的主机设备、网络通信设备及外围设备的管理。

（四）主机系统运行管理是指对机房运行的主机、操作系统、数据库和中间件等操作、维护过程的管理。

（五）网络系统管理是指对所辖网络通信系统运行的管理。

（六）操作权限与口令管理是指对主机系统、网络通信运行实行操作权限与口令的管理。

第二章　职责与权限

第三条　信息科技部负责人职责：

（一）负责主机系统参数修改的批准。

（二）负责内部网络规划与开通的审核、审批。

（三）负责内部网络变更应用的审批等。

第四条信息科技部职责：

（一）负责实施与监督计算机机房运行环境。

（二）负责内部网络的规划、实施、安全管理及维护工作。

（三）负责对业务网络接入方案做出安全性评估及审定等。

第三章　内容与要求

第五条　计算机系统运行应遵循“严密制度、控制风险、规范操作、严格管理”的原则。

第六条机房运行管理

（一）机房建设应符合省联社机房建设相关规范。

（二）机房为重要设备运行管理场所，除机房工作人员外，其他人员未经批准不得进入。确因工作需要必须进入的，需填写“机房出入登记簿”，经批准后由机房工作人员陪同进出。

（三）机房管理实行责任制。信息科技部应根据规范要求实施管理、操作、监控和维护保养。机房工作人员应具备相应的机房管理知识。

（四）机房工作人员应每天定时巡检设备运行情况，及时维护保养，发现问题立即报告并处理，必要时可实行全时监控。

（五）机房设备的操作规程、制度应当明示上墙，安全防护措施齐备，各项操作必须在确保安全的前提下依照规程进行，严禁违规操作。

（六）机房的温度、湿度、粉尘度等各项指标必须严格控制在规定范围之内。

（七）机房应保持卫生清洁，严禁吸烟、会客、聚餐和娱乐等与机房管理无关的行为。

（八）机房值班人员要认真做好机房出入登记、设备巡检登记、操作记录登记等各项记录，登记资料内容必须完整，并定期整理归档。

第七条　设备运行管理

（一）设备安装时，相关技术人员必须按规定的步骤操作，其中关键设备的安装必须由原厂商（供货商）技术人员现场支持。

（二）设备在投入使用前，应依据供货厂商提供的项目和相关指标，经测试合格后才能使用。

（三）设备升档要经过充分的技术论证和审批，升档过程中应保证现有生产系统的正常运行。

（四）设备管理员应做好核心设备的日常维护工作：

1．做好设备的日常监测、检查、记录，及时掌握设备的运行状况；

2．设备发生故障时应及时维修，必要时，通知供货商或维保单位的技术人员到场解决。

第八条　主机系统运行管理

（一）维护人员须按照规定的步骤执行，并详细记录维护工作情况。

（二）系统维护人员应密切监控系统运行状况，及时处理系统运行中出现的故障，并详细记录系统故障的处理过程。对影响较大且影响业务正常办理的故障，须及时报告信息科技部负责人。对应用系统的故障，及时反馈给项目开发人员，并对故障产生原因进行认真的分析总结。

（三）系统维护人员每日须对系统日志进行检查，具体分析系统可能存在的安全隐患和漏洞，及时研究并提出补救性措施，经批准后实施，确保系统运行的安全。

（四）系统维护人员修改系统参数，须经负责人批准且双人临岗，修改前须进行系统备份或参数备份，详细记录操作过程并整理归档。

（五）严格控制对业务数据库的非应用性操作。特殊原因必须修改业务数据库的，由需要修改的部门提出数据修改申请，报单位分管领导批准后，双人上机操作并做好修改前的数据备份。

（六）系统维护人员必须制定备份计划，对备份的时间、内容、级别、人员、保管期限、异地存取和销毁手续等进行明确规定，需用备份介质对运行系统进行故障恢复时，视同重要事件进行管理控制。

（七）主机系统、应用软件升级或更新、新旧系统切换、应用系统年终结转、应用系统存贷结息等重要操作，系统维护人员应与相关业务部门密切配合，共同制定详细的工作计划和方案。

1．应用系统增加新业务功能的，系统开发人员须提供业务功能说明书、操作手册、用户手册、软件包，系统维护人员在指定FTP服务器存储，并提前2个工作日向应用单位发出书面的安装新业务程序通知，各应用单位须在规定时间内做好新业务程序安装工作。

2．主机系统硬件、操作系统升级，由相关公司提供升级方案，系统维护人员协助相关公司技术人员进行操作维护。

3．数据库、中间件升级的，由相关公司提供升级方案和技术支持，系统维护人员根据升级方案，负责实施。

4．应用软件后台服务程序升级，由应用软件开发人员提供升级方案、模块功能说明书，并通知应用网点。在业务周期结束后，由系统维护人员负责实施。

5．应用软件前台服务程序升级，由应用软件开发人员提供升级方案、模块功能说明书、操作手册、用户手册、升级程序`包等，由系统维护人员在指定FTP服务器存储，并提前2个工作日发出前台服务程序升级通知，各单位在规定时间做好升级工作。

（八）计算机病毒的防范工作应明确专人负责，并建立本行的计算机病毒防范管理制度，定期进行计算机病毒的检查、清除。

（九）建立计算机系统运行日志，具体记载系统运行情况，运行日志作为机密档案进行管理。

（十）系统维护人员应定期对系统运行情况进行检查，分析系统资源应用及运行情况，并提出系统资源的优化报告。

（十一）运行系统的配置、技术方案、软件和业务测试方案的修改由信息科技部门提出，报分管行长审批后实施。

（十二）系统运行与系统开发和维护要严格分离，确保信息科技部内部的岗位相互制约。

第九条网络通信管理

（一）区域性网络系统改造按省联社网络设计相关规范执行，网络系统改造前应将改造方案形成规范性文档，报省联社科技管理部批准后实施。

（二）网络改造必须在信息科技部统一规划下进行，各支行不得擅自增加、删除网络节点及修改网络参数，确需增加、删除网络节点或修改网络参数的，应严格履行审批手续。并报省联社计算机中心备案。

（三）严格控制远程登录，建立远程登录登记簿，详细记录登录原因、登录人员、起止时间、批准人等内容。登录结束后须及时更改相关的密码、口令。

（四）网络拓扑结构图、网络通信设备的配置参数、网络地址（如IP地址等）等网络通信的技术性资料应及时归档保管，并建立严格的保密制度。

（五）本行内部网络与外单位的联网必须按省联社关于外联业务接入网络的相关要求执行。

（六）网络维护人员应做好网络通信系统的日常运行维护工作：

1．密切监控网络的运行，及时排除网络运行中出现的故障，并做好网络运行和维护的记录。

2．定期分析网络运行状况，形成网络性能优化方案，优化方案报信息科技部负责人批准后实施。

3．严格控制内部网络各节点的通信，防止各种非法访问。

4．网络的通信线路应有备份，对长期处于休眠状态的备份线路应按月进行检测。

第十条权限与口令管理

（一）信息科技部须对主机系统、网络通信运行实行操作权限与口令的管理，并建立操作权限与口令管理登记簿。

（二）操作口令的设置应具备安全性、保密性，密码长度不少于6位，由字母与数字混合组成。

（三）操作口令应定期修改，使用时间一般不得超过一个月，如发现或怀疑泄露应立即更改，修改后须在口令管理登记簿上登记用户名、修改时间、修改人等内容，以备查考。

（四）主机、路由器等重要设备的超级用户口令由信息科技部负责人指定专人设置与管理，并由口令设置人员将口令装入密码信封，在骑缝处加盖个人名章或签字后登记存档。特殊情况需启用封存口令时，必须经过部门负责人书面批准。使用完毕后，须立即更改并封存，同时在口令管理登记簿中登记备查。

（五）普通用户的建立必须由用户使用者提出申请，报信息科技部负责人审批后，由系统、网络维护人员遵循有限授权原则建立。

（六）相关被授权工作人员调离岗位，信息科技部负责人须指定专人接替并对口令立即修改或将用户删除，同时在口令管理登记簿中登记备查。

（七）掌握系统或设备最高用户权限的人员须严格控制该系统或设备的多余用户，一经发现，立即删除，并记录有关信息。

第四章　管理流程

第十一条　网络规划

（一）全辖内部网络系统的规划、设计及设备安装，统一由信息科技部网络管理员负责，并要求严格遵守保密制度。

（二）生产业务网络的规划，原则上必须严格将网络和办公网实行完全的物理隔离。

（三）由于网上银行、远程办公等特殊应用，不能做到完全物理隔离的互联接入应用规划，必须采用国家级计算机信息安全和保密机构，以及中国人民银行计算机信息安全主管机构认可的计算机网络安全架构、设备进行隔离和规划，并应按照上级主管部门相关要求执行或备案。

第十二条　开通流程

（一）由具体应用项目部门填写《内部网络开通、变更审批表》，并提交本部门负责人审批后上报信息科技部。

（二）信息科技部负责人对《内部网络开通、变更审批表》进行审核后，交网络管理人员拟定网络接入方案。

（三）由信息科技部对该应用网络接入的安全性作出安全性评估，信息科技部负责人审批，最后由网络管理人员实施。

第十三条　变更流程

（一）由应用变更需求部门或个人填写《内部网络开通、变更审批表》，并提交本部门负责人审批后上报信息科技部。

（二）信息科技部负责人对《内部网络开通、变更审批表》进行审批后，交网络管理人员实施。

（三）对涉及接入方式和安全架构发生重大变化的应用变更，应按项目开通流程执行。

第十四条　安全管理

（一）网络管理人员负责本行网络（包含局域网、广域网）设备的安装、调试和维护工作，改变网络路由配置和通信地址等参数的操作，必须具有包括时间、目的、内容及维护人员等要素的书面记录，认真填写《网络日志检查登记薄》。

（二）网络系统专用主机设备的用户口令及超级用户口令仅限于信息科技部网络管理人员使用，其口令使用“双人保管，各保管一半”的方式进行管理。口令要求每月进行不定期的更换两次以上，设定口令后要求密封存放在口令保险柜中，以作备份应急时使用。

（三）信息科技部网络管理人员应经常巡查网络系统是否有可疑设备及非法电缆的接入，定期检查网络日志，随时监测和定期检查网络运行状况，对获得的信息应进行分析，发现安全隐患应即时通知安全隐患所辖区负责人和系统管理员并报告信息科技部负责人，提前制止可能的网络犯罪，保护网络系统的安全。

（四）网络管理人员应实时注意观察系统的运行情况，检查登录日志文件，若发现有可疑人员侵入，应立即采取网络应急措施，报告信息科技部负责人。

（五）网络系统实行物理隔离、访问控制、防火墙、网络监控、定期杀毒等安全手段，防止非法用户侵入系统。

（六）实行生产业务网络与办公网络隔离、办公网与互联网隔离的方式进行管理。

（七）任何内部网络终端用户，未经信息科技部许可不得擅自采用任何网络互连设备或其它方式接入网络或其它用途的计算机设备，实行专机专用，专人负责。

（八）网络系统技术文档资料、应用软件及参数设置文件，应交档案管理人员统一管理。

（九）严禁任何人向非授权机构和个人泄露内部网络配置参数和信息资料，擅自更改内部网络的接入方式和架构，以及相关网络和计算机设备的配置参数。

（十）严禁任何人将未经信息科技部许可的计算机及通信设备接入本行内部网络、挪用或移动内部网络通信设备和线路。

第十五条　网络维护

（一）严禁非网络管理人员对网络系统主机进行任何操作。

（二）重要网络通信硬件设施、应用软件设施及网络参数配置应有备份。

（三）支行系统管理人员应协助信息科技部管理好本支行的网络系统设备，不定期地对设备进行检查，若发现设备有异常情况或有可疑设备、非法电缆的接入等，应立即向信息科技部或有关部门反映，及时处理。

（四）各使用部门按照要求加强维护，认真执行有关规定。

第十六条　检查

（一）检查内容：

是否有未允许接入内部网的设备，内部网生产业务用机是否为单应用内部生产业务网络，是否做到“单一应用，专机专用”。

（二）检查时间

信息科技部网络管理人员对内部网用户的连接和使用实行不定期检查。

第十七条　处置

发现问题，信息科技部网络管理人员可立即切断问题设备与内部网的连接，通知应用部门负责人，上报信息科技部负责人，责令其立即整改，并可视情况的严重程度，按本行员工违规违章行为管理规定对违规人员进行处罚。

第五章　附　则

第十八条　本办法未尽事宜，按国家有关法律、法规的规定执行；本制度如与国家日后颁布的法律、法规相抵触时，按国家有关法律、法规的规定执行，并立即修订。

第十九条本办法由xxx银行信息科技部负责解释和修订。

第二十条　本办法自发文之日起施行。