**xxx银行**

信息安全管理办法

第一章 总 则

第一条 为加强xxx银行(以下简称“本行”) 信息安全管理工作，规范信息安全管理过程，建立、健全安全控制措施，保证信息的机密性、完整性、可用性，根据《中华人共和国计算机信息系统安全保护条例》、《金融机构计算机信息系统安全保护工作暂行规定》及相关法律法规特制定本办法。

第二条 信息安全是指保证信息的保密性，完整性，可用性；另外也可包括诸如真实性，可核查性，不可否认性和可靠性等特性。

第三条 信息安全事件是指系统、服务或网络的一种可识别的状态的发生，它可能是对信息安全策略的违反或防护措施的失效，或是和安全关联的一个先前未知的状态。

第四条 一个信息安全事故由单个的或一系列的有害或意外信息安全事件组成，它们具有损害业务运作和威胁信息安全的极大的可能性。

第五条 风险是指在信息系统安全领域，信息资产遭受损坏并给企业带来负面影响的潜在可能性；风险管理是指以可接受的代价，识别、控制、减少或消除可能影响信息系统的安全风险的过程。

第六条 安全措施是指通过防范威胁、减少弱点、限制意外事件造成的影响等途径来削减风险的方法，包括策略、程序、指南、实践或组织结构，它们具备可管理性、技术性、可操作性和合法性。

第七条 访问控制是指为防止对资源的未授权使用而采取的安全措施。

第八条 主机及系统是指小型机、开放平台服务器的操作系统、数据库系统等应用支撑平台及在其上运行的业务应用系统。

第二章 职责与权限

第九条 信息安全管理工作领导小组职责：

按《xxx银行信息科技管理委员会工作制度》（xxx银行行发[2016]84 号）执行。

第十条 信息科技部门的主要职责：

1.负责管理和指导本行信息安全工作；

2.负责牵头制订本行信息安全管理制度、规范、标准和安全方案；

3.负责牵头组织实施本行信息安全方案；

4.负责牵头组织本行信息安全风险防范和安全监督等工作；

5.负责牵头组织本行信息安全知识培训；

6.负责本行安全技术产品的选型、购置等。

第十一条 风险管理部门主要职责：

1.负责信息科技风险管理工作；

2.负责协调制定有关信息科技风险管理策略；

3.负责实施持续性信息科技风险评估，跟踪整改意见的落实；

4.负责监控信息安全威胁的发生。

第十二条 合规管理部门主要职责：

1.负责为业务部门和科技部门提供建议及相关合规性信息；

2.负责监控不合规事件的发生。

第十三条 内部审计部门主要职责：

1.设立专门的信息科技风险审计岗位；

2.负责信息科技审计制度和流程的实施；

3.负责制订和执行信息科技审计计划；

4.负责对信息科技整个生命周期和重大事件等进行审计。

第十四条 各支行、部门的主要职责：

1.按照安全体系规范的要求，组织落实本单位、本部门承担的各专业安全管理任务，制定本单位信息安全实施方案；

2.按专业实施各类安全措施，并对实施结果负责；

3.负责各类安全措施的日常维护和管理。

第三章 信息风险管理

第十五条 信息科技部门应在信息系统的建设、运行、变更管理的过程中引入风险管理，对风险进行评估和控制。

第十六条 信息科技部门应组织各相关部门根据信息资产的重要等级对实施风险管理的信息资产进行识别，并有效识别信息资产的脆弱性、安全威胁，根据及安全事件发生的可能性和产生的影响，定期组织对风险的识别，确定风险等级。

第十七条 各相关部门应根据风险的等级，从技术和管理方面选择和实施安全控制措施，削减、转移或接受风险。选择控制措施时应综合考虑实现成本、技术成熟性、可操作性、实用性等因素。

第十八条 信息资产出现变更后，各相关部门应重新识别风险、确定风险等级并选择和实施安全控制措施。

第十九条 各相关部门应建立相应的管理制度，保证风险管理的落实及维护。应建立和完善安全防范措施，降低安全威胁因素发生的可能性。应建立和完善安全监控措施，提高安全问题和事件的检测、响应和处理效率。

第四章 人力资源安全

第二十条 员工录用前必须进行严格的审查，并应与新员工签署保密协议，明确规定员工的信息安全责任、保密要求及违约的法律责任。

第二十一条 员工任职期间应进行相关安全培训，增强安全意识，提高安全技能，明确安全责任：

1.应进行上岗前的培训，掌握基本技能，培训内容包括：法律、法规、技术、业务、各种管理办法和操作规程、信息系统紧急事件的处理等；

2.要求信息安全管理人员具有较高的政治素质和职业道德，各类安全工作人员必须经过相关的培训，严格考核，持证上岗；

3.应组织员工进行信息安全知识培训；

4.应组织员工进行法律、法规培训；

5.应定期（或不定期）组织员工进行安全教育、安全技能培训，以增强员工遵守信息安全策略和信息安全规范的安全意识，提高安全技能水平；

6.应组织员工进行安全职责、安全程序、安全知识、安全管理规章制度及应急处理程序等方面的培训。

第二十二条 安全管理岗应定期对各部门和员工进行安全责任落实情况考核，考核内容包括安全意识、责任事故、责任问题、问题整改、制度执行等。

第二十三条 安全管理、敏感信息处理等高风险操作岗位必须遵循权力分散、相互制约、权限最小化的原则，并定期轮换。

第二十四条 必须制定员工的安全守则，明确员工在信息系统安全方面的职责、违反安全规定时的惩罚措施、聘用关系结束后的有效期。以适当形式的文件给出工作说明、岗位职责，阐明安全任务和职责，并备案；互斥、不兼容的工作角色必须进行角色分离。

第二十五条 制定并落实信息安全奖惩机制，明确员工奖惩使用情况、证据提供、奖惩手段、审批程序等；奖惩手段包括行政警告或处分、经济奖励或处罚、调离岗位，根据合同予以辞退等方式，对于触犯刑律者，应该交于司法机关处理。

第二十六条 凡涉及本行计算机业务系统和网络安全等的内容，未经批准，任何单位和个人不得在新闻媒体、技术刊物、非保密的外部会议上擅自公开发表，涉密人员不得利用公开通信工具谈论有关机密资源的内容。

第二十七条 员工雇佣合同或条款发生变动时，特别是员工要离开单位或其合同到期时，必须根据保密协议对其工作进行审查；信息系统安全管理人员在调离岗位时，要求履行保密协议，承诺保密事项，并上交有关资料、证件。

第二十八条 信息系统安全管理人员、敏感信息处理人员在转职、离职时，必须对其任职期间工作情况严格审查并执行脱敏期制度。

第二十九条 员工在转职、离职之后，应及时撤销其访问权限，并收回相关信息资料。

第五章 信息资产管理

第三十条 信息资产识别和分类作为信息安全管理工作的基础，安全管理岗应清晰识别本行所有信息资产，并对组成信息系统的系统、设备数据等信息资产进行全面识别和统计，形成资产文档并统一归档管理，建立并维护信息资产清单。

第三十一条 信息资产出现变更后，应对资产清单进行相应的变更处理，并定期对资产文档进行回顾。

第三十二条 信息资产应依据其重要程度，如影响业务的类型和范围、敏感性、关键性等，按照机密性、完整性和可用性进行级别划分，并确定保护需求。

第三十三条 信息科技部门应根据信息资产分级机制，建立信息标记和处理程序。

第三十四条 信息科技部门应明确不同级别的信息资产责任人和访问控制原则，建立信息资产访问的授权机制。

第六章 物理与环境安全

第三十五条 信息科技部门应以信息资产的安全等级、设备对环境要求、易管理性及物理空间分布为主要依据，划分物理安全区域，并根据物理区域安全等级，为其提供相应的安全环境保护。

第三十六条 生产环境、测试环境、开发环境相互之间必须有明确的物理安全边界，在安全边界采取设置门禁、有人管理的接待台等控制措施。

第三十七条 物理安全区域必须有明确的标志，根据物理安全区域等级，制定不同的保护措施和严格的访问控制措施。

第三十八条 信息系统环境的安全控制措施及管理要求按照《xxx银行机房管理办法》执行。

第三十九条 设备管理岗应对本行所有设备建立设备清单，定期对设备清单进行复查。

第四十条 设备管理岗应保护好设备，以减少未授权访问的几率。

第四十一条 对信息系统的相关计算机和数据通信设备及其连接关系，要编制与实际相符的物理连接图和逻辑结构图，并归档保存。

第四十二条 合理规划传输数据或支持信息服务的电源布缆和通信布缆，防止被窃听或破坏。

第四十三条 生产运行系统和网络的关键设备应有备份策略。

第四十四条 信息科技部门应建立设备维护规范，确保维护人员能正确有效的对设备进行维护。

第四十五条 信息科技部门应制定明确的管理制度，来管理办公设备和介质在办公区域以外的使用，保护其免遭破坏、丢失和非法使用。

第四十六条 各单位对存放有信息的磁盘、光盘、磁带、纸张等存储介质必须建立清单并定期复核检查，不同安全级别的存储介质应采用不同的使用和存储要求。

第四十七条 对长期存放的存储介质，必须在介质有效期内对信息进行转存，同时应确保转存所需的物理环境、各种类型介质所对应的转存期限。

第四十八条 设备（包括存储介质）的处置或再利用：

1.必须制定设备在销毁和重用过程中的安全流程；

2.对于存储敏感信息的设备，在将其销毁时，应该确保存储在其上的所有敏感数据被不可恢复地彻底销毁；

3.对于存储敏感信息的设备，在停止使用后或重用前，应确保所有敏感数据已被彻底删除或覆盖；

4.对于已毁坏的包含敏感数据的设备，应对其进行风险评估，以确定是否应该销毁、修理或弃置。

第四十九条 放置在桌面上暂时不用的物理文档，应该及时采用适当的形式进行安全保管。

第五十条 个人计算机、终端在无人使用时，应保持注销状态，并采用锁屏、口令等措施保护起来。

第五十一条 白板、计算机等物品使用后，应及时隐藏或消除其上的信息。

第七章 第三方与外包安全

第五十二条 必须对第三方和外包服务单位应进行严格的资格审查，与第三方或外包服务单位签订合同，且合同中应该明确外包方的安全责任和必须遵守的安全要求。

第五十三条 当第三方与外包服务单位需要对敏感的信息资产进行访问时，应与其签订安全协议书，明确安全责任和义务。

第五十四条 根据信息资产等级及访问形式进行风险评估，确定其安全风险，根据风险等级，采取适当的控制方法对第三方访问进行安全控制，保护信息处理设施和信息资产的安全。

第五十五条 各单位必须做好外来人员的出入管理、访问控制和陪同工作。对需要长期进入本单位工作的第三方和外包服务单位和人员，必须做好其工作区域的隔离和访问控制，并告知工作期间的安全要求。

第五十六条 对第三方的逻辑访问必须严格控制访问权限，并对访问过程进行全程监控、详细记录和及时审计。

第五十七条 对于外包软件开发，必须与软件开发商明确代码所有权和知识产权等条件，并签订保密协议，保证软件相关的文档、源程序、数据结构在软件的整个生命周期内不被非法访问和利用。

第五十八条 本行应建立合理的软件外包验收机制，确保外包方能准确实现软件产品的功能和安全要求，并把整个外包过程纳入检查机制。

第五十九条 信息科技部门应对外部审计所要访问的信息资产进行风险评估并采取有效控制措施，确保审计过程不影响信息资产的安全。

第六十条 信息科技部门应对外包活动履行情况进行检查与评审，以确保外包方履行其安全责任和遵守安全要求。

第六十一条 信息科技部门应对第三方或外包服务商提供的服务变更进行管理，包括保持和改进现有的信息安全方针策略、程序和控制措施，对涉及的业务系统、关键程序再次进行风险评估。

第六十二条 应急事件发生时，应及时通知各相关合作伙伴、供应商协助参与应急处理。

第八章 网络与通信安全

第六十三条 网络管理岗应将全行整个网络系统划分为相对独立的安全域，通过安全域的边界防护和安全域内的统一安全管理实现安全域内的网络安全。

第六十四条 网络管理岗应根据网络安全域的安全级别和风险分析确定的安全需求来设计、实施网络安全方案，安全管理岗应定期组织对网络安全方案进行回顾，检查与实际系统的符合性。

第六十五条 网络系统设计中应采取适当措施，尽可能减少网络崩溃和拥塞发生的几率，提高出现崩溃和拥塞后的系统恢复能力。

第六十六条 网络系统应拥有完善的网管系统提供网络系统状态的实时监控和故障报警。

第六十七条 网络管理岗必须对网络设备配置命令和信息的完整性、合理性及保密性进行验证。

第六十八条 网络管理岗必须对所有当前使用和备用的网络设备建立清单并定期检查。对访问生产系统的外联网络设备应集中管理，应明确外联网络设备的使用方式并对其使用情况进行详细记录。

第六十九条 必须进行规范化网络安全管理，管理内容详见《xxx银行网络安全管理办法》。

第七十条 新建网络、网络改造或变更在投入使用前，网络管理岗应制定相应的网络安全防范措施。安全管理岗负责组织对新建网络或改造后网络实施安全检验，未通过检验不允许投产使用。

第七十一条 严禁擅自将本行内网与外网直接连接，本行内网与外网连接的方案必须经信息科技部门负责人审批，在确保网络安全的前提下实施。

第七十二条 办公网与生产网必须采取严格的隔离措施。对于目前尚无法做到彻底隔离的单位，须采取控制措施。外来人员严禁通过办公网访问生产网。

第七十三条 严格管理 TELNET、PC ANYWHERE 和 WINDOWS 终端服务、X-WINDOWS 等远程访问生产系统方式的使用，使用前应经过安全管理岗审批，限制在只可以从安全的网络进行访问并对系统进行安全配置和记录日志。安全管理岗应定期进行检查。

第七十四条 对路由器、交换机等通讯设备必须采取严格的管理措施，未经批准不得随意移动和接入。

第七十五条 各单位的无线网络建设、无线网络可访问的资源和适用人员范围必须通过信息科技部门审批，无线网络必须采用认证和加密传输等安全技术，并严格按照相关网络技术规范进行建设。

第七十六条 各单位不得建设 Internet 移动办公系统。

Internet 移动办公系统（VPN）可访问的资源和适用人员范围必须通过信息科技部门审批，各单位 VPN 系统的访问范围和权限如需变更，必须对存在的风险进行评估，并将风险评估报告和详细变更方案报信息科技管理委员会审批，未经批准不得擅自变更。

第七十七条 网络设备用户访问网络资源须经过安全认证、合理授权和日志记录。网络管理岗应定期对网络设备用户进行检查。

第七十八条 防火墙策略的制定要遵循最小授权原则和除非明确允许禁止所有其他访问的原则，只开放必须的地址、协议和端口。

第七十九条 利用防火墙、防病毒、安全漏洞扫描、网络非法外联、网络入侵监测软件和工具对获得的信息进行分析时，如发现安全事件，必须按照规定及时处理和报告，并对其日志进行保存和审计。

第八十条 对于外单位需临时从外部网络拨入本行网络的情况，必须遵循以下管理要求：

1.安全管理岗与网络管理岗必须对拨入的必要性、可行性和拨入存在的风险进行评估。

2.拨入前，必须采取必要的隔离和安全控制措施，确保与生产环境的完全隔离，并遵循访问权限和范围的最小化原则。远程拨号接入方式要采取安全方式，确保所有活动的可监控和可审计。

3.拨入过程中，要采取严密监控措施，进行实时监控，要按照既定变更计划控制访问范围和使用时间，防范非法操作。

4.在远程工作完成后，要及时采取物理和逻辑方式断开临行性连接，修改必要的用户权限和配置，防止出现未经授权的再次访问。

第八十一条 严禁将含有涉及本行商业秘密和有关重要业务信息数据的计算机与互联网连接，严禁用于上网的计算机保留涉及本行秘密和有关业务信息的数据。

第八十二条 对网络设备和通信线路应进行定期的检测和维护，确保随时处于可用状态。

第八十三条 必须建立、健全电子邮件、电话、传真、视频会议等办公系统的安全使用制度，并实施必要的安全控制措施，确保办公系统的安全。

第八十四条 不得在本行信息交流群、网络邮件系统中发布、传递与业务无关的信息，及时删除垃圾邮件，不得利用网络系统从事危害本行信息系统安全的活动。

第八十五条 重要专用邮箱的使用应遵循以下安全控制要求：

1.必须安排专人管理和维护重要专用邮箱，限制无关人员对其进行物理访问。

2.发送重要邮件必须经过审批，并进行记录。

3.发送重要邮件的网关/服务器必须配置防止非授权进入内网的机制。其服务器只能发送或接收邮件，不能提供访问网络的途径。

第八十六条 必须明确员工在使用电话等语音设备时的流程及职责，保护交换机设备不被非法使用和重新配置。必须保证 IP 电话的安全，防止被窃听。

第八十七条 视频会议设备必须安排专人负责管理和维护；在公网使用视频会议必须采用加密传输保证视频会议的安全性；视频会议应采用集中控制方式，禁止终端主动呼叫参会。

第八十八条 应对机要传真的使用进行安全控制。配备专门的机要传真机管理和维护人员，发送机要传真需要经过审批，机要传真网关/服务器必须配置防止非授权进入内网的机制，在没有经过安全控制下，传真不能携带高/中安全要求的信息，制定保护机要传真数据的机密性和完整性的措施，进/出的业务传真应该进行记录。

第九章 移动设备安全

第八十九条 本行应建立适当的移动设备安全管理程序, 以防止文件、计算机媒体（如磁带、磁盘）、输入/输出数据和系统文件遭受未授权泄露、修改、删除和破坏。

第九十条 对移动计算机、手机、通讯系统等远程设备设计保护手段，防止移动设备丢失时造成数据丢失或非法接入。

第九十一条 防止外部移动设备非法接入内网，需经过严格审批后方可接入。

第九十二条 信息科技部门应建立移动设备处置机制，防止移动设备在送修、维护、废止时，敏感信息泄露给未授权人员。

第九十三条 在移动设备送修时，对其上的数据进行删除覆盖处理，防止信息泄露。

第九十四条 信息科技部门应建立信息处理及存储程序，以防止信息未授权泄露。

第九十五条 信息科技部门应建立系统文件访问权限管理，以保护系统文件安全。

第九十六条 移动工作终端应该设置超时保护机制。

第十章 信息系统管理

第一节 项目与工程安全

第九十七条 在项目立项前，根据项目所涉及的信息资产的安全等级、项目范围及项目类别，定义项目的安全目标。

第九十八条 根据项目的安全目标，从安全风险管理的角度对项目进行安全风险分析，识别项目所面临的威胁、评估项目的脆弱性、确定发生风险的可能性、明确风险的影响程度，确定风险等级，形成风险分析报告，以确定项目的安全需求。

第九十九条 应根据项目范围、目标、类别，确定项目实施部门、人员，明确其职责；根据安全需求分析，综合考虑实现成本、技术成熟性、可操作性、实用性等，制定安全设计方案，明确安全控制措施及所采取的安全技术。

第一百条 根据设计方案的要求，对使用的软硬件产品进行选型，并对产品进行功能、性能、压力、支持环境等方面的测试，最终确定具体采用的产品。

第一百零一条 在编制实施方案时，方案必须考虑到实施过程中的风险，必须包含详细的实施步骤、应急方案、测试方案和项目实施计划。

第一百零二条 在项目实施过程中如需变更，必须制定明确的变更方案提交相关部门审批后，严格按照变更方案实施变更，确保项目变更的安全。变更方案包括变更的原因、变更设计、变更的风险，变更后的剩余风险、变更对项目的影响，变更的测试内容，变更实施步骤、资源要求，变更的时间安排及回退方案等内容。

第一百零三条 在项目实施过程中必须进行安全管理，明确实施过程中的各种活动和操作的程序及职责，并形成文件。

第一百零四条 项目实施过程中必须由独立部门根据工程安全要求监控项目建设和实施过程，降低实施风险，保证项目安全有效的完成。

第一百零五条 项目实施完成后，必须根据项目验收流程，对项目进行必要的测试和评定并形成验收报告。

第一百零六条 在项目进行过程中，当项目工程的需求不再存在或被新的方案、产品所替代时，经相关部门审批，在确保不对本行的安全生产和业务持续性产生影响的条件下可废止项目。

第二节 应用系统开发与支持

第一百零七条 应用系统开发必须符合项目与工程安全控制规范，应用系统开发整个过程都必须在严密的监督下进行，保证应用系统的安全。所采用的技术和方案，必须保护其信息资产的安全。

第一百零八条 在应用需求调研阶段，应依据风险分析的结果明确所有的安全需求并形成文档，已确定的安全需求应体现在应用系统设计中。安全需求应包括身份鉴别、访问控制、数据安全性、交易安全性、日志生成和分析、容量需求等方面。

第一百零九条 在应用系统安全设计阶段必须对安全需求进行详细的分析，并将已确定的安全需求体现于应用系统设计中。

第一百一十条 在应用系统设计中必须建立访问控制机制，确保可以对系统信息和系统功能的访问进行授权，并且保证只有经过授权的访问才能进行。

第一百一十一条 在应用系统编码阶段，应规范编码，并加强代码安全检查，以减少由于编码不规范给系统带来安全隐患。

第一百一十二条 必须对完成的应用系统进行安全测试，检查所有的安全设计是否得到实现以及应用系统所存在的其它脆弱性。

第一百一十三条 应用系统必须通过安全测试之后才能上线。

第一百一十四条 必须建立代码安全管理机制，对代码进行统一管理，做好代码的登记、备份、存放、访问、变更、作废等整个生命周期的安全管理。

第一百一十五条 对投入运营的应用系统，要具备开发和测试环境，同时开发部门要成立专门技术团队，保持对应用系统代码的升级维护能力和对使用部门的及时响应能力。

第一百一十六条 在对投产后应用系统技术支持时，如涉及变更和升级需求，必须严格按照相关管理规定实施。

第一百一十七条 投入运营的应用系统，开发部门必须对故障记录和维护记录建立规范的档案。

第一百一十八条 必须为应用系统编写管理文档和使用文档，管理文档和使用文档中必须包含正确管理和使用应用系统的方法，并帮助应用系统的管理和使用人员正确理解应用系统提供的安全功能，及紧急情况下所应采取的措施。

第三节 主机及系统开发与支持

第一百一十九条 主机及系统的安全设计必须符合应用系统的安全要求以及主机及系统的安全技术标准，运行关键业务的主机及系统还应考虑性能、冗余、灾备、系统容量、资源分配等。

第一百二十条 系统安全实施部门应按照主机及系统安全规范和标准对所负责的主机及系统进行安全配置，完成后应将配置信息文档化，配置的修改必须严格遵循审批流程。

第一百二十一条 安全管理岗应定期组织进行安全标准的符合性检查。

第一百二十二条 安全管理岗应组织制定主机及系统的命名规范并定期检查落实情况，系统安全实施部门负责命名规范的执行。

第一百二十三条 主机及系统必须在合理的访问控制机制下运行，用户对主机及系统资源的访问，必须进行身份认证和授权，用户的权限分配应该遵循最小授权原则并做到角色分离。

第一百二十四条 对于运行关键业务的主机及系统只允许通过安全的客户端登录程序从安全的网络节点进行访问，用户口令不能采用明文方式在认证请求端和验证端之间传输。

第一百二十五条 用户登录主机及系统没有完全成功时，终端不能显示任何系统标识的信息；在执行操作之前，主机及系统应该有明显的警示信息。

第一百二十六条 用户登录过程中，主机及系统不能提供任何帮助消息，以免被非法用户利用；只有在用户输入所有登录数据后，主机及系统才验证登录信息；主机及系统只显示验证结果，不对登录数据进行任何提示性输出；口令或其它认证方式的变更应当在系统认证成功之后才能进行；登录成功后提示用户上次登录日期。

第一百二十七条 主机及系统应具备警示功能：在执行操作前，所有对主机及系统的访问都必须向用户提供示警信息。

第一百二十八条 安全管理岗应开启主机及系统的用户密码复杂度功能，设置安全的用户密码；严禁多人同时具有同一用户的使用权限；限制登录程序所允许的时限，如超时系统将终止登录过程；应定期对用户进行核对，清理冗余用户。

第一百二十九条 安全管理岗应严格管理生产主机及系统超级用户的使用，使用前应经过审批，安全管理岗应定期对超级用户的使用进行检查。

第一百三十条 主机及系统软件安装时应采用最小安装方式，只安装必须的授权软件，只开启必须的系统服务和功能。

第一百三十一条 各单位和部门必须使用本行统一的防病毒软件，严禁自行安装其他防病毒软件。及时进行防病毒软件的升级工作。总行安全管理岗及网点信息安全员要及时开展防病毒管理工作的监督和检查，对病毒感染事件，及时处理并上报。

第一百三十二条 安全管理岗应及时进行操作系统补丁程序的测试、发布和安装工作。

第一百三十三条 安全管理岗应定期进行主机及系统的漏洞扫描工作，及时发现安全漏洞并督促相关部门整改。

第一百三十四条 安全管理岗应对关键业务的主机及系统采取监控措施，监控主机及系统状态，记录异常状态，处理主机及系统报警，且对监控活动结果进行定期检查。

第一百三十五条 必须对主机及系统的日志进行安全有效的管理。必须创建记录异常事件和安全相关事件的日志，并按照规定的保留期限进行保留。有证据收集方面需求的日志或其它重要日志必须记录归档，必须安全地存储在介质中并定期备份。

第四节 软件安全管理

第一百三十六条 必须对软件进行清单登记管理，并进行复查。登记内容主要包括：来源、使用范围、软件版本、版权、使用情况等。

第一百三十七条 各单位的计算机必须使用本行授权的操作系统、数据库、应用软件和工具软件。

第一百三十八条 各单位的生产、开发、测试及办公计算机必须安装、使用正版软件产品，禁止各类非授权软件在本行的使用。

第一百三十九条 必须对软件（商业软件、自主开发软件、下载软件）获得途径进行严格的管理。

第一百四十条 软件在安装前必须经过严格的测试，安装时必须通过安全控制，安装后必须进行安全性检查。

第一百四十一条 对于本行下发的各类应用软件和工具软件（包括注册码、用户帐户和密码等信息），严禁向软件产品发布范围以外的单位或个人提供。

第一百四十二条 各单位要建立辖内外部软件使用情况监督检查机制，加强日常例行化检查工作，切实杜绝各类非授权软件在本行的使用。

第一百四十三条 对因使用非授权软件给本行带来不良影响的，将追究相关单位和人员的责任。

第一百四十四条 原则上不能安装任何个人软件，如果有特殊需求必须经过严格的审批程序。

第五节 安全技术及使用

第一百四十五条 安全技术包括防病毒、漏洞扫描、入侵监测、拨号外联监测、集中用户管理等。

第一百四十六条 各单位必须根据信息科技部门的部署，安装统一的防火墙、防病毒、拨号外联监测、入侵监测、安全漏洞扫描等安全产品。

第一百四十七条 使用各类安全技术前应报送本行安全管理岗审批，严禁擅自使用。

第一百四十八条 安全技术的使用和管理应制定相应的使用手册、工作流程和工作计划。

第一百四十九条 对生产系统可能造成影响的安全技术，在使用前应经过严格的审批，并与相关部门共同确定影响最小的时间段和安全使用的方法。

第一百五十条 严格保管安全技术的硬件设备、软件介质、使用记录和问题报告，未经批准严禁扩散使用范围和泄露敏感信息。

第六节 密码技术与管理

第一百五十一条 信息系统安全设计和安全管理过程中，应该充分使用现代密码技术提供的安全功能来保护信息资产安全并降低信息系统风险；密码技术的选择和使用必须符合国家密码技术相关的规定和技术标准。

第一百五十二条 密码技术的确定应有相应的专家或组织来评审确定。

第一百五十三条 确定加密使用标准，以指导行内密码技术的使用。加密使用标准应该包含以下内容：

1.加密技术所使用的环境和场合；

2.允许使用的加密技术种类和密钥长度；

3.密钥的管理。

第一百五十四条 选择加密技术应遵循以下要求：

1.根据信息系统风险评估结果，选择密码技术（如数字签名、抗抵赖、数字证书、加密等）和恰当的密码算法；

2.选用密码算法或机制应该遵循国家及本行相关的法律、法规和标准；

3.在项目需求分析及总体方案确定阶段，需根据保护的信息类型、信息的使用方式及保护的时间段来选定相应强度的加密机制；

4.密码算法的选择和强度的确定应该维持“风险－安全－投资”的平衡关系；

5.选用的加密硬件必须符合相关的法律、法规，并达到相应的国际、国家或行业标准。

第一百五十五条 使用加密技术应遵循以下要求：

1.当敏感的或重要信息的完整性与真实性受到威胁时，应该使用数字签名机制；

2.当敏感的或重要信息的机密性受到威胁时，应该使用加密机制；

3.当对事件或行为的发生或未发生可能产生纠纷时，应该使用抗抵赖技术；

4.当使用数字签名的时候，应当考虑相关的法规，使数字签名具有法律约束力；

5.用于数字签名的密钥应当区别于用于加密的密钥。

第十一章 操作与维护管理

第一百五十六条 本行应建立所有信息处理设施的管理和操作职责和程序，并形成操作手册。

第一百五十七条 在正常的生产运行中，所有对生产系统的实质性操作必须按照经过审批的操作手册，由操作员按权限控制要求执行并由双人进行。

第一百五十八条 根据系统变更所涉及的信息资产的安全等级，对系统变更进行分级，针对不同等级的系统变更以文档的形式明确相应的审批管理程序。

第一百五十九条 在系统变更审批前，变更申请部门要提交系统变更方案及申请报告，明确变更存在的风险及对系统的影响。

第一百六十条 信息系统变更应有严格的变更控制机制。

第一百六十一条 所有用户对系统资源的访问必须按照系统安全强度的要求进行授权和认证，用户的权限分配应该遵循最小授权原则。

第一百六十二条 信息科技部门应严格限制和控制关键业务系统特权的分配及使用、账号管理、密码长度及复杂度，防止系统特权的滥用。

第一百六十三条 系统管理员应对用户的口令及口令的使用进行有效的管理。

第一百六十四条 信息科技部门应建立数据备份策略，数据备份策略应包括以下内容：

1.日常备份、特殊日备份或版本升级备份；

2.备份方式、备份时间、备份周期、备份介质、保存环境、保存期限以及数据清理周期。

第一百六十五条 对关键的系统和数据必须进行异地备份,对于在异地进行备份的系统和数据的管理，要与被备份的系统和数据管理保持一致。

第一百六十六条 信息科技部门应依照数据备份策略，定期备份和测试信息和软件。

第一百六十七条 信息科技部门应提供足够的备份设施，以确保所有必要的信息和软件能在灾难或媒体故障后进行恢复。

第一百六十八条 信息科技部门应制定数据恢复策略，包括恢复的时间、周期、可用性要求、实施部门、责任人等。

第一百六十九条 生产系统中不得保留与生产业务无关的程序或数据。

第一百七十条 信息科技部门应定期清理生产数据，数据清理前必须进行数据备份。

第一百七十一条 信息科技部门应记录用户活动、异常和信息安全事件的审计日志，并至少保存一年以上，以支持将来的调查和访问控制监控。

第一百七十二条 信息科技部门应建立信息处理设施的监控使用程序，监控活动的结果要定期评审。根据信息处理设施的重要程度确定监控级别和评审周期。

第一百七十三条 记录日志的设施和日志信息应加以保护，以防止篡改和未授权的访问。

第一百七十四条 管理员和操作员的活动应记入日志，且日志不能被删除或修改。

第一百七十五条 由与信息处理或通信系统的问题有关的用户或系统程序所报告的故障要加以记录。对于处理所报告的故障要有明确的规则，包括评审故障日志和纠正措施。

第一百七十六条 同一区域内所有相关信息处理设施的时钟应使用已设的精确时间源进行同步。

第一百七十七条 应建立访问控制策略并文件化，并基于访问的业务和安全要求进行评审。

第一百七十八条 应有正式的用户注册及注销的程序，以进行对所有信息系统及服务的访问权利的授予和注销。

第十二章 科技文档管理

第一百七十九条 科技文档管理人员要负责审核科技文档的密级定级并按各级别保密要求对涉密文档进行保管和使用管理，严格落实各项保密措施，形成例行化工作内容，以全面落实保密工作责任制。对未达到商密管理要求的文档，也要建立必要的管理措施。

第一百八十条 依据本行各项有关商业秘密保护及信息科技专业保密信息的密级及保密期限划分的制度和文件要求，对科技文档准确划分保密级别并明确安全要求，实施分级安全管理。

第一百八十一条 确定为商业秘密的科技文档应在其载体上以显著方式注明商业秘密密级、保密期限、知悉范围和确定部门，且标注不可与信息内容分离。

第一百八十二条 要以工作需要为原则确定科技文档的授权知悉和使用范围，禁止非必须权限。

第一百八十三条 对科技文档要采取适当的访问控制措施，防止信息的丢失和泄露。对科技文档的访问历史信息进行记录，做到科技文档的访问历史可追溯。

第一百八十四条 在发送确定为商业秘密的科技文档时应采取适当的保密措施。禁止在未采取保密措施的情况下使用公用通讯手段发送科技文档。

第一百八十五条 为确保科技文档安全，各单位保管科技文档的地点应具备防盗、防火、防有害生物等条件，并采用先进技术、设备和监控防护手段，逐步实现科技文档保管的现代化。

第一百八十六条 要建立科技文档存储介质的转移、销毁及重用的安全机制，有效清除或销毁敏感信息，防止信息泄露。

第一百八十七条 在未经授权的情况下，各类科技文档和各单位的内部文档，以及在科技项目研发、测试、生产运行、综合管理等工作中产生的一些过程文档，任何人不能作为个人成果发表和应用。

第一百八十八条 因安全保密管理工作不到位，造成本行科技文档资料泄露，对本行商业利益和信誉直接或间接造成影响，以及对本行信息系统安全带来较大风险隐患的事件，将按照本行商业秘密保护及解除违规违纪员工劳动合同的制度和文件中有关规定对相关单位及个人进行严肃处理。

第十三章 信息安全事故管理

第一百八十九条 本行应建立正常的事件报告及分类程序，来报告可能对本行的财产产生影响的不同种类的事件和弱点。

第一百九十条 信息科技部门应建立信息安全事件报告、事故应答和分类机制，在接到信息安全事件报告后着手采取措施。

第一百九十一条 信息系统和服务的所有第三方用户都要求记录并报告他们观察到的或怀疑到的任何系统或服务的弱点。

第一百九十二条 信息科技部门应建立信息安全事故管理职责和程序，以确保能对信息安全事故做出快速、有效和有序的反应。

第一百九十三条 信息科技部门应建立一套机制对信息安全事故的类型、数量和代价进行量化和监视。

第一百九十四条 当一个信息安全事故涉及到法律行为（民事的或刑事的），需要接下来对个人或组织进行起诉时，应进行证据的收集、保留和展示，以符合相关司法程序中对证据的提交要求。

第十四章 业务连续性管理

第一百九十五条 为贯穿整个组织的业务连续性，应建立一个管理过程，以解决组织的业务连续性对信息和信息安全的需求。

第一百九十六条 本行应能有效识别业务中断事件（例如，设备故障、人为错误、盗窃、火灾、自然灾害及恐怖事件等），以及其对信息安全的影响。

第一百九十七条 本行应制定和实施包含信息安全的连续性计划，以确保在关键业务过程中断或失败后能够在要求的水平和要求的时间内恢复信息的可用性。

第一百九十八条 本行应建立唯一的业务连续性框架，以确保所有计划是一致的，能够协调一致地解决信息安全需求，并确定优先次序以进行测试和维护。

第一百九十九条 业务连续性计划应定期测试和更新，以确保其及时性和有效性。

第十五章 监督检查

第二百条 信息安全管理岗应配合各级监管机构及相关部门的检查。

第二百零一条 安全管理岗应明确监督检查的对象、内容、周期、实施岗位、配合部门和交付件模板，形成监督实施方案，并以此为依据，具体实施监督检查工作。

第二百零二条 安全管理岗在实施监督检查工作过程中，要保留必要的工作记录，整理监督检查报告，并落实整改。

第二百零三条 监督检查应选择对信息系统运行影响最小的方式和时间进行，相关部门应做好配合。

第二百零四条 必须对监督检查工具的使用进行控制，防止滥用。

第二百零五条 对于安全性要求高的信息系统应由独立的第三方安全服务机构进行专业安全测试，促进信息系统安全体系进一步完善。

第二百零六条 安全管理岗应定期组织进行信息安全内部自查活动。

第二百零七条 安全管理岗应从问题发现、问题分类、问题报告、整改实施、追踪反馈等方面建立健全安全问题整改工作机制，督促责任部门采取整改和防范措施，消除问题直接和潜在风险隐患。

第二百零八条 各类安全问题的整改，必须在确认整改方案有效后才能实施。

第二百零九条 通过定期组织生产、测试、研发等环节事故、问题的责任分析和鉴定，以查找安全管理中的漏洞和薄弱环节，不断提高各级部门和人员的安全控制意识，防范问题的再次发生。

第十六章 评 价

第二百一十条 安全管理岗应根据安全管理的内容制定全面衡量管理水平的指标体系。

第二百一十一条 定性指标应包括信息资产管理、风险管理的全面性和时效性、用户访问的安全性、主机及系统的安全设置、网络访问控制的安全性、系统日志的管理和分析的全面性和及时性、数据安全性、员工安全意识、安全规范和标准的符合性、各类补丁及防病毒软件安装的全面性等。

第二百一十二条 定量指标应包括安全违规事件发生次数和增减率、安全培训次数等。

第二百一十三条 评价包括：数据采集、指标计算和对各项指标进行评价。

第二百一十四条 安全管理岗要定期根据安全管理的各项指标采集相关数据，并进行评价。

第二百一十五条 安全管理岗应当根据管理水平指标发展趋势，以及评估报告，制定安全管理的改进计划。

第二百一十六条 根据改进计划，对安全管理的实施过程进行持续改进，对管理的关键部分进行控制，对影响安全管理水平提高的部分进行调整和优化。

第二百一十七条 安全管理岗在对指标体系进行全面评估的同时，根据实际情况可对其进行修订，并提交信息科技部门审批后，对相应的管理指标进行调整。

第十七章 附 则

第二百一十八条 本办法由xxx银行信息科技部负责解释和修订。

第二百一十九条 本办法自发文之日起施行。