非银行支付机构信息科技风险管理指引

第一章　总　则

第一条 为加强非银行支付机构信息科技风险管理，根据国家法律法规和信息安全相关要求、人民银行的行业监管要求以及中国支付清算协会的行业自律相关规定，制定本指引。

第二条 本指引所称信息科技是指计算机、通信、微电子和软件工程等现代信息技术，在支付机构业务交易处理、经营管理和内部控制等方面的应用，并包括进行信息科技治理，建立完整的管理组织架构，制订完善的管理制度和流程。

第三条 本指引所称信息科技风险，是指支付机构运用信息科技的过程中，由于自然因素、人为因素、技术漏洞和管理缺陷导致的操作、法律和声誉等风险。

第四条 本指引适用于中国支付清算协会会员单位中根据中国人民银行《非金融机构支付服务管理办法》规定，取得《支付业务许可证》的非银行支付机构，以下简称“支付机构”。

第二章　信息科技风险管理

第五条 支付机构的负责人是本机构信息科技风险管理的第一

责任人，负责组织本指引的贯彻落实。

第六条 支付机构管理层履行以下信息科技管理职责:

(一) 遵守并贯彻执行国家和行业有关信息科技管理的法律、法规和技术标准，落实中国人民银行相关监管要求，以及中国支付清算协会的相关自律规范，确保持续符合国家、行业相关标准要求。

(二) 配合监管部门及行业自律组织做好信息科技风险监督检查工作，并按照监督检查意见进行整改。

(三) 审查批准信息科技战略，确保其与支付机构的总体业务战略和重大决策相一致; 评估信息科技及其风险管理工作的总体效果。

(四) 履行信息科技风险管理其他相关工作。

第七条 支付机构应制定符合本机构总体业务规划的信息科技战略、信息科技运行计划和信息科技风险评估计划，确保配置足够资源，维持稳定、安全的信息科技环境。

第八条 支付机构应设立专门的高级管理职位，统筹负责信息化规划、建设、运行维护、信息安全、业务连续性等工作，并负责协调制定有关信息科技风险管理策略，尤其是在涉及信息安全、业务连续性计划和合规性风险等方面。

第九条 支付机构应制定全面的信息科技风险管理策略，包括但不限于下述领域:

(一) 信息分级与保护。

(二) 信息系统开发、测试、运行和维护。

(三) 访问控制。

（四） 物理安全。

（五） 人员安全。

（六） 数据安全。

（七） 业务连续性计划。

第十条 支付机构应制定持续的信息科技风险识别和评估流程，确定信息科技中存在隐患的区域，评价风险对其业务的潜在影响。

第十一条 支付机构应依据信息科技风险管理策略和风险评估结果，实施全面的风险防范措施。防范措施应包括但不限于：

（一） 制定明确的信息科技风险管理制度、技术标准和操作规程等，定期进行更新。

（二） 确定潜在信息科技风险区域，并对这些区域进行详细和独立的监控，实现风险最小化。

（三） 建立适当的控制框架，以便于检查和平衡风险。

第十二条 支付机构设立相应岗位和部门，负责信息科技审计制度和流程的实施，制订和执行信息科技审计计划，对信息科技整个生命周期和重大事件等进行审计。

第十三条 支付机构应对信息科技部门内部管理职责进行明确的界定；各岗位的人员应具有相应的专业知识和技能；应对各岗位的人员定期开展信息安全相关培训教育，使其充分掌握信息科技风险管理制度和流程，了解违反规定的后果，并对违反相关规定的行为采取措施。

第三章　信息安全

第十四条　支付机构信息科技部门负责制订信息安全整体方针、政策、制度、规范、流程、实施方案、实施计划和监督机制，支付机构应使所有员工都了解信息安全的重要性，并组织必要的培训，让员工充分了解其职责范围内的信息保护流程及要求。

第十五条　支付机构信息科技部门负责从安全技术和安全管理角度推动信息安全保护措施落地执行，安全技术要求覆盖物理安全、网络安全、主机安全、终端安全、应用安全和数据安全等方面；安全管理要求覆盖安全管理制度、 安全管理机构、 人员安全管理、 系统建设管理、系统运维管理和业务连续性等方面。

第十六条　支付机构应确保其办公区域的安全。明确工作人员的职责，对区域的访问进行授权管理，对敏感数据的访问以及存储设备进行想要的管理，对可能影响安全的时间采取必要的预防、检测和恢复控制措施。

第十七条　支付机构应根据网络承载的业务重要性和数据敏感度，将网络划分为不同的逻辑安全域（以下简称为域），对每个域的边界进行识别控制，采取网络内容过滤、逻辑访问控制、传输加密、网络监控、记录活动日志等措施，保障网络免受干扰、破坏或者未经授权的访问，防止信息泄露或者被窃取、篡改。并制定安全产品与网络设备配置基线。支付机构应考虑对每个域内部进行子域划分，将安全风险隔离在子域单元。

第十八条　支付机构应通过以下措施，确保所有计算机操作系

统和系统软件的安全:

(一) 制定每种类型操作系统的安全要求基线,确保所有系统满足基本安全要求。

(二) 对不同的接触人群进行权限划分,明确定义包括终端用户、系统开发人员、系统测试人员、计算机操作人员、系统管理员、数据库管理员、网络管理员和用户管理员等不同用户组的访问权限。

(三) 制定最高权限系统账户的审批、验证和监控流程,并确保最高权限用户的操作日志被记录和监察。

(四) 要求技术人员定期检查可用的安全补丁,并对切实需要的安全补丁进行评估后进行安装。

(五) 在系统日志中记录不成功的登录、重要系统文件的访问、对用户账户的修改等有关重要事项,手动或自动监控系统出现的任何异常事件。

第十九条 支付机构应采取切实有效的措施,确保所有终端设备的安全,并定期对所有设备进行安全检查,确保符合中国人民银行及银联的监管要求,检查范围应包括台式个人计算机(PC)、便携式计算机、销售终端(POS)等。

第二十条 支付机构应通过以下措施,确保所有信息系统的操作安全:

(一) 明确定义不同职能部门在信息系统中的角色和职责。

(二) 针对信息系统的重要性和敏感程度,采取有效的身份验证方法。

（三） 采取安全的方式处理保密信息的输入和输出，防止信息泄露或被盗取、篡改。

（四） 对信息系统的访问、运行等行为以书面或电子格式保存审计痕迹。

（五） 要求用户管理员监控和审查未成功的登录和用户账户的修改。

（六） 应用系统日志与审计要求。

第二十一条 支付机构应制定相关制度和流程，保护客户身份信息和业务信息，严格管理客户信息的采集、处理、存贮、传输、分发、备份、恢复、清理和销毁。遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围。应采取安全技术措施和安全管理等必要措施，确保客户信息安全，防止客户信息泄露、毁损、丢失和被非授权访问。

第二十二条 支付机构应采取加密技术，防范涉密信息在传输、处理、存储过程中出现泄露或被篡改的风险，并建立密码设备管理制度，以确保：

（一） 使用符合国家、行业管理部门要求的加密技术、加密设备和相关服务。

（二） 管理、使用密码设备的员工经过专业培训和严格审查。

（三） 加密强度满足信息机密性的要求。

（四） 制定并落实有效的管理流程，尤其是密钥和证书生命周期管理。

（五） 重要管理用户与关键业务用户应使用双因素认证。

第二十三条 支付机构应根据不同职能部门职责进行“最小化授权”，对用户权限进行跟踪审计，用户调动到新的工作岗位或离开支付机构时，应在系统中及时检查、更新或注销用户身份，同时要求离岗离职员工签署相关保密承诺。

第二十四条 支付机构应制定相关策略、流程并建设审计系统，管理所有生产系统的活动日志，以支持有效的审核、安全取证分析和预防欺诈。日志保存期限应符合相关法规要求。

支付机构应保证业务日志和系统日志中包含足够的内容、并确保其完整性，以便完成有效的内部控制、解决系统故障和满足审计需要。

第四章 信息系统开发、测试和维护

第二十五条 支付机构应有能力对信息科技工作进行规划、采购、研发、实施和维护，并制定管理制度和流程。应在信息系统投产后一定时期内，组织对系统的后评价，并根据评价结果及时对系统功能进行调整和优化。

第二十六条 支付机构应认识到信息科技项目相关的风险，包括潜在的各种操作风险、政策风险、财务损失风险，并采取适当的项目管理方法，控制信息科技项目相关的风险。

第二十七条 支付机构应制定信息系统相关变更的制度和流程，确保系统的可靠性、完整性和可维护性。

第二十八条 支付机构应将生产环境与开发环境、测试环境进

行有效隔离。

第二十九条 支付机构对个人敏感信息的使用应严格控制使用范围，在开发环境、测试环境等非生产环境使用时应进行脱敏处理，不应使用真实、完整的个人敏感信息。

第三十条 支付机构应制定并落实相关制度、标准和流程，确保数据的完整性、保密性和可用性。

第三十一条 支付机构应建立有效的问题管理流程，以确保全面地追踪、分析和解决信息系统问题。

第五章 信息系统运行

第三十二条 支付机构在选择数据中心机房的地理位置时，应充分考虑环境威胁（如是否接近自然灾害多发区、危险或有害设施）。物理机房应按国家标准设计，严格采取消防、空调、防潮、防静电、防雷击等物理控制措施，监控对信息处理设备运行构成威胁的环境状况，并防止因意外断电或供电干扰影响数据中心的正常运行。

第三十三条 支付机构应建立并实行机房出入的安全管理制度，对人员进出机房情况进行监控和登记。电子设备或存储介质进出机房，须经审批和登记。严格控制第三方人员进入安全区域，如确需进入应得到适当的批准，其活动也应受到监控。

第三十四条 支付机构应确保信息科技部门内部的岗位制约，开发人员不能兼任系统管理员或业务操作员，并对关键岗位和职责做出明确规定。

第三十五条 支付机构应按照有关法律法规要求保存交易记录，采取必要的程序和技术，确保存档数据的完整性，满足安全保存和可恢复要求。

第三十六条 支付机构应建立事件管理流程，及时响应信息系统运行事件，逐级向相关的信息科技管理人员报告事件的发生，并进行记录、分析和跟踪。

第三十七条 支付机构应建立服务水平管理相关的制度和流程，对信息科技运行服务水平进行考核。

第三十八条 支付机构应建立连续监控信息系统服务水平（包括性能、功能等）的相关机制，及时、完整地报告异常情况。

第三十九条 支付机构应制定容量规划，以适应由于外部环境变化产生的业务发展和交易量增长。容量规划应涵盖生产系统、生产备份系统及相关设施。

第四十条 支付机构应制定有效的变更管理流程，以确保生产环境的完整性和可靠性。包括紧急变更在内的所有变更都应做详细记录，执行有效的审核流程。

第六章 业务连续性管理

第四十一条 支付机构应根据自身业务的性质、规模和复杂程度制定适当的业务连续性规划，以确保在出现无法预见的中断时，系统仍能持续运行并提供服务；定期对规划进行培训、更新和演练，以保证其有效性。

第四十二条 支付机构应评估因意外事件导致其业务运行中断的可能性及其影响，包括评估可能由下述原因导致的破坏:

(一) 内外部资源的故障或缺失(如人员、系统或其他资产)。

(二) 信息丢失或受损。

(三) 外部事件(如自然灾难或战争等)。

第四十三条 支付机构应采取双机热备、集群多活、跨机房灾备等措施降低业务中断的可能性，并通过应急预案和演练等方式降低影响。

第四十四条 支付机构应建立维持其业务连续性策略的制度和规范，并制定对策略的充分性和有效性进行检查和沟通的计划。

第七章 外 包

第四十五条 信息科技外包是指支付机构将原本应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；支付机构不得将其信息科技管理责任外包，应合理监督信息科技外包职能的履行。

第四十六条 信息科技外包可能产生风险，并导致支付机构的战略、声誉、合规风险，应当将信息科技外包管理纳入全面风险管理体系，建立与本机构信息科技战略目标相适应的外包管理体系，控制或降低由于外包而引发的风险。

第四十七条 支付机构应当制定和落实信息安全管控措施，防范因外包活动引起的信息泄露、信息篡改、信息不可用、非法入侵、

物理环境或设施遭受破坏等风险。

第四十八条 支付机构应当对外包服务过程进行持续监控，要求服务提供商建立阶段性服务目标及任务，并跟踪任务的执行情况，及时发现和纠正服务过程中存在的各类异常情况。

第四十九条 为降低外包突发事件的可能性及影响，支付机构应当事先对业务连续性管理造成重大影响的外包服务建立风险控制、缓释或转移措施。支付机构应当针对重要外包服务中断的场景，拟定相应的应急计划，并定期进行演练。

第八章 审 计

第五十条 支付机构应根据业务的性质、规模和复杂程度，对相关系统及其控制的适当性和有效性进行评估。支付机构应配备足够的资源和具有专业能力的信息科技审计人员，独立于本机构的日常活动，具有适当的授权访问本机构的记录。

第五十一条 支付机构内部信息科技审计的责任包括但不限于:

(一) 制定、实施和调整审计计划，检查和评估本机构信息科技系统和内控机制的充分性和有效性。

(二) 进行审计工作，在此基础上提出整改意见。

(三) 检查整改意见是否得到落实。

(四) 执行信息科技专项审计。信息科技专项审计，是指对信息科技安全事故进行的调查、分析和评估，或审计部门根据风险评估

结果对认为必要的特殊事项进行的审计。

第五十二条 支付机构可以在符合法律、法规和监管要求的情况下，委托具备相应资质的外部审计机构进行信息科技外部审计。

第五十三条 支付机构应根据业务性质、规模和复杂程度，信息科技应用情况，以及信息科技风险评估结果，确定信息科技外部审计范围和频率，但至少应每一年进行一次全面审计。

第五十四条 支付机构在委托外部审计机构进行外部审计时，应与其签订保密协议，并督促其严格遵守法律法规，保守本机构的商业秘密和信息科技风险信息，防止其擅自对本机构提供的任何文件进行修改、复制或带离现场。

第九章 附 则

第五十五条 本指引由中国支付清算协会负责解释、修订。

第五十六条 本指引自颁布之日起施行。