银联卡账户信息安全管理制度规范汇编

（2014 年版）

中国银联　风险控制部

2014 年 4 月

目 录

第一部分 银联卡账户信息安全管理规则 2
- 银联卡收单机构账户信息安全管理标准 1
- 银联卡账户信息与交易数据安全管理规则（修订） 21
- 银联卡账户信息安全事件应急预案 32
- 银联卡账户信息安全事件调查处理流程 38
- 银联卡收单业务账户信息安全合规评估管理暂行规定 45
- 银联卡账户信息安全合规评估机构管理办法 58
- 银联卡账户信息安全合规评估机构工作指引 79
- 银联卡密钥安全管理规则【磁条卡部分】**V1.0** 85
- 银联卡账户信息泄漏点损失补偿流程 110
- 关于双倍长密钥算法加解密迁移时间进度的要求 119

第二部分 银联卡账户信息安全管理指南及工具 120
- 银联卡账户信息与交易数据安全管理指南 121
- 银联卡密钥安全管理指南【磁条卡部分】**V1.0** 160
- 银联卡 **MIS** 商户账户信息安全管理调查问卷 **V1.0** 191
- 银联卡第三方处理商账户信息安全管理调查问卷 **V1.0** 200

第三部分 典型案例分析 211
- ［案例一］**TJX** 公司账户信息泄漏案 212
- ［案例二］**Heartland** 公司账户信息泄漏案 215
- ［案例三］境内某 **MIS** 商户账户信息泄漏案 217
- ［案例四］收单机构账户信息泄漏案 220
- ［案例五］东莞某酒店侧录案 222

第一部分　银联卡账户信息安全管理规则

银联卡收单机构账户信息安全管理标准

（中国银联风险管理委员会二〇〇八年二月函审通过，
第四届第五次会议第一次修订）

第一章　总则

1.1 目的

为加强银联卡收单网络账户信息安全管理，进一步明确和细化对收单业务各参与方账户信息安全管理要求，防范由收单网络引发的账户信息泄漏风险，根据《银联卡账户信息与交易数据安全管理规则》，特制定本标准。

1.2 适用范围

本标准适用于下列三类机构：

1.2.1 银联网络内从事银联卡收单业务的收单机构

1.2.2 向银联卡收单机构提供收单专业化服务的机构

1.2.3 银联卡收单特约商户

对于上述机构，只要业务涉及银行卡主账号（卡号）的处理、传输或存储，均适用本标准。

收单机构应根据本标准及《银联卡账户信息与交易数据安全管理规则》相关规定，对收单专业化服务机构或特约商户的账户信息安全管理提出具体要求，并通过合作协议的方式予以明确。

第二章　基本要求

2.1 定义

2.1.1 账户信息

账户信息是指银联卡上记录的所有账户信息以及与银联卡交易相关的用户身份验证信息。记录在银联卡上的账户信息包括卡号、卡片有效期、磁道信息（含芯片等效磁道信息）、卡片验证码（CVN 及 CVN2）等信息；与银联卡交易相关的用户身份验证信息包括个人标识代码（PIN）、网上业务、电话银行、手机

银行等业务中的用户注册名、登录密码、支付密码、真实姓名、证件号码、手机号码、动态验证码、生物特征等信息。

2.1.2 敏感账户信息

个人标识代码（PIN）、磁道信息（含芯片等效磁道信息）、卡片验证码（CVN和CVN2）、卡片有效期为敏感账户信息。

2.2 敏感账户信息保护要求

各收单机构、商户、收单专业化服务机构系统不得存储敏感账户信息。

敏感账户信息只用于完成银联卡交易，不得用于除此之外的任何其他用途。

2.3 其他账户信息保护要求

严格控制卡号、证件号码、手机号码等信息的使用和存储。

使用和存储卡号、证件号码、手机号码等账户信息仅限以下业务需要：业务处理，清分与清算，差错处理，业务对账，交易查询与分析，案件协查，风险管理与监控，以及根据法律法规要求使用和存储的业务场景。

对开展基于用户定制类交易需要存储、传输证件号码、手机号码、登录密码、支付密码等账户信息时，必须建立使用与销毁登记制度，并采取严格的保护措施。

在满足上述基本要求的基础上，各收单机构、收单专业化服务机构、特约商户必须按照本标准第三章至第九章的规定管理银联卡账户信息。

第三章　政策制定

3.1 建立账户信息安全管理制度体系

各收单机构应依照本标准，建立账户信息安全管理制度体系，以明确工作职责、规范工作流程。制度体系的管理范畴应涵盖本单位、收单专业化服务机构、特约商户，相关制度至少应包括以下内容：

3.1.1 账户信息安全管理规定

3.1.2 日常管理及操作流程

3.1.3 检查及监督机制

3.1.4 应急处理流程和预案

3.2 制订账户信息安全管理规定

根据本标准中的各项规定，提出本单位账户信息安全管理工作原则，建立内部组织管理架构，明确账户信息安全管理总体要求，并每隔两年或者在业务、系统发生重大变更时根据业务需要及时修订或调整有关制度。

3.3 建立账户信息安全日常管理及操作流程

对账户信息的访问、存储、使用、传输、加密、销毁等环节提出具体安全管理工作要求，明确各岗位在账户信息安全管理方面的工作内容。

3.4 落实账户信息安全管理权限及责任

严格账户信息安全的权限管理，确保以下账户信息安全核心工作落实到岗位，责任落实到人：

3.4.1 管理、控制对账户信息的访问权限

3.4.2 监控所有对机构内部账户信息的访问活动

3.4.3 及时处理突发账户信息安全事件

3.4.4 检查、监督账户信息安全管理规定的落实

3.5 建立账户信息安全检查及监督机制

3.5.1 建立日常管理监督机制（如用户登录日志及操作日志审核），确保落实账户信息安全管理的各项要求。

3.5.2 建立账户信息安全检查机制和工作流程，及时发现管理漏洞，确保账户信息安全。包括：

3.5.2.1 建立账户信息安全日常检查机制和工作流程；

3.5.2.2 定期评估账户信息安全管理方面存在的不足；

3.5.2.3 根据安全管理实际，及时对检查机制和工作流程进行调整。

3.6 建立对收单专业化服务机构及特约商户的账户信息安全管理机制，包括但不限于：

3.6.1 收单专业化服务机构及商户必须严格遵守本标准中的各项规定；

3.6.2 在合作协议或合同中明确收单专业化服务机构及商户应承担的账户

信息安全管理责任；

3.6.3 根据本标准对收单专业化服务机构及商户的账户信息安全管理进行监督检查及认证。

3.7 建立账户信息安全事件应急处理流程和预案

建立账户信息安全事件应急处理流程和预案，定期演练并及时总结演练效果。

3.8 账户信息安全管理审计

定期开展账户信息安全管理相关的内部或外部审计，并根据审计结果完善相关制度、流程。

第四章 组织管理

4.1 岗位职责

4.1.1 设置账户信息安全管理岗位

各收单机构应设置账户信息安全管理岗位，具体负责：

4.1.1.1 制订、管理本单位账户信息安全管理制度与流程；

4.1.1.2 对本单位账户信息的使用进行管理监督及内部审计；

4.1.1.3 对与本单位合作的收单专业化服务机构及特约商户的账户信息安全管理进行监督；

4.1.1.4 对账户信息安全相关事件进行分析处理。

4.1.2 明确各岗位安全责任

各收单机构应明确本单位各相关岗位账户信息安全管理中承担的责任。

4.1.3 账户信息安全管理关键岗位设置

各收单机构、收单专业化服务机构、特约商户对关键的账户信息安全管理岗位应设置专人专岗。

4.2 人员管理

4.2.1 录用员工之前需进行必要的背景调查，确保员工未从事或参与过危害持卡人账户信息安全的事件。

4.2.2 各收单机构应与所有可访问账户信息的员工签署保密协议，或在劳动合同中设置保密条款。

4.2.3 各收单机构应加强员工账户信息安全培训，确保员工了解各自岗位职责、本岗位可访问账户信息的安全等级，以及违反安全规定可能导致的后果。

4.2.4 机构应至少每年一次开展账户信息安全相关制度及管理规定培训或宣贯，并保留相关记录至少 2 年。

4.2.5 员工岗位调动或离职时，应立即终止、删除或变更该员工对账户信息的访问权限。

4.3 违规人员风险信息共享

对因严重违反账户信息安全管理规定而被开除的员工，收单机构应通过中国银联风险信息共享系统报送违规员工个人信息，并标明报送原因。

第五章　访问控制

5.1 基本要求

5.1.1 权限管理

根据“业务需要”和“最小权限”原则，严格控制访问和使用账户信息，任何人都只能访问其开展业务所必需的账户信息，并且只能够获得访问账户信息所必要的最少权限。防止未经授权擅自对账户信息进行查看、篡改和破坏。

应根据“双人控制”原则，对敏感账户信息的访问权限进行分配。

传输、处理、存储账户信息的系统默认用户权限应为“拒绝所有访问”。

5.1.2 身份验证

应至少采用下列一种因素验证访问账户信息的人员身份：

5.1.2.1 根据用户知道的身份证明信息进行身份验证（如密码等）；

5.1.2.2 根据用户持有的身份证明信息进行身份验证（如智能卡、动态口令（OTP）、手机短信验证码）；

5.1.2.3 根据用户特有的身份证明信息进行身份验证（如指纹等生物标志）。

通过远程方式访问账户信息，应采用双因素验证。

5.2 逻辑访问控制

5.2.1 用户账号管理

应分配唯一的用户账号给每个有权访问账户信息的系统用户，并采取以下管理措施：

5.2.1.1 在添加、修改、删除用户账号或操作权限前，应履行严格的审批手续；

5.2.1.2 对于连续 90 天未使用的账号应予以权限冻结,冻结后一定期限仍未使用的，应予以注销；

5.2.1.3 用户间不得共用同一个访问账号。

5.2.2 用户密码管理

应对可访问账户信息的应用系统用户密码管理采取下列措施，降低用户密码遭窃取或泄漏的风险：

5.2.2.1 对不同用户账号设置不同的初始密码；用户首次登录系统时，应强制要求其更改初始密码；

5.2.2.2 用户密码长度不得少于 6 位，应由至少包括数字和字符的组合共同组成，不得设置简单密码；

5.2.2.3 系统应强制要求用户定期更改登录密码，修改周期最长不得超过 3 个月，否则将予以登录限制；

5.2.2.4 应对密码进行加密保护，密码明文不得以任何形式出现；

5.2.2.5 重置用户密码前必须对用户身份进行核实。

5.2.3 系统登录控制

对于可访问和处理账户信息的系统应启用系统登录控制，可采取结束会话、限制登录间隔、限制非法登录次数和自动退出等措施。

5.2.4 远程访问控制

应严格控制通过远程网络对存储或处理账户信息的系统或设备进行访问，如确因业务需要而开放此功能的，应符合如下要求：

5.2.4.1 严格限制远程登录操作业务范围,实施严格的审批程序，对超出业务范围的操作请求应予以拒绝；

5.2.4.2 加强对远程网络或无线网络接入设备的管理，对接入设备进行限制，仅允许指定的设备接入；

5.2.4.3 仅在访问开始前激活远程登录端口，访问结束后应及时关闭；

5.2.4.4 在进行远程登录操作时，不得将账户信息通过远程网络存储到本地硬盘、软驱及其他外部存储介质；

5.2.4.5 远程登录操作应采取加密措施或通过安全加密通道进行，防止鉴别信息在网络传输过程中被窃听；

5.2.4.6 建立远程登录操作文档记录，至少包括：远程访问人员、工作内容、持续时间，并要求监督人签字确认。

5.2.5 无线和移动网络访问控制

若使用无线或移动网络，应采取有效措施确保其使用的安全性：

5.2.5.1 在网络拓扑图中明确标识出使用环境及节点；

5.2.5.2 无线和移动网络与生产网络之间部署防火墙；

5.2.5.3 无线和移动设备的初始默认配置必须进行修改；

5.2.5.4 确保无法通过无线或移动设备直接访问处理、存储账户信息的生产系统。

5.2.6 用户配置文件管理

应严格管理记录有系统用户登录或注册信息控制参数的配置文件，控制访问配置文件的权限，除系统管理员以外，不得向其他系统用户开放对配置文件的访问权限。

5.2.7 日志管理

各收单机构应建立完善的日志记录及审核机制,日志的内容应包括用户 ID、操作日期及时间、操作内容、操作是否成功等。

5.2.7.1 系统应对用户访问账户信息等行为进行日志记录；

5.2.7.2 所有重要系统时钟时间应保持同步，以真实记录系统访问及操作

情况；

5.2.7.3 采取有效措施，防止系统日志被非法篡改；

5.2.7.4 应对系统日志定期进行审核，系统日志记录至少保存一年。

5.3 物理访问控制

5.3.1 存储或处理账户信息的设备和介质应安装在安全的物理隔离区域，实行专人管理，并严格限制对这些设备和介质的物理访问。

5.3.2 安装有存储或处理账户信息设备的物理隔离区域应与其他业务、办公区域相隔离，并设置门禁系统，只有通过身份验证的人员才能进入。

5.3.3 物理隔离区域进出通道均应安装录像监控设备，对人员、设备进出情况进行监控，监控录像资料至少保存三个月。

5.3.4 外部来访人员必须在获得审批授权并进行身份登记后方可进入物理隔离区域,登记记录至少保存一年。

5.3.5 存储或处理账户信息的相关设备必须在获得审批授权后方可移入或移出物理隔离区域。

第六章　账户信息生命周期安全管理

6.1 账户信息处理

6.1.1 个人标识代码的加密

商户终端、公共自助终端等银联卡受理终端应配备经银联技术安全认证的专用密码键盘对个人标识代码进行硬加密，前置系统、主机系统应配备硬件加密机对个人标识代码信息进行加密保护。

对个人标识代码采用双倍长密钥算法或等效安全强度的密钥算法加密保护，密码键盘应具备“开机自毁”功能，在密码键盘外壳被强行打开的情况下，自行销毁设备内的密钥。

通过互联网、移动设备、固定电话等支付渠道输入的个人标识代码，应通过加密等技术措施进行保护，包括但不限于使用支付控件、密码软键盘等。

6.1.2 其他账户信息的加密

个人支付终端采集磁道信息时应进行加密保护，包括但不限于使用加密芯片等。

通过互联网、移动设备、固定电话等支付渠道输入有效期、CVN2、支付密码等账户信息后，应通过加密等技术措施进行保护，包括但不限于使用支付控件、密码软键盘等措施。

6.1.3 密钥管理

6.1.3.1 对称密钥管理

各收单机构应依照《银联卡密钥安全管理规则》（银联风管委〔2004〕2 号），对用于加密保护敏感账户信息的密钥实施严格管理，基本要求如下：

6.1.3.1.1 必须遵循随机或伪随机原则，使用硬件加密机生成密钥；

6.1.3.1.2 除加密机主密钥外的密钥，必须经上级密钥加密保护，以密文形式传输；

6.1.3.1.3 密钥必须保存在密码键盘或硬件加密机内，不得在其他介质中以明文形式显示；

6.1.3.1.4 定期更换密钥；在“双重控制”下，及时删除或销毁已失效、作废或泄漏的密钥。

6.1.3.2 非对称密钥管理

收单机构如采用基于非对称密码体系的加解密、认证、签名等机制，应依照银联卡非对称密码算法使用及密钥管理相关规范，对用于加密保护敏感账户信息的密钥实施严格管理，基本要求如下：

6.1.3.2.1 公私密钥对应在安全计算环境内产生，应正确使用密钥管理规则以确保私钥的机密性和公私钥的完整性及真实性；

6.1.3.2.2 将私钥存储在安全密码设备中，以完整性受到保护的密钥组件的方式存储；

6.1.3.2.3 密钥周期结束或者已知或怀疑私钥已经泄漏时，应停止密钥对的使用，应实施物理控制和逻辑控制来防止密钥的非授权使用；

6.1.3.2.4 应以安全方式实现数字证书的申请和签发。

6.2 账户信息传输

账户信息通过互联网或无线网络传输时，必须进行加密或在加密通道中传输（如 WPA、WPA2、SSL、TLS、IPSEC）。

禁止通过未加密的电子邮件、即时通信工具等终端用户通讯方式，以及通过 FTP 等未加密的网络协议，传输未加密的卡号等账户信息。

6.3 账户信息的使用

6.3.1 开发测试使用要求

采用专门用于测试的测试卡片进行开发测试，真实账户信息不得用于开发测试。严格分离开发环境、测试环境与生产环境，系统开发人员与运行维护人员之间禁止相互兼职或兼岗。

测试环境必须与外部网络物理隔离，否则必须配置防火墙。

6.3.2 通讯日志管理

确因业务需要从生产环境中获取包含账户信息的通信日志（报文）的，必须办理审批手续，在生产环境现场的专有指定环境使用通信日志（报文）。所有通信日志（报文）不得带离现场。确因业务需要将通信日志带离现场的，应建立并执行严格的审批、使用、销毁流程。

6.3.3 卡号屏蔽

在商户终端、公共自助终端等银联卡受理终端打印的交易凭条，以及网页、移动通讯设备或电子邮件中显示卡号信息时，必须采用卡号屏蔽等方式保护卡号安全。其中：

ATM 的打印凭条应遵循以下原则：除吞没卡、转账交易的转入卡号之外，其他交易凭条所打印的卡号应隐去但不限于卡号校验位前 4 位的数字；

POS 及商户自助终端打印凭条应遵循以下原则：除预授权交易外，其他交易打印凭条的卡号应隐去除卡号前 6 位和最后四位的其他位数。

对上述屏蔽的信息使用相同位数的同一特殊字符（*或#等）代替进行替换。

6.3.4 其他账户信息屏蔽

通过互联网、移动设备等渠道采集个人标识代码、支付密码、登录密码等

信息时，应采取屏蔽措施，确保密码信息不明文出现。

对上述屏蔽的信息使用相同位数的同一特殊字符（*或#等）代替进行替换。

6.4 账户信息的存储与备份

收单机构存储支付平台客户账户鉴别信息，包括登录密码、支付密码、生物特征信息等，应加密存储，防范明文泄漏的风险。

卡号与证件号码、手机号等账户信息构成交易授权的完整要素时，对系统中存储的全部或部分信息应采取加密或屏蔽等措施。

所有存储账户信息的系统、设备、介质必须使用物理安全保护措施，禁止未授权访问、读取、打印、截屏、复印、扫描等行为。

备份账户信息的介质必须保存在安全的位置。每年至少检查一次备份介质的安全性、完整性和可用性。

6.5 账户信息的销毁

6.5.1 对于下列情形中超出使用期限，或已经使用完毕的账户信息，均应建立严格的销毁登记制度：

6.5.1.1 因业务需要存储的已超出使用期限的卡号、证件号码、手机号等账户信息；

6.5.1.2 报废设备或介质中存储的账户信息；

6.5.1.3 其他超过保存期限需销毁的账户信息。

6.5.2 账户信息的销毁应符合以下要求：

6.5.2.1 对于所有需销毁的账户信息，应在监督员在场情况下，及时妥善销毁，系统定期自动销毁的除外；

6.5.2.2 对于不同类别账户信息的销毁，应分别建立销毁登记记录，销毁记录至少应包括：使用人、用途、销毁方式与时间、销毁人签字、监督人签字等内容；对于系统定期自动销毁的信息，应通过系统日志等方式建立销毁记录。

第七章　系统及网络安全管理

7.1 网络及防火墙管理

7.1.1 基本要求

所有接入互联网的系统都必须安装防火墙，阻止来自 Internet 网络的非法访问。防火墙应分别安装在互联网接入点与 DMZ 区之间、DMZ 区与内部网络之间。

当存储、处理账户信息的相关系统与本系统安全域之外的不可信网络之间存在网络连接时，应在系统与不可信网络之间安装防火墙。

在任何无线网络与存储、处理账户信息的相关系统之间安装边界防火墙。

7.1.2 防火墙及路由器管理

建立防火墙及路由器的管理规范，规范内容应包括：

7.1.2.1 明确网络拓扑图中所有到账户信息处理相关系统的网络连接（包括无线网络连接）；

7.1.2.2 明确业务必需的服务和端口清单；

7.1.2.3 所有允许从防火墙通过的传输协议都必须经过审批（包括 HTTP、SSL、SSH、VPN 等）；

7.1.2.4 如果允许 FTP 等风险较高的传输协议通过防火墙，应记录使用该协议的原因和已采取的安全措施；

7.1.2.5 按季定期检查防火墙、路由器的规则配置并保留检查记录。

7.1.3 网络访问控制

7.1.3.1 限制通过互联网访问 DMZ 区 IP 的流量；

7.1.3.2 禁止通过互联网访问内部网络 IP 地址；

7.1.3.3 采取动态包过滤技术，只允许“已建立”的网络连接的数据包进入网络；

7.1.3.4 将数据库放置于内部网络，通过防火墙与 DMZ 区隔离；

7.1.3.5 在所有可直接访问互联网的办公电脑及移动电脑上安装个人防火墙软件；

7.1.3.6 采取 IP 伪装技术防止内部网络地址被识别并暴露在互联网上。

7.2 设备安全管理

7.2.1 系统正式投产之前，应更改设备生产厂商提供的设备管理初始密码及相关安全参数（如设备初始管理口令等）；

7.2.2 对于无线网络设备，应更改厂商设定的 WEP key、SSID、管理口令等初始设置，并关闭 SSID 广播；

7.2.3 每台服务器只承担一项处于同一安全级别的主要功能（如 Web 服务器、数据库服务器应该分别部署在不同的设备上），并且虚拟化系统也应视为一台独立服务器，部署前应禁用所有不必要的或不安全的服务和协议，并删除不必要的功能，如脚本、驱动程序或应用。

7.3 防病毒管理

各收单机构均应对本单位所有系统安装防病毒软件，以防范病毒、木马及恶意软件，具体要求包括：

7.3.1 在所有系统中部署防病毒软件（UNIX、Linux、专用 winCE 系统及大型主机系统除外）；

7.3.2 严格限制下载和使用免费软件或共享软件；

7.3.3 通过设置防病毒软件的服务器及时更新病毒库；

7.3.4 定期检查各系统防病毒软件运行及更新情况，并报告检查结果；

7.3.5 所有外部存储介质（软盘、移动硬盘和 U 盘）在使用前，必须进行病毒扫描。

7.4 系统补丁管理

7.4.1 所有操作系统、应用系统均应及时安装厂商提供的最新版本安全补丁，安全补丁应在厂商发布二个月内安装；

7.4.2 在安装安全补丁之前，应通过相应测试，方能投产运行。

7.5 系统安全检查

7.5.1 例行检查

每年定期对系统安全状况进行检查测试（如网络访问控制），确保系统能够有效地识别和阻止来自外部的非法访问。每年/半年测试无线访问点，对未经授权的无线访问点进行侦测并限制其访问内部网络。

7.5.2 弱点扫描

每年定期或在网络发生重大变更后，对系统进行弱点扫描；网络重大变更应包括但不限于下列情形：

7.5.2.1 安装新的设备

7.5.2.2 网络拓扑结构调整

7.5.2.3 调整防火墙配置

7.5.2.4 应用系统升级

收单机构、收单专业化服务机构、特约商户可选择由中国银联认可的有资质的第三方机构进行弱点扫描。

7.5.3 渗透性测试

每年定期或在系统发生重大变更以后，对系统进行渗透性测试，适用情形包括但不限于：

7.5.3.1 操作系统升级

7.5.3.2 应用系统升级

7.5.3.3 网络拓扑变更

7.5.3.4 WEB 服务器变更

收单机构、收单专业化服务机构、特约商户可选择由中国银联认可的有资质的第三方机构进行渗透性测试。

7.5.4 系统入侵检测

应采用入侵检测系统对网络数据传输进行实时监控。对重要服务器进行入侵的行为，能够记录入侵的源 IP、攻击的类型、攻击的目的、攻击的时间，并在发生严重入侵事件时提供报警。

7.6 安全开发流程

开发软件及应用时应满足以下基本要求：

7.6.1 在关键应用系统开发中，不能在程序中配置固定的口令；

7.6.2 系统上线之前进行代码审计，识别可能的恶意代码和可能的安全漏洞。

7.7 变更管理

制定变更管理的流程，以及变更失败的应急方案及回退机制。对系统的所有变更必须遵循变更管理流程，并满足以下基本要求：

7.7.1 将变更流程进行详尽的文档记录；

7.7.2 变更流程由授权方进行审批签字方可执行；

7.7.3 执行变更之前进行功能测试，以确保变更不会影响系统的安全稳定运行。

7.8 Web 安全管理

7.8.1 涉及账户信息的 Web 网站，应至少具备以下方面的防范能力：穷举登录尝试、重放攻击、SQL 注入、跨站脚本攻击、钓鱼、木马等；

7.8.2 涉及账户信息的 Web 网站应使用安全可靠的加密通信方式，保障数据在传输中的安全，如 HTTPS 协议。

7.9 安全配置管理

7.9.1 统一制定基于主机操作系统、网络设备、数据库等方面的安全配置规范，并按照安全配置规范对相关设备进行配置；

7.9.2 对主机操作系统、防火墙、路由器、交换机的重要配置文件进行管理与监控，定期对文件的一致性进行检查，防止在未授权条件下对核心文件进行修改。

第八章　银联卡受理终端及支付应用软件安全管理

8.1 基本要求

银联卡受理终端包括个人支付终端、公共支付终端、商户终端，其允许开通的交易类型应符合《银联卡受理终端业务准入管理办法》(银联业管委[2012]14 号)的要求。

支付应用软件是为完成存储、处理或传输持卡人授权或结算数据的应用软件或程序，包括但不限于支付客户端、支付插件、支付控件、WEB 支付页面以及公共支付终端、商户终端、个人支付终端中的应用程序和配套后台服务器中

的涉及支付业务处理的应用程序等。

银联卡受理终端及支付应用软件应符合《银联卡受理终端安全规范》与银联卡支付应用软件安全相关规范要求，且均需经过中国银联指定的检测机构进行检测并获得安全认证。

8.2 安全要求

银联卡受理终端及支付应用软件仅限于保存当前交易批次内用于交易清分所必需的基本信息要素，并在该批次结束后及时予以清除。

各类受理终端及支付应用软件均不得存储银行卡磁道信息、卡片验证码、个人标识代码、卡片有效期等敏感账户信息。

8.3 对终端机具的日常监控

各收单机构应建立对受理终端的日常监控巡查机制，重点检查 POS、自助支付终端以及自助银行门禁刷卡器，实体终端的入卡口、密码键盘、ATM 出钞口等部件是否被非法改装，防止不法分子窃取账户信息。

第九章　附则

本标准经银联风险管理委员会审议通过后，自发布之日起实施。《银联卡收单机构账户信息安全管理标准》（银联风管委[2008]1 号）同时废止。

附录：

术语表

收单业务

银行卡收单业务，是指收单机构与特约商户签订银行卡受理协议，在特约商户按约定受理银行卡并与持卡人达成交易后，为特约商户提供交易资金结算服务的行为。

收单机构

收单机构，包括从事银行卡收单业务的银行业金融机构，获得银行卡收单业务许可、为实体特约商户提供银行卡受理并完成资金结算服务的支付机构，以及获得网络支付业务许可、为网络特约商户提供银行卡受理并完成资金结算服务的支付机构。

收单专业化服务机构

从事商户拓展与服务，终端布放与维护，交易接入服务，渠道接入服务等的专业化机构。

受理终端

受理终端，是指通过银行卡信息（磁条、芯片或银行卡账户信息）读取、采集或录入装置生成银行卡交易指令，能够保证银行卡交易信息处理安全的各类实体支付终端。

个人支付终端

收单机构对经审核的个人用户发放的，用于完成个人自助支付的一类银行卡受理终端。

经收单机构审核布放于个人使用的固定电话 I 型终端纳入个人支付终端管理。

公共自助终端

收单机构布放于公共场所且无人值守，供持卡人自助完成支付或现金存取的一类银行卡受理终端。

经收单机构审核布放于便民服务点等公共场所使用的固定电话 II 型终端纳入公共自助终端管理。

商户终端

收单机构对符合要求的特约商户布放的，用于商户销售收款的一类银行卡受理终端。

经收单机构审核布放于无集中收银的批发市场用于现场消费使用的固定电话 II 型终端纳入商户终端管理。

固定电话支付终端

电话支付终端通过与电话支付中心进行信息交互、由后台定制交易完成基于银行卡的各种业务功能。以其适用的环境及功能不同分为Ⅰ型终端与Ⅱ型终端。Ⅰ型终端用于家庭等私有场所，Ⅱ型终端用于有人值守的小区和便民点、单位办公室和无集中收银的商品批发市场。

账户信息（AccountInformation）

本标准所指账户信息，是银联卡上记录的所有账户信息以及与银联卡交易相关的用户身份验证信息。记录在银联卡上的信息包括卡号、卡片有效期、磁道信息（包括芯片等效磁道信息）、卡片验证码（CVN 及 CVN2）等信息；与银联卡交易相关的用户身份验证信息包括个人标识代码（PIN）、网上业务、电话银行、手机银行等业务中的用户注册名、登录密码、支付密码、真实姓名、证件号码、手机号码、动态验证码、生物特征等信息。

银行卡主账号（primary account number; PAN）

即卡号，用于标识银行卡所有者及卡片唯一性的号码，由发卡行标识代码、个人账户标识和校验位组成。

个人标识代码（personal identification number; PIN）

即个人密码，是在联机交易中识别持卡人身份合法性的数据信息。本标准中个人标识代码主要限定在发卡机构与持卡人约定的交易密码，不包含支付平台自身的客户鉴别信息，包括登录密码、支付密码、生物特征信息等。

登录密码（Login Password）

用户登录到商户平台、支付平台所使用的用于身份鉴别的密码信息，一般与登录用户名共同使用。

支付密码（Payment Password, Payment Cipher）

用户在商户平台、支付平台进行电子支付交易时提供的用于完成身份鉴别的密码信息。

生物特征信息（biometric recognition infomation）

生物特征信息是指人的生理特征或行为特征，例如指纹、虹膜等信息，可用来进行个人身份的鉴定。

卡片有效期（Expiration date）

发卡机构规定的卡片有效使用时间，印制在卡片的正面左下方位置，超过该时间后，卡片将停止使用。

卡片验证码（card verification number；CVN/CVN2）

CVN 是对磁条信息合法性进行验证的代码，通常写入磁道中；CVN2 是非面对面交易中验证交易者是否持有卡片的代码，通常位于卡片背面。

动态验证码

动态验证码包括动态口令（Dynamic Password/One Time Password（OTP））和短信动态密码（SMS Dynamic Key）等形式，其中动态口令也称动态密码，由令牌种子与其他数据，通过特定算法，运算生成的一次性口令；短信动态密码，又称短信动态验证码、短信密码，是身份认证系统以手机短信形式发送到客户手机上的随机数，也是一种手机动态口令形式，客户在登录或者交易认证时输入，从而确保系统身份认证的安全性。

双因素验证（two-factor authentication）

要求用户从以下三种类型的身份证明措施中出示两种身份证明措施的组合完成验证：一是用户所持有的身份证明（如智能卡），二是用户所知道的身份证明（如密码），三是用户所特有的身份证明（如指纹）。

双人控制（Dual control）

利用两个或多个人共同协调操作以保护敏感或重要信息，确保任何一个人

均不能单独访问、使用敏感或重要信息。

DMZ（隔离区；demilitarized zone）

设置在内部网络和外部公共网络（如 Internet）之间的缓冲带，一般用于对外提供必须公开的服务器设施。

IP（互联网协议）

一种网络层协议，包含地址信息和部分控制信息，数据包根据这些信息被路由，IP 是互联网协议集中最重要的网络层协议。

IPSEC

一系列由互联网工程工作组（IETF）正式制定的，基于 IP 网络（包括 Intranet、Extranet 和 Internet）的开放性 IP 安全标准，通过对所有 IP 数据包进行加密和认证以确保 IP 通信安全。

SSL（安全套接层协议层；secure sockets layer）

一种国际标准的加密及身份认证通信协议，能在浏览器和服务器之间建立一条安全的、可信任的通讯通道，确保数据保密性、完整性和相互鉴定。

TLS(安全传输层协议；transport layer security protocol)

安全套接层协议层(SSL)的后继协议，保障两个相互通信应用之间数据的机密性和完整性。

VPN（虚拟专用网；virtual private network)

通过对网络数据的封包和加密传输，在公用网络上传输私有数据，达到私有网络的安全级别。

硬加密

硬加密是指终端配备专用密码键盘（密码输入模块与加密模块无缝连接，并且密码键盘具备“开机自毁”功能），使用专用密码键盘中的加密芯片进行加密。

银联卡账户信息与交易数据安全管理规则（修订）

（银联风管委〔2004〕8 号审议通过，后经银联风管委〔2006〕6 号修订）

第一章　总则

1.1 目的

为加强银联卡账户信息与交易数据安全管理，保障成员机构及持卡人利益，防止账户信息与交易数据的丢失和泄漏，避免由此带来的欺诈风险，特制定本规则。

1.2 基本原则

银联卡账户信息与交易数据的管理应遵循从严管理、权责明确、过失赔偿的原则，确保账户信息与交易数据在银联卡业务处理各环节中的安全性、完整性和可用性，防止数据遭到篡改、泄漏和破坏。

1.3 适用范围

本办法适用于中国银联、中国银联所有成员机构、所有参与银联卡业务的第三方服务机构以及所有银联卡收单特约商户。其中第三方服务机构既包括从事商户管理、设备维护、信用分析、交易清算、银行卡市场推广等的金融专业化服务机构，也包括参与银行卡产业相关的硬件、软件等产品开发及服务的机构。

1.4 定义

1.4.1 账户信息

账户信息是指银联卡（包括银联标识卡和银联标准卡）上记录的所有账户信息以及与银联卡交易相关的用户身份验证信息。记录在银联卡上的信息包括：卡号、卡片有效期、磁条信息、卡片验证码。与银联卡交易相关的用户身份验证信息包括：网上业务、电话银行、手机银行等业务中的用户注册名、密码、真实姓名、证件号码、联系方式等。

1.4.2 交易数据

交易数据是指银联卡在各类业务中的交易处理数据，数据内容视业务不同而有所不同。基本内容包括：卡号、密码、磁条信息、有效期、卡片验证码。

第二章 权利与义务

2. 1 权利

各机构有权监督与本机构账户信息和交易数据安全相关的其他机构的信息管理状况，一旦发现问题，可向中国银联风险管理委员会报告。

各机构一旦发现其他机构因泄漏本机构持卡人账户信息及交易数据、并给本机构造成损失的，可通过中国银联风险管理委员会向该机构申请损失赔偿。

2.2 义务

各机构应定期就账户信息及交易数据安全状况按照《中国银联账户信息与交易数据安全管理自查问卷》进行自查，并向中国银联提供自查结果等书面报告，证明本机构已按照规定的程序实施了自查。

中国银联将牵头组织成立由各成员机构组成的调查评估小组，对各机构账户信息与交易数据安全管理进行调查，各机构应积极配合调查工作。

第三章 人员及组织管理

3.1 基本要求

建立完善的信息安全管理体制，并制订账户信息与交易数据安全相关的制度及检查程序，明确各数据安全相关岗位的责任与权限。

3.2 人员管理

应与所有接触账户信息及交易数据的员工签署保密协议，在协议中明确员工需要承担的保密责任以及员工离职时的脱密期。

第四章 访问控制

4.1 基本要求

根据“业务需要”的原则，严格控制访问和使用账户信息和交易数据，防止未经授权擅自对数据进行查看、篡改和破坏。业务需要是指“有业务上需要者才能访问相关数据，并且只能访问需要使用的数据”。

4.2 身份验证

使用身份验证机制来授权和确认访问账户信息和交易数据的人员身份，包括进入存储或处理数据物理场所的身份鉴别机制，以及逻辑访问数据的身份鉴别机制。

4.3 权限管理

限制数据访问权限，任何人都只能访问其开展业务所必需的数据。

严格控制员工对账户信息及交易数据的访问权限，访问权限的分配应遵循双人控制的原则，避免单个员工对账户信息及交易数据的完全控制。

在员工调离相关岗位时，应立即通知系统管理人员删除该员工注册的用户名及权限。

4.4 设备访问

为了防止非法访问或者使用通讯设备擅自更改、破坏或泄露数据，应对访问通讯设备的特定程序和访问数据的时间和日期进行严格的控制和记录。

只有被授权人员才能按照事先制定的维护程序来更改设备的设置。

在设备维护前后都应对设备的访问授权控制进行测试。

4．5 密码管理

为不同的用户设置不同的初始密码， 然后由用户自行设定密码。要求用户定期更改密码。

第五章 数据的保护、使用与销毁

5.1 数据的保护

5.1.1 基本要求

严格保护以任何形式出现的账户信息及交易数据，具体包括：存储于各类计算机系统中的、存储在 POS、ATM 及其他终端设备中的、通过网络传送的、显示在电脑屏幕上的、通过 POS 或 ATM 等设备打印出来的各类信息。

指定专人保管保存在磁带、光盘等备份介质中的账户信息及交易数据，应将数据存放在装有门禁系统的机房或保险柜中。

5.1.2 卡号屏蔽

在 ATM 交易凭条、账单、网页、移动通讯设备或电子邮件中显示卡号信息时，必须采用卡号屏蔽的方式保护卡号安全。

5.1.3 账户密码

交易数据中的个人密码除了可以在硬件加密设备上以及在打印密码信封时可以以明文出现，其他情况下都不得以明文出现。

5.1.4 数据传输与存放

账户信息与交易数据在互联网中传输时必须进行加密。对无法以电子方式传输的文件，应以发送方和接收方约定的安全方式传送。

必须对存储在能够通过外网访问的数据库中的数据进行加密。

不得将写有（存有）账户数据与交易信息的文件、软盘、光盘及电脑放置在没有安全保护的地方；同时只能由专人处理这些账户与交易数据。

5.2 数据的使用

5.2.1 基本要求

未经发卡机构的书面许可，其他机构均不得将该发卡机构真实的账户信息及交易数据提供给第三方。

不得将真实的账户信息及交易数据用于软件开发及模拟测试。有特殊情况需要使用真实的账户信息及交易数据进行开发及测试的，必须获得发卡机构的书面许可并签署保密协议。使用时须指定专人保管，并在开发及测试结束后立即销毁。

5.2.2 日志记录

建立账户信息及交易数据访问与使用的日志记录机制与审核机制。日志记录的内容包括：用户身份、使用类型、日期和时间、访问成功标记、访问的数据或系统设备名称等等。风险主管人员应定期审核日志内容。

5.3 数据的销毁

5.3.1 基本要求

各机构可根据本机构的实际情况确定账户信息及交易数据的保存期限，通常不少于两年。对于超出保存期限的账户信息及交易数据，必须及时销毁，以免造成信息的泄漏。

5.3.2 销毁方式

以粉碎或焚毁的方式销毁所有无用或过期的账户信息与交易数据；

通过消磁、删除、破坏等方式对报废设备或介质中的账户信息与交易数据进行处理。

第六章 系统管理

6.1 基本要求

账户信息及交易数据必须在具有安全保护措施的系统中存储、传输， 系统的安全保护措施包括确保网络安全，安装、更新防火墙、防病毒软件等。

6.2 管理措施

当内部网络与外部网络相连接时，必须对网络进行监控， 以及时发现对内部网络的攻击。

当用户通过公共网络访问账户与交易信息时，必须提醒用户“在公共网站填报、访问账户信息可能泄漏交易数据”。

对软件的版权、来源、版本等作详细审核和登记；及时更新操作系统软件，并及时安装软件的安全补丁。

应定期对系统安全性能进行测试，测试的内容包括：系统漏洞，防病毒、防火墙性能等。

从内到外以及从外到内的数据都必须通过防火墙，防火墙必须隐藏它所保护的网络的结构， 并在侦测到异常现象时发出警报。

不得将设备或系统供应商提供的默认值作为与系统安全有关的控制参数，如设备或系统访问密码。

第七章 事故处理

7.1 基本要求

专门制订针对账户信息及交易数据安全事故处理的应急处理方案，确保及时有效地处理各种意外情况。

一旦出现账户信息与交易数据遭到篡改、泄漏和破坏的安全事故，必须立即对事故进行调查处理，并直接或通过中国银联通报相关机构采取措施，避免造成进一步的损失。

7.2 事故报告

成员机构可通过银行卡风险报告系统报告与账户信息与交易数据相关的安全事故；商户及第三方服务机构可通过相关成员机构提交有关报告或直接向中国银联及其分支机构提交有关报告。

第八章 特别要求

8.1 对成员机构的特别要求

8.1.1 第三方服务机构及商户管理

成员机构应每年定期或不定期地监督、检查其第三方服务机构及特约商户，确保其认真执行本办法中对第三方服务机构及特约商户的要求。对于不符合本办法中安全规定的第三方服务机构及特约商户，必须采取控制措施直至其符合规定为止。

成员机构必须对其签约的第三方服务机构或商户的账户信息和交易数据安全负全部责任。

8.1.2 与第三方服务机构或商户签订协议的要求

协议中应当明确第三方机构及商户在账户信息和交易数据安全方面承担的责任，对于所有与自身存在合作关系并能够访问账户信息和交易数据的机构（包括第三方服务机构与商户），必须在与其签订的协议、合同或相关附件中包括以下内容：

严格遵守《银联卡账户信息和交易数据安全管理规则》

未经特别许可，不得将账户信息及交易数据提供给第三方。

承担因本机构账户信息与交易数据管理不善，导致账户信息与交易数据因篡改、泄漏和破坏而造成的全部损失。

如果未能满足中国银联银联卡账户信息与交易数据管理办法的各项要求，成员机构有权解除或终止协议。

无条件配合成员机构或中国银联对其进行的有关账户信息与交易数据安全的检查。

8.2 对商户和第三方服务机构的特别要求

禁止将账户信息和交易数据提供给除收单机构或收单机构指定的代理机构以外的第三方。

除了专门从事发卡系统外包服务的第三方机构外，其他机构只能存储用于交易清分所必需的最基本的账户信息和交易数据， 不得存储磁条信息、卡片验证码及个人密码。

账户信息和交易数据只用于辅助完成银联卡交易，不得将账户信息和交易

数据用于除此之外的任何其他用途，也不能将上述数据提供给任何未被授权的个人或机构。

未经收单机构或中国银联授权，不得擅自对包含账户信息或交易数据的设备进行更改和维护。

第九章 赔偿及处罚

9.1 适用情形

出现下列情形之一者，中国银联风险管理委员会将对经认定的责任方进行处罚：

9.1.1. 泄漏账户信息导致银联入网机构遭受损失[1]：是指经中国银联风险管理委员会认定，由于责任方泄漏账户信息，或者不及时报告、不协助调查账户信息泄漏情况而造成银联入网机构遭受损失。

9.1.2.未达到账户信息安全管理要求：是指在账户信息安全检查中不符合要求，且在检查后的 12 个月内仍不符合本规则要求。

9.2 账户信息泄漏的责任方

9.2.1. 未达到账户信息安全管理要求，或泄漏账户信息造成银联入网机构遭受损失的转接机构。

9.2.2. 未达到账户信息安全管理要求，或泄漏账户信息造成银联其它入网机构遭受损失的入网机构；

9.2.3. 银联卡特约商户未达到账户信息安全管理要求，或泄漏账户信息造成银联入网机构遭受损失的，其收单机构为责任方；

9.2.4. 第三方机构未达到账户信息安全管理要求，或泄漏账户信息造成银联入网机构遭受损失的，与其签订合作协议的成员机构为责任方；

9.3 账户信息泄露事件分级

经 2 家（含）以上成员机构投诉或举报；或中国银联从司法渠道、监管部门获知，中国银联风险管理委员会根据账户信息泄漏规模或账户信息泄漏导致的损失金额大小，将账户信息泄漏事件划分为以下四级：

[1] 本章所指“损失”是指因银联卡账户信息泄露导致卡内资金或卡片信用额度被伪冒使用而形成的直接经济损失。

9.3.1 满足以下任一条件的，为一级账户信息泄漏事件：

- 泄漏银联卡量达 1000 张以上（含）；
- 损失金额 500 万元人民币以上（含）

9.3.2 满足以下任一条件的，为二级账户信息泄漏事件：

- 泄漏银联卡量达 600－999 张；
- 100 万元人民币≤损失金额＜500 万元人民币

9.3.3 满足以下任一条件的，为三级账户信息泄漏事件：

- 泄漏银联卡量达 200－599 张；
- 30 万元人民币≤损失金额＜100 万元人民币

9.3.4 满足以下任一条件的，为四级账户信息泄漏事件：

- 泄漏银联卡量低于 200 张；
- 损失金额低于 30 万元人民币

同一信息泄漏事件中，若泄漏卡片数量和损失金额分别符合以上不同级别的分类条件时，按其所涉及的最高一级分类来确定。

9.4 处罚

9.4.1 对账户信息泄漏责任方的处罚措施

对造成账户信息泄漏的责任方，经由中国银联风险管理委员会同意，根据以上账户信息泄漏事件级别，采取以下处罚措施：

9.4.1.1 通报：向各成员机构通报账户信息泄漏事件和相关责任方；

9.4.1.2. 检查与培训：要求责任方一个月内提交账户信息与交易数据安全管理改进实施计划，接受中国银联风险管理委员会对其进行的安全培训和检查，培训和检查的差旅费用[2]由责任方承担，单次总差旅费用原则上不超过 2 万元人民币；

9.4.1.3. 补偿费：本着“责任方向受害方补偿”的原则，银联卡账户信息发生泄漏的，无论是否已形成损失，责任方均需按照每张卡 10 元人民币的金额补偿发卡机构。对于一级账户信息泄露事件，补偿费总额最高不超过 40 万元。

[2] 本章所指“差旅费用”包括培训、检查人员的往返交通费、市内交通费用、住宿、餐饮等其它差旅相关费用。

账户信息泄漏责任事件由责任方自行发现并主动向中国银联书面报告，且书面报告送达时间早于其它成员机构书面投诉举报时间的，经中国银联风险管理委员会认定，可按照每张卡 5 元人民币的金额补偿发卡机构。对于一级账户信息泄露事件，补偿费总额最高不超过 30 万元。

发卡机构收到中国银联的相关通报后，应在三个月内对已被泄漏信息的银联卡采取换卡、止付等措施，防止损失进一步扩大。

9.4.1.4.罚款：除以上补偿费外，责任方泄漏账户信息造成银联卡交易参与机构遭受损失的，将被处以罚款：

- 对于一级账户信息泄露事件，罚款总额为该起账户信息泄漏事件所造成各受害方累计损失金额的百分之二十五，罚款总额最高不超过 50 万元，所有罚款将根据各受害方遭受损失的比例进行分配；
- 对于二级账户信息泄露事件，罚款总额为该起账户信息泄漏事件所造成各受害方累计损失金额的百分之二十五，罚款总额最高不超过 30 万元。所有罚款将根据各受害方遭受损失的比例进行分配；
- 对于三级账户信息泄露事件，罚款总额为该起账户信息泄漏事件所造成各受害方累计损失金额的百分之二十五，罚款总额最高不超过 20 万元。所有罚款将根据各受害方遭受损失的比例进行分配。
- 对于四级账户信息泄露事件，罚款总额为该起账户信息泄漏事件所造成各受害方累计损失金额的百分之二十五，所有罚款将根据各受害方遭受损失的比例进行分配。

经中国银联通报已发生泄漏的银联卡，自通报发出日起的三个月后再度发生的伪冒使用损失，发卡行不得再要求相关损失计入损失补偿范围。

9.4.1.5 对连续发生账户信息泄漏责任方的追加处罚

对于责任方一年之内再次发生账户信息泄漏事件的，除按照 9.4.1 的相关规定予以处罚外，还应追加处罚，加收 10 万元罚款。加收罚款部分将根据各受害方遭受损失的比例进行分配。

9.4.2 **对未达到账户信息安全管理要求责任方的处罚**

经中国银联风险管理委员会认定，对未达到账户信息安全管理要求的责任方，视情况分别采取以下处罚措施：

9.4.2.1.在账户信息安全检查中，对违反规定或未达到规定相关要求的银联入网机构，由中国银联风险管理委员会发出书面通报，要求其提出具体的整改计划，接受复查，并承担复查人员的差旅费用，单次总差旅费用原则上不超过 2 万元人民币；

9.4.2.2. 经复查仍未达到整改要求的，处以 5 万元罚款，由中国银联风险管理委员会用于对账户信息安全的检查和培训。

9.4.2.3 对拒绝履行处罚义务或拒绝整改，经中国银联风险管理委员会仲裁后仍拒绝履行的，中国银联风险管理委员会有权向中国银联董事会提请暂停或取消其银联卡业务资格。

9.4.3 对于同时出现 9.1 所述两种情形的，分别按照 9.4.1 和 9.4.2 的有关规定进行处罚。

9.5 责任认定及处罚启动

出现 9.1 所述情形的，由中国银联风险管理委员会办公室启动接受投诉、调查取证、情况核实等相关工作，并提交风险管理委员会进行责任认定和处罚实施，具体工作机制另行细化。

9.6 免责条款

对于发生账户信息泄露事件的责任方,在达到银联卡账户信息安全标准的情况下，经由中国银联风险管理委员会裁定,可免于承担相关责任。

第十章 附则

10. 1 修订

中国银联将在广泛征集成员机构合理建议的基础上,对本规则的相关规定进行修订。

10. 2 发布与实施

本规则经中国银联风险管理委员会审定，由中国银联发布并组织实施。各成员机构、专业化服务机构及特约商户可依据本规则，制定内部实施细则。

附录：术语表

访问权限控制（Access Control）：是指通过授权接触信息的人来限制接触信息和信息处理资源的功能。

物理访问控制（Physical Access Control）：是指在未授权人员和被保护的信息来源之间设置物理保护的控制。

逻辑访问控制（Logical Access Control）：指利用其他方法控制访问。

账户和交易信息(Account and Transaction Information)见1.1节中定义。

账号(Account Number)主卡持卡人的账号是指凸印或平印在银联规则卡上的号码。

身份鉴别(Authentication)用来验证身份或证实信息完整性的 过程。

分级(Classification)将信息分成许多类别，以便对不同类别施行适当控制的方法。可以基于信息的类别、重要程度、潜在的欺诈危险性或敏感度进行分类。

信息(Information) 是指一个机构用作转移资金、设定等级、发放贷款、处理交易等所用的任何数据。这些数据可能是电子形式的，也可以是在会议中口头提出的，写在纸张或其他任何媒介上的。这个定义包含了处理系统的软件部分。

公共网络(Public Network) 普通大众都可以进入的网络，包括国际互联网和公共电话系统。

保密性（Confidentiality）：是指账户与交易数据不被泄露给未授权的用户、实体或过程，或供其利用的特性，即数据只供授权用户使用的特性。

完整性（Integrity）：是指账户与交易数据未经授权不能改变的特性。即数据在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱续、重放、插入等行为的破坏和丢失的特性。

可用性（Availability）：是指处理、存储账户与交易数据的系统在规定条件下和规定时间内完成规定的功能的特性。可用性的测度包括：抗毁性、生存性和有效性。

银联卡账户信息安全事件应急预案

（银联风管委〔2007〕7 号）

第一章　总　则

第一条　为及时、有效应对银联卡账户信息安全事件，降低事件造成的经济损失及不利影响，根据《银联卡账户信息与交易数据安全管理规则》相关规定，特制定本预案。

第二条　本预案所称账户信息安全事件（以下简称“事件”）是指银联卡账户信息在存储、传输或使用过程中被泄漏、篡改或破坏，可能或已经对银联、成员机构与持卡人造成经济损失或不利影响的事件；所称事件当事方是指账户信息安全事件涉及的相关方，包括信息泄露方和受损方。

第三条　本预案对应急组织管理、事件先期处理和后续跟踪、事件信息发布等方面做出了相关规定，适用于中国银联、中国银联成员机构、参与银联卡业务的第三方专业化服务机构以及银联卡特约商户等所有存储、传输或处理银联卡账户信息的银联网络参与方。

第四条　中国银联风险管理委员会（以下简称“风管委”）负责制定、修订银联卡账户信息安全事件应急处理工作机制与流程，并监督各参与方执行。

第二章　组织管理要求

第五条　中国银联及各成员机构应根据自身情况，制定内部账户信息安全事件应急预案，包括但不限于以下内容：

（一）指定专门部门或人员负责应急处理；

（二）明确内部应急处理流程；

（三）规定各项应急处理措施；

（四）管理应急事件的信息发布。

第六条　中国银联、各成员机构及其他所有存储、传输或处理银联卡账户信息的银联网络参与方应指定专人及其候补人员作为银联卡账户信息安全事件应急处理联系人（申报信息详见附表 1），保证 7 天×24 小时通讯畅通，其主要

工作包括：

（一）按照本预案的时限要求，及时向中国银联报告银联卡账户信息安全事件；

（二）接收并及时向机构内部负责人报告其他机构发送的事件通报，配合实施应急处理；

（三）配合公安机关或其他机构调查及处理账户信息安全事件；

（四）其他应急处理事宜。

第七条　中国银联及各成员机构应将与之合作的第三方机构及商户纳入本机构账户信息安全事件的应急处理范围，建立与第三方之间的应急处理流程，并监督其落实账户信息安全管理要求，配合应急预案的实施。

第八条　各成员机构应结合实际情况，有计划、有重点地组织进行应急处理预案演练，不断完善应急处理流程。

第九条　中国银联负责收集、公布、维护各机构账户信息安全事件联系人名单，及时通报账户信息安全事件，协调组织并参与事件应急处理，协助成员机构降低风险损失。

第三章　事件先期处理

第十条　一旦发生账户信息安全事件，事件当事方应在发现后 3 个工作日内填报《银联卡账户信息安全事件基本情况通报表》（见附表 2），报送至中国银联；涉及跨行的账户信息安全事件，事件当事方应在发现后 1 个工作日内通报中国银联。

第十一条　信息泄露方应立即采取应急处理措施，如：

（一）暂停涉嫌发生账户信息事件的商户终端、MIS 系统、网站、第三方机构系统等信息泄露点的交易处理，并与网络内其他系统实施隔离；

（二）对已被隔离的泄露点进行排查，必要时应联系系统厂商或开发方协助调查，初步确定事故发生原因；

（三）对涉嫌泄漏账户信息的操作人员进行调查，要求其暂时离岗；

（四）如有必要，应向公安机关报案，并积极配合案件侦破工作；

（五）其他应急处理措施等。

第十二条　事件受损方应立即采取应急措施，对于本机构可能或已确认发生信息泄露的相关卡片及时采取止付、换卡等风险控制措施，防止损失进一步扩大。

第十三条　中国银联在收到事件当事方通报后二个工作日内，向疑似或已确定遭受损失的成员机构发送风险提示，并向信息泄露方反馈应急处理指导意见，要求其尽快落实各项应急措施，协助控制不利影响。

第四章　事件续报与跟踪

第十四条　信息泄露方应在发现账户信息安全事件的十个工作日内，向中国银联提交《账户信息事件应急处理通报》，通报以下情况：

（一）事件基本情况：事件持续时间、涉及卡片数量、初步确定的损失金额等；

（二）事件风险点分析：事件发生原因、风险管理漏洞或系统缺陷等；

（三）已采取的应急处理措施；

（四）改进措施及整改方案。

第十五条　信息泄露方应尽快实施账户信息安全整改工作，消除安全隐患，包括但不限于以下方面：

（一）清除系统中病毒、木马等非法程序；

（二）对相关系统执行漏洞扫描，消除技术漏洞；

（三）更正或修补相关管理制度的问题或缺陷；

（四）要求相关第三方机构或商户修补、消除管理和技术漏洞，对于拒不执行的，终止合作或撤销其银联卡受理资格；

（五）对内部相关责任人员实施处理。

第五章　事件信息发布

第十六条　各成员机构应遵循保密原则，密切关注社会公众对事件的反应，审慎发布相关信息。信息发布时，不得损害其他成员机构利益和银联品牌形象。

第十七条　中国银联协助各成员机构在应急处理过程中，及时应对媒体，协调沟通信息，避免引起不良社会影响。

第十八条　账户信息安全事件基本得到控制，中国银联风险管理委员会办公室将按照《银联卡账户信息安全事件调查处理流程》，启动对事件的调查、责任认定及处理程序。

第六章　附　则

第十九条　本预案经中国银联风险管理委员会审定、发布。

第二十条　本预案自发布之日起实行。

附表 1：

银联卡账户信息安全事件应急处理联系人申报表

填报单位：　（印章）　　填报时间：　　年　月　日

联系人	姓 名		部门（处室）	
	职 务		传 真	
	办公电话		手 机	
	邮 编		电子邮箱	
	通信地址			
候补联系人	姓 名		部门（处室）	
	职 务		传 真	
	办公电话		手 机	
	邮 编		电子邮箱	
	通信地址			

附表 **2:**

银联卡账户信息安全事件基本情况通报表

通报单位		**发现事件的时间**	
事发单位			
事件概述			
已明确的事件情况			
涉及发卡机构			
涉及信息泄露点 **（请对应打“√”）** 篇幅所限，可另行附件说明	☐ ATM　　请说明：终端编号：_____，　机具地址：_____ ☐ 特约商户　是否为 MIS 商户：☐ 是　☐ 否 商户代码：_____，　终端编号：_____， 商户地址：_____ ☐ 其他信息泄漏点　　请说明泄漏点详细信息：_____		
涉及卡片范围和数量	如涉及泄漏的卡片 BIN 号范围、泄漏时段内涉及的卡号清单等（篇幅所限，可另行附件说明）	**涉及欺诈金额（万元）**	
其它情况			
本单位已采取的应急处理措施			
需进一步调查确认的问题及拟采取的工作措施			
经办人签字：		**单位负责人签字（公章）：** **报告时间：**	

银联卡账户信息安全事件调查处理流程

（银联风管委〔2007〕8 号）

第一章　总 则

第一条　为落实《银联卡账户信息与交易数据安全管理规则》第九章“赔偿及处罚”相关规定，界定账户信息安全事件责任，实施对事件责任方的处理，保障成员机构合法权益，特制定本流程。

第二条　本流程所称账户信息安全事件（以下简称“事件”），是指银联卡账户信息在存储、传输或使用过程中被泄漏、篡改或破坏，可能或已经对银联、成员机构与持卡人造成经济损失或不利影响的事件。

第三条　对账户信息安全事件责任方的处理，应遵循实事求是和公平、公正原则，经中国银联风险管理委员会（以下简称“风管委”）同意，由中国银联风险管理委员会办公室（以下简称“风管委办公室”）负责实施。

第四条　本流程适用于中国银联、中国银联成员机构、参与银联卡业务的第三方专业化服务机构以及银联卡特约商户等所有存储、传输或处理银联卡账户信息的银联网络参与方。

第二章　成立事件调查工作小组

第五条　账户信息安全事件基本得到控制，风管委办公室将依照本流程，启动对事件的调查、责任认定及处理工作。

第六条　风管委办公室接受中国银联风险管理委员会委托，成立事件调查工作小组（以下简称“工作小组”），对银联卡账户信息安全事件进行调查处理，其工作职责主要包括：

（一）对账户信息安全事件进行调查，核实事件波及范围，评估事件不良影响，确定事件责任方；

（二）收集并核实遭受信息泄漏的成员机构卡片更换及发生损失的情况；

（三）判定账户信息安全事件等级，执行风管委对事件责任方的处理决议，协调组织向遭受损失成员机构进行换卡成本补偿和损失赔偿。

第七条　风管委办公室可视事件实际情况，邀请有关单位委派专家，共同参

与调查及处理工作。

第三章　事件调查

第八条　工作小组根据信息泄露方的报告及其他机构的投诉举报材料，以及司法、监管部门提供的相关材料，对于账户信息安全事件展开调查，调查过程中，信息泄露方应按要求提供包括但不限于以下资料：

（一）已初步明确的泄露点、泄露持续时间和涉及卡片的交易流水；

（二）信息泄露事件的引发原因说明及风险点分析，及已采取的应急处理措施说明；

（三）如涉及内部人员作案，对相关人员的处理情况说明；

（四）如涉及与之合作的第三方机构或商户，对第三方机构或商户的处理情况说明；

（五）信息泄露方内部相关管理制度和操作日志；

（六）下一步整改措施和方案。

第九条　工作小组视情况决定是否需要进行实地调查，实地调查时，信息泄露方应积极配合提供资料，安排访谈，并协助工作小组对泄露终端或商户、系统机房等物理区域进行检查。

第十条　工作小组根据调查结果于 1 个月内提交调查报告，并提请信息泄露方对调查报告予以反馈确认。

第十一条　信息泄露方对调查报告有异议的，应在收到报告后的 5 个工作日内予以反馈，并向工作小组提交相关补充材料。

第十二条　工作小组审核信息泄露方提交材料的真实性和合理性，决定是否对调查报告进行修订，并将最终调查报告于 10 个工作日内再次向信息泄露方反馈。

第四章　责任及损失范围界定

第十三条　工作小组根据调查报告，形成《关于明确账户信息安全事件责任及损失补偿范围的工作建议》（以下简称“《工作建议》”），明确如下内容：

（一）明确账户信息安全事件责任方；

（二）确定账户信息安全事件的具体泄露点和泄露持续时间；

（三）划定可能或已经遭受损失的成员机构范围；

（四）明确涉嫌信息泄漏的卡号及交易明细清单、卡片数量，及初步损失金额等。

第十四条 工作小组将《工作建议》及相关材料提交风管委进行审议，以全体委员的三分之二以上（含）表决意见，作为本次事件调查处理的有效决议。

第十五条 审议通过后，《工作建议》将作为对事件责任方进行责任追究及处理的依据，并通报相关成员机构；如未获通过，风管委将责成工作小组于 10 个工作日内对相关事件重新核实损失补偿范围，再次提交风管委审议。

第十六条 如事件当事方未尽配合义务，工作小组将在准确核实基础上，以各成员机构投诉举报资料作为损失补偿范围界定依据，提交风管委审议。

第五章 申报损失

第十七条 相关成员机构根据《工作建议》，在 3 个月内向工作小组申请更换卡片的成本补偿及损失赔偿。申报材料应通过快递方式直接寄送至风管委办公室。

第十八条 申报换卡成本补偿的，应提交加盖单位公章的换卡成本补偿申请表（详见附表 1）。

第十九条 申报损失赔偿的，应提交加盖单位公章的损失赔偿申请表（详见附表 2），并应同时满足以下条件：

（一）仅针对因账户信息泄漏所产生伪卡、账户盗用的欺诈损失进行申报；

（二）遭欺诈使用的卡片在损失申报日前已被止付；

（三）相关欺诈交易发生日期应早于《工作建议》发布日期，且不超过账户信息泄漏风险提示发布之日起三个月；

（四）已在损失申报日前向中国银联报送欺诈交易，并以中国银联反馈的“交易报告序列号”为准；

（五）损失申报截止日之前，相关欺诈交易未提起退单或争议。（举例说明：若《工作建议》发布日期为 2007 年 7 月 1 日，则损失申报截止日（2007 年 9 月 30 日）之前已提交退单或争议的欺诈交易，无论退单或争议成功与否，将不列

入损失赔偿范围。）

第二十条　如事件责任方提出要求，中国银联可协助各损失申报方提供被伪冒使用的卡片在已认定的泄漏点和泄漏时间内发生的经银联转接的跨行交易明细。

第二十一条　申报材料未达到上述要求的，工作小组通知成员机构尽快补充完善；逾期申报的不予受理。

第二十二条　成员机构不得对同一张卡片重复申报换卡补偿，也不可就同一笔交易重复提交损失赔偿。

第六章　责任承担

第二十三条　工作小组审核申报材料是否真实、完备和有效，并在 2 个月内对所有申报材料进行汇总，形成《对账户信息事件相关责任方的处理意见》（以下简称“《处理意见》”）通报风管委，并明确如下内容：

（一）账户信息安全事件等级；

（二）账户信息安全事件涉及的更换卡片数量，以及损失金额；

（三）事件责任方应承担的换卡成本补偿及损失赔偿的总金额；

（四）换卡成本补偿及损失赔偿的分配；

（五）是否对责任方进行其他处理的建议。

第二十四条　工作小组根据《处理意见》编制《账户信息安全事件受偿金额明细表》（详见附件 3），连同已发生的，应由责任方承担的调查、培训及检查相关费用明细清单，提交责任方和相关报损方。

第二十五条　工作小组将资金划拨指令提交中国银联上海信息中心纳入当日清算，通过差错处理平台“收/付费交易”，直接从责任方清算账户中扣除，并向报损机构清算账户中划拨补偿资金。

第七章　附　则

第二十六条　本流程经中国银联风险管理委员会审定、发布。

第二十七条　本流程自发布之日起实行。

附表 1：

换卡成本补偿申请表

申报机构名称（公章）：_____ **申报机构代码：**_____ **申报日期：**____年___月____日

序号	持卡人姓名	持卡人身份证号	原卡号	原卡止付日期 (YYYY/MM/DD)	新发卡号	卡片新开日期 (YYYY/MM/DD)	备注

（以下为事件调查工作小组成员填写）

审核人签字：_____ 复核人签字：_____ 工作小组负责人签字：_____

附表 2：

损失赔偿申请表

申报机构名称（公章）：_____　　申报机构代码：_____　　申报日期：____年___月____日

序号	卡号	卡片类型	卡有效期（YY/MM）	交易日期 (MM/DD)	交易金额（元）	服务点输入方式码	发卡方应答码	收单机构代码	特约商户代码	欺诈类型	备注

卡片类型：01 借记卡、02 贷记卡、03 准贷记卡

欺诈类型：01 失窃卡、02 未达卡、03 虚假申请、04 伪卡、05 账户盗用、06 商户欺诈、07 其他

（以下为事件调查工作小组成员填写）

审核人签字：_____　　复核人签字：_____　　工作小组负责人签字：_____

附表 3：

账户信息安全事件受偿金额明细表

受偿机构名称	受偿机构代码	换卡数量（张）	换卡补偿金额（元）	欺诈损失金额（元）	该机构损失金额占该事件总损失金额比例（%）	账户信息安全事件等级	损失赔偿金额（元）	该机构应得受偿总金额（元）
总　计								

换卡补偿金额＝换卡数量×单卡补偿标准

损失赔偿金额＝某机构欺诈损失金额×该机构损失金额占该事件总损失金额比例×对应事件等级的罚款标准

以上换卡补偿标准、罚款标准比照《银联卡账户信息与交易数据安全管理规则》第九章“赔偿及处罚”（银联风管委 2006〔6〕号）相关规定执行

制表日期：_____年___月___日　　制表人签字：_____　　复核人签字：_____　　工作小组负责人签字：_____

银联卡收单业务账户信息安全合规评估管理暂行规定

（银联风管委〔2008〕3 号）

第一章 总则

第一条 为提高银联卡收单业务账户信息安全管理水平，规范账户信息安全合规评估工作，依据《银联卡账户信息与交易数据安全管理规则》和《银联卡收单机构账户信息安全管理标准》（以下简称“《标准》”）相关要求，特制定本规定。

第二条 本规定所称账户信息安全合规评估，是指根据银联卡账户信息安全管理相关规则，通过问卷自查或聘请银联卡账户信息安全合规评估机构（以下简称“合规评估机构”）等方式，履行合规义务以确认符合银联卡账户信息安全管理要求的过程。

第三条 本规定所称银联卡账户信息安全合规评估机构，是指依据《银联卡账户信息安全合规评估机构管理暂行办法》，取得合规评估资质，提供账户信息安全合规评估服务的专业化机构。

第四条 中国银联风险管理委员会授权其办公室（以下简称“风管委办公室”）具体组织实施银联卡账户信息安全合规评估管理工作。

第五条 中国银联、中国银联风管委及其办公室不对合规评估机构与银联卡业务机构之间，因账户信息安全合规评估过程和结果产生的损失负有赔偿责任，但应督促有关单位依照本规定开展合规评估工作，并积极协助成员机构进行风险责任界定及处理。

第六条 收单机构及收单业务合作机构（以下统称为“收单机构”）依照本规定工作流程及要求，积极组织与本机构开展合作的特约商户或第三方收单专业化服务机构进行合规评估。以下将合规评估对象统称为“被评估单位”。

第二章 评估要求

第七条 银联网络内业务涉及银联卡主账号（卡号）处理、传输或存储的特约商户或第三方收单专业化服务机构每年需开展一次账户信息安全问卷自查。其中，满足以下任一条件的单位，还需聘请合规评估机构开展外部合规评估：

（一）上一年度银联卡跨行交易处理量达一定笔数的实体商户或互联网商户

(标准详见附 1)；

（二）上一年度银联卡跨行交易处理量达一定笔数的实体商户第三方收单专业化服务机构或互联网第三方收单专业化服务机构(标准详见附 1)；

（三）过去一年内曾发生二级以上（含）账户信息泄漏事件的特约商户、第三方收单专业化服务机构；

（四）经银联风管委认定，或国家监管部门要求需开展外部合规评估的特约商户、第三方收单专业化服务机构。

第八条 对于第七条情形以外的开展收单业务的各类机构,鼓励主动申请开展外部合规评估。

第九条 收单机构如发生二级以上（含）账户信息泄漏事件，经中国银联风险管理委员会建议或国家监管部门要求进行账户信息安全外部合规评估的，可依照本规定工作流程执行。

第三章 评估流程及结果运用

第十条 每年 3 月底前，风管委办公室根据上一年度银联卡跨行交易处理量统计情况，分析、整理达到外部评估条件的被评估单位名单，报备银联风管委；其余机构则按要求开展问卷自查。

第十一条 收单机构督促辖内第三方收单专业化服务机构和特约商户完成问卷自查，根据自查情况在年内完成整改，并报备风管委办公室。风管委办公室负责对机构的自查和整改情况进行抽样检查，实施相应处理。

第十二条 对于达到外部评估条件的被评估单位，风管委办公室将向与其签约的收单机构发送《外部合规评估通知书》（附 2）。收单机构需组织被评估单位在 90 个工作日内，依照流程及评估要求完成外部合规评估工作。

第十三条 收单机构在收到通知后的 20 个工作日内，需组织被评估单位启动以下合规评估准备工作，并将《外部合规评估预备工作情况反馈表》（附 3）报送风管委办公室：

（一）指定本次评估工作专项联系人；

（二）制定合规评估工作计划；

（三）启动问卷自查工作；

（四）选择确定合规评估机构。

第十四条　合规评估费用的支付。

（一）对于符合本规定第七条（一）、（二）款情形的，由合规评估机构与被评估单位及其收单机构自行协商确定。

其中，同一家特约商户或第三方收单专业化服务机构的分支单位（如分公司、分店等）分别与不同收单机构签约开展业务合作的，有关收单机构可协商共同组织开展账户信息安全联合评估。评估计划、工作进度、费用支付等具体事宜由被评估单位、有关收单机构与合规评估机构共同协商确定。

（二）对于符合本规定第七条（三）、（四）款情形的，主要由负有责任的特约商户、收单专业化服务机构承担评估费用。

第十五条　收单机构组织被评估单位选择已取得银联卡账户信息安全合规评估资质的专业化机构，签订书面协议，明确保密条款。

第十六条　合规评估机构根据《银联卡收单机构账户信息安全管理标准》等账户信息安全制度规范，向被评估单位提供账户信息安全合规评估服务，包括但不限于以下方面：

（一）与被评估单位的信息安全管理人员进行访谈，审核自查问卷，了解其账户信息安全管理基本情况，分析可能存在的安全隐患；

（二）查阅被评估单位信息安全岗位设置、人员管理、工作流程、应急处理等方面的规章制度；

（三）通过现场查看、弱点扫描、渗透性测试、穿行测试等手段，对被评估单位的账户信息安全管理水平和风险控制措施进行评估；

（四）发现被评估单位在账户信息安全管理方面存在的问题和漏洞，提出整改建议。

第十七条　合规评估机构在评估完成后的 10 个工作日内，以书面形式向被评估单位的收单机构出具《银联卡账户信息安全合规评估报告》，明确被评估单位是否达到合规要求，指出现存问题，提出改进建议，并由被评估单位确认评估结果。

对于被评估单位不能确认的评估意见内容，评估机构应出具详细的解释或说明。

第十八条　收单机构确认《评估报告》内容，并在 15 个工作日内将以下材料提交风管委办公室审核：

（一）银联卡账户信息安全合规评估报告；

（二）银联卡账户信息安全整改工作计划（如需整改）；

（三）银联卡账户信息安全合规评估服务意见反馈表（附 4）。

第十九条　银联风管委办公室围绕以下内容，在 15 个工作日内对收单机构提交的合规评估材料进行审核：

（一）合规评估过程是否遵循本规定工作要求；

（二）合规评估内容是否涵盖主要的考察要素；

（三）合规评估结果是否客观、真实地反映被评估单位的风险状况

（四）其他合规评估工作情况。

第二十条　风管委办公室对合规评估过程和结果如有疑问，合规评估机构、被评估单位及其收单机构需予以解释说明，必要时补充相关书面材料。

第二十一条　经评估未达到合规要求的被评估单位应在 3 个月内完成账户信息安全合规整改，并由其收单机构将整改报告提交风管委办公室。

第二十二条　风管委办公室审核整改报告，决定是否需要进行复评估。对于需要进行复评估的被评估单位，由原合规评估机构进行评估。

第二十三条　对于复评估仍未达到合规要求的单位，风管委办公室将根据《银联卡账户信息与交易数据安全管理规则》中“赔偿与处罚”有关规定进行处理。

对于未达到合规要求的特约商户，其他收单机构和第三方服务机构不得以此作为唯一理由，采取竞争方式将其发展成为本行特约商户。

第二十四条　经收单机构书面同意，银联风管委办公室将在中国银联官方网站公布和更新符合账户信息安全合规评估要求的被评估单位名单。

第四章 例外情况处理

第二十五条　对于外部合规评估合格，达到银联卡账户信息安全管理相关标准的被评估单位，如发生账户信息泄漏事件，经中国银联风险管理委员会认定，可减轻或免除《银联卡账户信息与交易数据安全管理规则》中相关罚款责任。

第二十六条　对于在合规评估工作中不予配合致使未能按时完成合规评估的被评估单位及其收单机构，风管委办公室将视情况建议风险管理委员会进行处理，包括但不限于以下措施：

（一）书面警告；

（二）行业通报；

（三）建议银联董事会终止其受理、处理银联卡交易的业务资格，或接入银联受理网络。

第二十七条　对于合规评估机构未按本规定开展合规评估工作的，收单机构可向风管委办公室提出书面投诉。经确认属实，将根据《银联卡账户信息安全合规评估机构管理暂行办法》进行处理。

第二十八条　对于上一年度外部合规评估符合账户信息安全管理规定的被评估单位，可由收单机构向风管委办公室提出免除本年度外部合规评估的申请，并提交以下材料：

（一）免除外部合规评估的申请函；

（二）上一年度合规评估机构出具的评估报告。

对于符合免除本年度外部合规评估条件的单位，风管委办公室将在 10 个工作日内向其收单机构发送《关于免除外部合规评估申请的批复》（附 5）。该单位应在年内完成账户信息安全问卷自查。

下一年度该单位如达到外部合规评估条件，仍需按照本规定工作流程开展外部合规评估。

第五章 附则

第二十九条　本规定附 1 “需开展外部合规评估的单位划分标准”，由风管委根据银联卡业务发展和评估实施情况每两年进行一次讨论，并根据需要作相应调整。

第三十条　本规定经中国银联风险管理委员会制订、修改、解释。

第三十一条　本规定自中国银联风险管理委员会审议通过后发布之日起实行。

附 1:

需开展外部合规评估的单位划分标准

	每年处理的银联卡跨行交易量
实体特约商户	>=150 万笔
互联网特约商户	>=50 万笔
实体商户第三方收单专业化服务机构	>=5,000 万笔
互联网商户第三方收单专业化服务机构	>=500 万笔

附 2：　　**银联卡账户信息安全合规评估通知书**

（模版）

××××机构：

为提高银联卡收单业务账户信息安全管理水平，根据《银联卡收单业务账户信息安全合规评估管理暂行规定》（银联风管委〔2008〕3 号）（以下简称《合规评估管理规定》），经中国银联风险管理委员会认定，贵机构下属×××商户，（商户代码为××××××××）需开展外部合规评估，特此通知。

请贵机构积极配合本次外部合规评估工作，在收到本通知的 20 个工作日内，协调外部合规评估对象启动以下准备工作，填写《外部合规评估预备工作情况反馈表》报送银联风管委办公室：

（一）指定本次评估工作专项联系人；

（二）制定合规评估工作计划（如需整改）；

（三）启动问卷自查工作；

（四）选择确定合规评估机构。

根据《合规评估管理规定》，外部合规评估工作应在 90 个工作日内完成，请贵机构在××××年××月××日之前，将以下材料提交银联风管委办公室审核：

（一）银联卡账户信息安全合规评估报告；

（二）银联卡账户信息安全整改工作计划；

（三）银联卡账户信息安全合规评估服务意见反馈表。

关于银联卡账户信息安全外部合规评估具体工作要求详见《合规评估管理规定》。工作过程中如有任何意见和建议，请及时与银联风管委办公室联系。

感谢贵机构大力支持！

联系人：　　电　话：

传　真：　　E-mail：

中国银联风险管理委员会办公室

××××年××月××日

附 3-1：

外部合规评估预备工作情况反馈表

（特约商户专用）

被评估单位信息			
单位名称		商户代码	
联系人		联系人电话	
联系人 E-MAIL		传真号码	
单位地址			
提供服务类型（请在对应项目前打“√”）	☐ 普通 POS 特约商户； ☐ MIS 商户； ☐ 互联网商户； ☐ 邮购/电购商户； ☐ 其他，请说明_____		
所属收单机构信息			
机构名称		机构代码	
联系人		联系人电话	
联系人 E-MAIL			
聘请合规评估机构			
合规评估机构名称		“合规评估机构”证书编号	
合规评估工作计划			
时间安排		工作内容	
年 月 日——年 月 日			
年 月 日——年 月 日			
年 月 日——年 月 日			
年 月 日——年 月 日			
被评估单位单位（公章） ××××年××月××日			
所属收单机构（公章） ××××年××月××日			

附 3-2：　　**外部合规评估预备工作情况反馈表**

（第三方收单专业化服务机构专用）

被评估单位信息			
单位名称		机构代码	
联系人		联系人电话	
联系人 E-MAIL		传真号码	
单位地址			
提供服务类型（请在对应项目前打“√”）	☐ 收单处理服务； ☐收单主机托管 ☐收单运维托管； ☐ 渠道接入服务： ☐POS ☐ATM ☐支付网关 ☐其他，请说明_____ ☐ 清算准备服务； ☐ 差错处理服务； ☐ 数据挖掘服务 ☐ 其他，请说明_____		
所属收单机构信息			
机构名称		机构代码	
联系人		联系人电话	
联系人 E-MAIL			
聘请合规评估机构			
合规评估机构名称		“合规评估机构”证书编号	
合规评估工作计划			
时间安排		工作内容	
年　月　日——　年　月　日			
年　月　日——　年　月　日			
		被评估单位（公章） ××××年××月××日	
		所属收单机构（公章） ××××年××月××日	

附 4：

银联卡账户信息安全外部合规评估服务意见反馈表

一、外部合规评估工作基本信息	
1、被评估单位基本信息	
本单位基本信息	**所属收单机构基本信息**[3]
单位名称：	机构名称：
单位代码[4]：	机构代码：
机构性质： □ 特约商户 □ 收单专业化第三方机构 □ 收单机构 □ 其他，请说明_____	
主要联系人：	主要联系人：
联系电话：	联系电话：
联系人 E-MAIL：	联系人 E-MAIL：
2、合规评估机构信息	
本单位基本信息	**合规评估人员基本信息** **（本次合规评估项目主要负责人）**
机构名称：	姓名：
“合规评估机构”证书编号：	“合规评估师”证书编号：
主要联系人：	联系电话：
联系电话：	E-MAIL：
3、外部合规评估基本信息	
评估时间：**年**月**日至****年**月**日**	
评估所在地：_____国家_____省（自治区、直辖市）_____市（县）___	
邮政编码：	
二、外部合规评估服务评价	

[3] 如果被评估单位为收单机构，则“所属收单机构基本信息”栏目可无需填写。

[4] 对于被评估单位是特约商户的，则“单位代码”栏目填入 15 位“商户代码”；是收单机构或第三方机构的，则填入 8 位“机构代码”。

请被评估单位在收单机构的指导下，对合规评估机构服务质量进行评价，如实回答以下问题： 10-9 分表示“完全同意”；8-6 分表示“同意”；5-3 分表示“不同意”；2-0 分表示“完全不同意”	
评 价 项 目	**得分**
1、合规评估机构是否向贵单位详细解释本次评估的目标、时间安排、评估程序以及评估内容等信息？	
2、经双方讨论沟通，合规评估机构是否了解贵单位银行卡交易处理业务基本流程、技术架构、软硬件环境等信息？	
3、合规评估机构是否具备完成本次评估所必需的专业技能、人员配备等资源？	
4、合规评估机构是否熟悉银联卡账户信息安全管理相关工作要求，以及合规评估工作流程？	
5、合规评估机构是否严格按照协议约定的计划开展外部合规评估工作？	
6、评估过程中，合规评估机构是否采取安全控制措施保护贵机构账户信息安全？	
7、合规评估机构是否就合规评估过程中发现的问题，与贵机构进行深入沟通和讨论？	
8、合规评估机构出具的《评估报告》是否真实、客观、公正地反映贵机构账户信息安全管理状况？	
9、合规评估机构是否就贵单位账户信息安全管理提出富有建设性的工作建议，并协助贵单位研究、制订整改方案和工作计划？	
10、合规评估机构是否向贵机构列示项目收费标准及费用明细？	
合计	
对合规评估机构的其他工作建议和意见：	
对银联卡账户信息安全合规评估工作的建议和意见：	
对银联卡账户信息安全管理工作的建议和意见：	
被评估单位（公章） **××××年××月××日**	
所属收单机构（公章） **××××年××月××日**	

附 5：

关于免除外部合规评估申请的批复

（模版）

××机构：

贵机构《关于申请免除银联卡账户信息安全外部合规评估的函》收悉，根据《银联卡账户信息安全合规评估管理暂行规定》，经中国银联风险管理委员会审核认定，批准×××单位（单位代码：××××）免除本年度外部合规评估，特此批复。

请贵机构指导该单位在年内完成银联卡账户信息安全内部合规评估，并接受银联风管委办公室的监督检查。工作过程中如有任何意见和建议，请及时与银联风管委办公室联系。

联系人：

电　话：

传　真：

E-mail:

中国银联风险管理委员会办公室

××××年××月××日

附 6：

术语表

穿行测试

在正常运行条件下，将初始数据输入控制流程，穿越全流程和所有关键环节，把实际运行结果与控制设计要求对比，以发现控制流程缺陷的方法。

弱点扫描

利用漏洞扫描工具，采用模拟攻击的形式对系统组成元素可能存在的安全漏洞进行逐项检查和评估，以尽早发现安全漏洞并进行修补，消除安全隐患。

按照工作模式，漏洞扫描器分为主机漏洞扫描器和网络漏洞扫描器。其中前者基于主机，通过在主机系统本地运行代理程序来检测系统漏洞，例如操作系统扫描器和数据库扫描器。后者基于网络，通过请求/应答方式远程检测目标网络和主机系统的安全漏洞。

渗透性测试

经过授权的，从一个攻击者的角度采用可控制、非破坏性质的方法和手段发现目标服务器和网络设备中存在的弱点来检查和审核一个网络系统的安全性的过程。

银联卡账户信息安全合规评估机构管理办法

（中国银联第二届风险管理委员会第四次会议审议通过，
第三届第四次会议第一次修订，第四届第四次会议第二次修订）

第一章　总 则

第一条 为规范银联卡账户信息安全合规评估机构服务行为，保证合规评估服务质量，维护银联卡业务机构的合法利益，依据银联卡账户信息安全管理相关规定，特制定本办法。

第二条 本办法所称银联卡账户信息安全合规评估机构（以下简称“合规评估机构”），是指由中国银联风险管理委员会（以下简称“银联风管委”）授予合规评估服务资质，能够向银联卡业务机构提供账户信息安全合规评估服务的专业化机构。

第三条 本办法所称银联卡业务机构，包括以下机构：

（一）银联网络内从事银联卡业务的成员机构及合作机构；

（二）向银联卡成员机构提供专业化服务的第三方机构；

（三）银联卡收单特约商户。

第四条 中国银联风险管理委员会负责对合规评估机构资质进行审批，并授权风险管理委员会办公室（以下简称“风管委办公室”）依照本办法对合规评估机构进行日常管理，并定期向银联风管委汇报。

第五条 中国银联、中国银联风管委及其办公室不对合规评估机构与银联卡业务机构之间，因账户信息安全合规评估过程和结果产生的损失负有赔偿责任，但应监督评估机构依照本规定开展合规评估工作，并积极协助成员机构进行风险责任界定及处理。

第六条 本办法适用于正在申请或已获得银联卡账户信息安全合规评估服务资质的机构。

第二章　权利和义务

第七条 银联卡账户信息安全合规评估机构享有以下权利：

（一）获得银联风管委颁布的银联卡账户信息安全管理规定、合规评估流程等制度规范；

（二）获得银联风管委授权，依照银联卡账户信息安全制度规范开展合规评估业务；

（三）与银联卡业务机构协商收取合规评估费用；

（四）享有银联风管委对合规评估机构提供的业务咨询和培训服务；

（五）资质有效期内，可就本机构具备合规评估资质进行宣传推广。

第八条 银联卡账户信息安全合规评估机构应履行以下义务：

（一）遵守银联卡账户信息安全管理规章制度；

（二）履行提交合规评估资质申请时所做的各项承诺；

（三）独立、客观、公正地开展评估工作，并对合规评估报告负责；

（四）合规评估过程中，保护银联卡业务机构账户信息及商业机密信息不被泄露和篡改；

（五）妥善保管合规评估工作的文档资料，对银联卡业务机构账户信息予以严格保密；

（六）接受中国银联风险管理委员会的监督检查。

（七）未按银联卡账户信息安全管理规定及合规评估流程开展评估工作，或对银联卡业务机构账户信息保护不当致使发生泄露或遭篡改，对银联卡业务机构造成损失的，承担赔偿责任。

第三章 资质申请、审批和维持

第九条 申请合规评估服务资质的机构应同时具备以下基本条件：

（一）具备独立法人主体资格，注册资本不得少于1,500万元人民币，且全部为实缴资本；

（二）有固定的办公场所，以及合规评估服务所必需的测试工具、测试设备、模拟环境等软、硬件资源配置；

（三）具有5年（含）以上金融数据安全、网络安全、数据库和应用程序安全等任一方面工作的专业化服务经验，且从事业务不能与银联卡发卡业务或收单业务存在同业竞争关系；

（四）最近1年内已独立完成3个（含）以上与银行卡相关的数据安全，或金融数据安全、网络安全、数据库和应用程序安全相关的安全评估或审计项目；

（五）具备合规评估资质的专业人员占本机构从事信息安全工作人员总数的40%（含）以上，且不得少于5人；

（六）具备符合银联风管委要求的开展合规评估工作的制度规范和业务流程，以及配套的内部控制和人员管理制度规定；

（七）最近5年内在合规评估工作中未发生过账户信息泄露事件或信息泄漏事件。

第十条 从事合规评估工作的专业人员分为合规评估师和高级合规评估师两个等级，应具备以下条件：

（一）基础要求

1、具备信息安全、计算机、软件、通信等相关专业全日制学士或以上学位；

2、是合规评估机构的正式全职员工，并已签订保密协议；

3、无违法犯罪记录或不良信用记录。

（二）合规评估师

1、2年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面的工作经验；

2、至少具备以下任一项有效证书：注册信息系统安全专业人员证书（CISSP）、注册信息系统审计员证书（CISA）、注册信息安全经理人证书（CISM）、国际注册风险与信息系统安全控制认证（CRISC）、Cisco认证网络或安全等专业人员证书（CCNA、CCNP、CCSP、CCDP、CCIE等）、注册信息安全专业人员证书（CISP），或其他经银联风管委认可的网络安全相关证书等；

3、熟悉与银联卡账户信息安全相关的各项业务规则、技术规范、风险管理要求；

4、精通银联卡账户信息安全管理及合规评估各项制度规定；

5、熟悉银联卡账户信息安全合规评估操作流程，熟练运用各项合规评估工具和手段；

6、熟悉账户信息安全常见保密方法及合规评估应急处置措施；

7、了解当前银联卡各类业务参与方主要业务模式的账户信息安全风险隐患，并能提出针对性的风险防范解决方案。

（三）高级合规评估师

1、拥有经银联风管委认证的账户信息安全合规评估师资质；

2、4年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面的工作经验；

3、学历为硕士及以上的，工作年限要求可放宽至3年；

4、至少具备以下任一项有效证书：注册信息系统安全专业人员证书（CISSP）、注册信息系统审计员证书（CISA）、注册信息安全经理人证书（CISM）、国际注册风险与信息系统安全控制认证(CRISC)、Cisco认证网络或安全等专业人员证书（CCNA、CCNP、CCSP、CCDP、CCIE等）、注册信息安全专业人员证书（CISP），或其他经银联风管委认可的网络安全相关证书等；

5、至少全程参与5个以上银行卡行业、金融行业相关的信息安全检测或评估项目的主要工作；

6、具有较丰富的项目管理经验，熟悉检测或评估项目的工作流程和质量管理的方法，具有较强的组织协调和沟通能力；

7、具有综合分析和判断的能力，能够整体把握测评报告结论的客观性和准确性；

8、熟悉和跟踪国内外银行卡行业、支付行业账户信息安全的相关标准的发展。

第十一条 申请合规评估服务资质的机构（以下简称“申请机构”）根据以上要求，填写申请表（详见附 1、附 2）、提交申请材料至风管委办公室进行初审，风管委办公室应在 15 个工作日内完成审核，必要时可对申请机构进行调查。

第十二条 对于通过初审的申请机构，风管委办公室组织其专业人员参加银联卡账户信息安全管理专题培训及考核，并将初审考核结果及申请资料提交银联风险管理委员会进行表决。未通过审核的申请机构可在30个工作日内组织材料再次提出申请。第二次未通过审核的申请机构，需在自批复之日起一年后才能重新提交申请。

第十三条 符合第十条要求的候选合规评估师，由银联风管委办公室组织进行业务培训及考核，包括笔试考核及实务操作考核。通过考核的人员，由银联风管委授予《银联卡账户信息安全合规评估师证书》（以下简称“《合规评估师证书》”），有效期为自证书授予之日起二年。

对于未通过考核的人员，在30个工作日内再次参加考核，第二次考核未通过的人员，需在一年后才能重新提交申请。

合规评估师二年聘期届满，可申请高级合规评估师资质。对于不符合申请条件或者未申请高级合规评估师资质的，需向银联风管委申请例行资质确认，并且应在证书到期之日前30个工作日提出申请，通过资质确认方能换发资质证书，继续提供合规评估工作。

第十四条 符合第十条要求的候选高级合规评估师，需提交相关审核材料，由银联风管委审核通过后授予《银联卡账户信息安全高级合规评估师证书》（以下简称“《高级合规评估师证书》”），有效期为自证书授予之日起二年。高级合规评估师资质评定范围仅限于获得合规评估师资质的人员，未获得合规评估师资质的人员不得直接申请高级合规评估师资质。

高级合规评估师二年聘期届满，需向银联风管委申请例行资质确认，并且应在证书到期之日前30个工作日提出申请，通过资质确认方能换发资质证书，继续提供合规评估工作。

第十五条 符合以下基本要求的合规评估机构人员，可参加由银联风管委办公室组织进行业务培训及笔试考核，通过笔试考核的人员，可获得笔试合格证明，成为见习合规评估师，并参与账户信息安全合规评估辅助工作：

1、具备全日制学士或以上学位；

2、是合规评估机构的正式全职员工，并已签订保密协议；

3、无违法犯罪记录或不良信用记录；

4、具有1年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面的工作经验；

5、熟悉与银联卡账户信息安全相关的各项业务规则、技术规范、风险管理要求；

6、熟悉银联卡账户信息安全管理及合规评估各项制度规定；

7、熟悉银联卡账户信息安全合规评估操作流程。

第十六条　对于通过审核的申请机构，并且获得《合规评估师证书》人数达到本办法第九条第五项要求，银联风管委授予该机构《银联卡账户信息安全合规评估机构资质证书》（以下简称“《合规评估机构资质证书》”），有效期为自证书授予之日起两年。合规评估机构自获得资质证书之日起，每两年应向风管委办公室申请例行资质确认。通过资质确认方能换发资质证书，继续提供合规评估服务。

第十七条　风管委办公室将根据合规评估机构及合规评估专业人员参加培训情况、已评估的客户数量及被评估客户的满意度评价等因素，综合考虑是否给予其例行资质确认。

第十八条　合规评估机构新增人员申请合规评估师资质的，应由合规评估机构按照本办法第十条要求提交申请材料至风管委办公室进行初审。风管委办公室接收完整申请材料后两周内完成初审，初审合格后参加账户信息安全专题培训及考核，通过考核的人员将提交风管委审议，审议通过的授予《合规评估师证书》。

第十九条　合规评估机构新增人员申请高级合规评估师资质的，应由合规评估机构按照本办法第十条要求提交申请材料至风管委办公室进行初审。风管委办公室接收完整申请材料后两周内完成初审，初审合格后将提交风管委审议，审议通过的授予《高级合规评估师证书》。

第二十条　合规评估机构新增人员符合本办法第十五条要求的，可提交申

请材料至风管委办公室进行初审。风管委办公室接收完整申请材料后两周内完成初审，初审合格后参加风管委办公室账户信息安全专题培训及笔试考核，通过笔试考核的人员获得笔试合格证明，成为见习合规评估师，参与账户信息安全合规评估辅助工作。

第二十一条　风管委办公室定期公布并更新具备合规评估服务资质的合规评估机构名单，并向银联风管委定期报告。

第四章　日常管理

第二十二条 合规评估机构应建立开展账户信息安全合规评估的操作流程，对合规评估各个工作环节提出具体要求，明确合规评估专业人员的工作职责。其中，合规评估师、高级合规评估师在合规评估工作中分别具有以下职责：

（一）合规评估师可作为项目负责人全程参与合规评估工作，包括联系被评估单位，制定工作计划，参与现场评估，包括安排及参与现场访谈、文档审查、弱点扫描、穿行测试和渗透测试等，并负责撰写合规评估报告；

（二） 高级合规评估师负责安排合规评估工作计划，指导其他合规评估人员开展工作，对合规评估报告进行审核，并对合规评估报告带来的风险承担责任；

（三）参与合规评估工作的所有合规评估师及高级合规评估师需在合规评估报告签字，并对报告的真实性、有效性、规范性负责；

（四）见习合规评估师可部分参与合规评估工作，包括参与问卷调查、现场评估等工作，但不得作为合规评估项目负责人，不得独立负责撰写合规评估报告，并且不具备合规评估报告的签字权。

第二十三条　合规评估机构应建立账户信息安全合规评估服务质量的跟踪评价机制，根据银联卡业务机构反馈意见，改进合规评估服务质量。

第二十四条　合规评估机构应建立应急处理工作机制，及时控制、处理合规评估过程中可能发生的账户信息安全事件。

第二十五条　合规评估机构应加强对合规评估专业人员的管理，包括但不

限于以下方面：

（一）与合规评估专业人员签署保密协议，或在劳动合同中设置保密条款；

（二）加强对合规评估专业人员的培训，确保合规评估专业员工了解银联卡账户信息安全管理规定、明确工作流程、强化安全责任意识；

（三）督促合规评估专业人员遵守职业道德，不得利用工作便利获取银联卡业务机构账户信息，从事损害银联卡业务机构声誉及利益，或自身谋取不正当利益的活动；

（四）合规评估专业人员离职，或与合规评估机构解除劳动关系时，应及时报备银联风管委办公室。

第二十六条　合规评估机构应公布合规评估服务项目的收费标准，保证收费合理，服务诚信，并接受银联风管委及成员机构的监督。

第二十七条　合规评估机构应确保至少有 2 名具备合规评估师或高级合规评估师资质的专业人员全程参与每次合规评估。评估内容包括但不限于问卷调查、现场访谈、文档审查、弱点扫描、穿行测试和渗透测试等方面。

第二十八条　合规评估机构应对合规评估工作中接触的被评估单位账户信息以及商业机密信息进行保密，未经被评估单位授权，不得向其他机构或个人提供数据。

第二十九条　合规评估机构应对评估全过程工作进行记录，有关案例日志、评估结果、工作文档等资料应保留三年，对于超过保存期限的文档材料应及时删除或销毁，并接受银联风管委办公室的检查。

第三十条　合规评估机构或合规评估人员在评估过程中不得出现以下情形：

（一）合规评估机构与被评估的银联卡业务机构之间存在股权利益关系；

（二）合规评估机构或合规评估专业人员接受被评估的银联卡业务机构提供的可能对评估结果产生影响的资助或服务；

（三）合规评估专业人员在与被评估的银联卡业务机构有利益关系的关联机构中从事相关工作；

（四）向被评估的银联卡业务机构提出与合规评估活动无关的不正当要求。

第三十一条 合规评估机构或合规评估人员如具有或出现本办法第三十条所述情形，或未按本办法规定开展合规评估工作的，银联卡业务机构可向风管委办公室提出书面投诉。

第三十二条 合规评估机构应定期和不定期对照本办法相关要求进行自查，及时整改自查中发现的问题；对于重大风险问题，应及时报告风管委办公室。

第三十三条 银联风管委办公室有权对合规评估机构的日常管理及合规评估工作进行检查。检查方式包括但不限于：

（一）回访。银联风管委办公室向被评估单位了解对合规评估机构专业水平、服务意识等方面的评价及反馈意见；

（二）抽检。银联风管委办公室对合规评估机构已完成的银联卡账户信息安全合规评估项目有关文档进行检查；

（三）随检。银联风管委办公室派员参与账户信息安全合规项目，对合规评估机构合规评估过程进行检查和评价；

（四）互检。银联风管委办公室安排其他合规评估机构对本评估机构账户信息安全合规评估项目进行交叉复查。

第五章 资质失效和强制退出

第三十四条 合规评估机构或合规评估专业人员不得向第三方转让、分配或出售其拥有的合规评估服务资质。

第三十五条 合规评估专业人员如调至其他合规评估机构工作的，其合规评估师证书或高级合规评估师证书继续有效；如发生离职或工作调动单位不是合规评估机构的，则合规评估师证书或高级合规评估师证书自动失效。

第三十六条 合规评估机构主动放弃合规评估服务资质的，应提前 180 天

向银联风管委办公室提交书面申请，经风管委办公室审核批准、向成员机构发布公告后正式生效。

第三十七条　合规评估机构如发生以下任一情形，其合规评估服务资质将自动失效：

（一）合规评估机构破产、倒闭、停业或被其他机构兼并或收购的；

（二）经银联风管委办公室核实，合规评估机构不再具备本办法第九条相关要求的；

第三十八条　见习合规评估师及合规评估师应接受银联风管委办公室举办的各项日常业务培训及考核。对于单次考核未通过的，将受到强化培训、书面警告等处理；合规评估师在资质有效期内未通过考核累计达到 3 次数的，将被取消合规评估资质。

第三十九条　合规评估机构如发生以下任一情形，风管委办公室将视情况给予约谈负责人、书面警告、业内通报等处罚措施：

（一）在同一期业务考核中，本机构考核结果与其他机构存在明显差距的；

（二）经风管委办公室日常检查，确认资质有效期内违规次数累计 2 次（含）以内的；

（三）接受可能对评估结果产生影响的资助或服务；

（四）雇佣不具备合规评估资质的人员开展合规评估活动；

（五）向银联卡业务机构提出与合规评估活动无关的不正当要求。

第四十条　合规评估机构如发生以下任一情形，风管委办公室将责令其暂停合规评估业务并限期整改；情节特别严重的，将强制取消合规评估资质，通过中国银联风险信息共享系统报送违规机构及人员信息，并建议银联风管委对合规评估机构进行处罚：

（一）经风管委办公室日常检查，确认资质有效期内违规次数累计达到3次（含）以上的；

（二）出具虚假评估结论，或出具的评估结论严重失实；

（三）未按照银联卡账户信息安全管理规定，以及合规评估工作流程开展评估工作，导致银联卡业务机构遭受严重经济损失，或品牌声誉遭受严重影响；

（四）因严重违规遭到银联卡业务机构书面投诉，经风管委办公室核查属实的。

第四十一条　合规评估资质自风管委办公室发出书面失效通知之日起正式失效。资质失效后，合规评估机构应在风管委办公室的监督下，根据银联卡账户信息安全管理规定，将相关资料移交给中国银联风险管理委员会办公室保管或销毁。合规评估机构仍须对资质有效期内出具的评估报告负责。

第四十二条　合规评估资质被强制取消的机构，不得再从事银联卡账户信息安全合规评估工作；合规评估资质自动失效的机构，自资质失效之日起一年内不得提交资质申请。合规评估资质失效后，风管委办公室将资质失效相关情况在业内进行通报。

第六章　附 则

第四十三条　本办法经中国银联风险管理委员会制订、修改、解释。

第四十四条　办法自中国银联风险管理委员会审议通过后发布之日起实行。

第四十五条　原《银联卡账户信息安全合规评估机构管理办法（修订）》（银联风管委〔2010〕2 号）自本办法发布之日起废止。

附 1：

银联卡账户信息安全合规评估机构资质申请表

填制机构（公章）：_____ 填制日期：_____年____月____日

一、申请机构基本信息

1、基本信息
申请类型： □ 首次资质申请 □ 例行资质确认申请
注册名称：
注册时间：
注册地址：
营业执照编号：
注册资金：（小写）￥ ，（大写）
从事信息安全工作的人数： 人；其中，具备合规评估师证书的人数： 人，具备高级合规评估师证书的人数： 人
机构总体情况介绍
主营业务介绍（如与银行卡相关的数据安全，或金融数据安全、网络安全、数据库和应用程序安全等）
最近 1 年内安全评估或审计情况介绍（如与银行卡相关的数据安全，金融数据安全、网络安全、数据库和应用程序安全等）
最近 5 年内在合规评估工作中是否发生过账户信息泄漏事件或信息泄漏事件？ □ 是 □ 否

如果是账户信息泄漏事件，请根据《银联卡账户信息与交易数据安全管理规则》，说明事件等级：

☐ 一级事件　　☐ 二级事件　　☐ 三级事件　　☐ 四级事件

如果是重大信息泄漏事件，请说明事件基本情况（包括信息泄漏时间、泄漏规模、涉及损失等）

_____

_____

2、机构联系人信息			
第一联系人			
姓 名		**部 门**	
职 务		**传 真**	
办公电话		**手 机**	
电子邮件		**邮 编**	
通信地址			
第二联系人			
姓 名		**部 门**	
职 务		**传 真**	
办公电话		**手 机**	
电子邮件		**邮 编**	
通信地址			

二、声明及承诺事项

中国银联风险管理委员会：

本机构郑重承诺：本机构提交的材料内容属实。如果提交材料所述内容与真实情况不符，或有任何与法律相抵触的地方，本机构将承担由此产生的一切法律后果及责任。

若本机构的申请获中国银联风险管理委员会核准，本机构承诺成为银联卡账户信息安全

合规评估机构后，按照银联风管委颁布的账户信息安全管理规定（附后），合规评估流程等制度规范开展合规评估工作，履行作为合规评估机构的的各项义务，接受银联风管委及其办公室的监督检查。 本机构对以下工作要求作出承诺： 特此声明。 申请机构名称： 申请机构负责人： 申请机构负责人签名 ××××年×月×日
一、内部控制及管理
1、已建立开展账户信息安全合规评估的操作流程，对合规评估各个工作环节提出具体要求，明确合规评估人员的工作职责；
2、已建立账户信息安全合规评估服务质量的跟踪评价机制；
3、已针对合规评估工作建立账户信息安全应急处理工作机制；
4、已与合规评估专业人员签署保密协议，或在劳动合同中设置保密条款；
5、定期组织合规评估专业人员进行账户信息安全评估、系统安全审计等专业培训；
二、合规评估资质管理
1、确保及时掌握、熟悉银联风管委最新发布的银联卡账户信息安全管理制度规范；
2、未经银联风管委、中国银联或成员机构书面授权同意，不擅自使用上述单位的注册商标；
3、在向银联卡业务机构推介本单位自行开发、设计的产品或服务功能时，不向客户声明或暗示这些产品已得到银联风管委的认可或授权；
4、不擅自向其他机构转让、分配或出售合规评估服务资质；
5、资质失效后，及时销毁本机构保存的银联卡账户信息安全制度规范，以及银联卡业务机构的相关资料；
6、资质失效后，对资质有效期内出具的评估报告负责。

三、账户信息安全合规评估
1、确保至少配备 2 名具有合规评估资质的专业人员全程参与每次合规评估；
2、评估内容至少包括问卷调查、现场访谈、文档审查、弱点扫描、穿行测试、渗透测试等方面；
3、对合规评估全过程工作进行记录，相关工作文档至少保留三年；
4、合规评估报告能客观、公正地反映银联卡业务机构风险状况；
5、采取安全控制措施，防范银联卡业务机构账户信息遭到泄漏和篡改；
6、如未按银联卡账户信息安全管理规定，以及合规评估流程开展评估工作，对银联卡业务机构造成损失的，承担赔偿责任。

银联卡账户信息安全管理制度规范：

1、《银联卡账户信息与交易数据安全管理规则》（银联风管委[2004]8 号）

2、《银联卡账户信息与交易数据安全管理指南》（银联风管委[2004]9 号）

3、建立“银联卡账户信息泄漏责任及罚则”，并纳入《银联卡账户信息与交易数据安全管理规则》第九章“赔偿及处罚”（银联风管委[2006]6 号）

4、《银联卡账户信息安全事件调查及处理操作流程》（银联风管委[2007]8 号）

5、《银联卡账户信息安全事件应急预案》（银联风管委[2007]7 号）

6、《银联卡收单机构账户信息安全管理标准》（银联风管委[2013]9 号）

7、《银联卡收单业务账户信息安全合规评估管理暂行规定》（银联风管委[2008]3 号）

8、《银联卡收单业务账户信息安全合规评估工作试行办法》（银联风管委[2008]3 号）

9、《银联卡账户信息安全合规评估机构管理办法（修订）》（银联风管委[2013]5 号）

10、《银联卡账户信息安全合规评估机构工作指引》（银联风管委[2010]3 号）

11、《银联卡账户信息泄漏点损失补偿流程》（银联风管委[2013]10 号）

银联卡账户信息安全管理制度规范经中国银联风险管理委员会制订、修改、解释，并予以更新、发布。

附 2：

银联卡账户信息安全合规评估师/高级合规评估师资质申请表

申请类型	☐ **首次资质申请** ☐ **例行资质确认申请**		
申请人姓名（中文）		**拼音或英文姓名**	
证件类型		**证件编号**	
学 历		**学 位**	
工作单位及部门		**职 务**	
办公电话		**手 机**	
电子邮件			
累计工作年限		**现单位工作年限**	
具备的职业证书	☐ 注册信息系统安全专业人员证书（CISSP） ☐ 注册信息系统审计员证书（CISA） ☐ 注册信息安全经理人证书（CISM） ☐ 国际注册风险与信息系统安全控制认证(CRISC) ☐ Cisco 认证网络或安全等专业人员证书(CCNA、CCNP、CCSP、CCDP、CCIE 等） ☐ 注册信息安全专业人员证书（CISP） ☐ 其他证书，请说明_____		
申请人承诺	以上填写内容完全属实，并同意中国银联风险管理委员会及办公室对申请资料真实性进行核实。 若本人申请获中国银联风险管理委员会核准，本人承诺成为银联卡账户信息安全合规评估师/高级合规评估师后，按照银联风管委颁布的账户信息安全管理规定（附后），合规评估流程等制度规范开展合规评估工作，遵守合规评估工作要求，接受银联风管委及其办公室的监督检查。		

<table>
<tr><td></td><td colspan="2">申请人签名：
××××年×月×日</td></tr>
<tr><td rowspan="2">申请人工作单位
意　见</td><td>申请人资料是否属实</td><td>□ 是　　□ 否</td></tr>
<tr><td colspan="2">机构（公章）
××××年×月×日</td></tr>
</table>

银联卡账户信息安全管理制度规范：

1、《银联卡账户信息与交易数据安全管理规则》（银联风管委[2004]8 号）

2、《银联卡账户信息与交易数据安全管理指南》（银联风管委[2004]9 号）

3、建立“银联卡账户信息泄漏责任及罚则”，并纳入《银联卡账户信息与交易数据安全管理规则》第九章“赔偿及处罚”（银联风管委[2006]6 号）

4、《银联卡账户信息安全事件调查及处理操作流程》（银联风管委[2007]8 号）

5、《银联卡账户信息安全事件应急预案》（银联风管委[2007]7 号）

6、《银联卡收单机构账户信息安全管理标准》（银联风管委[2013]9 号）

7、《银联卡收单业务账户信息安全合规评估管理暂行规定》（银联风管委[2008]3 号）

8、《银联卡收单业务账户信息安全合规评估工作试行办法》（银联风管委[2008]3 号）

9、《银联卡账户信息安全合规评估机构管理办法（修订）》（银联风管委[2013]5 号）

10、《银联卡账户信息安全合规评估机构工作指引》（银联风管委[2010]3 号）

11、《银联卡账户信息泄漏点损失补偿流程》（银联风管委[2013]10 号）

银联卡账户信息安全管理制度规范经中国银联风险管理委员会制订、修改、解释，并予以更新、发布。

附 3：

合规评估机构及评估人员申请材料清单

一、合规评估机构申请材料清单

（一）首次申请

1、银联卡账户信息安全合规评估机构资质申请表；

2、营业执照原件及复印件一份；

3、具备固定办公场所的证明材料（如房屋租约或物业所有权证等）；

4、已具备合规评估服务所必需的测试工具、测试设备、模拟环境等软、硬件资源配置的相关证明材料（如相关工具设备的功能描述、软硬件设施配置的情况说明等）；

5、具有 5 年（含）以上银行卡相关的数据安全，或金融数据安全、网络安全、数据库和应用程序安全等任一方面工作专业化服务经验的证明材料，应包括但不限于：

（1）公司核心业务或主营业务介绍；

（2）在银行卡相关的数据安全，或金融数据安全、网络安全、数据库和应用程序安全评估方面的业务开展情况和经验介绍等；

（3）已服务过的主要客户数量、名单及相关评估项目名称一览表。

6、最近 1 年内独立完成至少 3 个与银行卡相关的数据安全，或金融数据安全、网络安全、数据库和应用程序安全相关的安全评估或审计项目的证明材料（如评估或审计合同、评估审计报告、评估结果证明等）；

7、具备合规评估资质的专业人员数量达到相关要求的证明材料；

8、开展合规评估工作的工作流程、应急预案、服务质量跟踪评价等制度规范；

9、机构内部组织架构、人员管理、风险内控等内部管理制度规范；

10、合规评估专业人员保密协议模版；

11、支持的工作语言列表；

12、其他证明材料。

（二）例行资质确认申请

1、银联卡账户信息安全合规评估机构资质申请表；

2、已获得合规评估机构资质的证书复印件；

3、最近两年内开展银联卡账户信息合规评估的服务评价表；

4、最近两年内参加银联风管委或相关信息安全评估培训的证明；

5、具备合规评估资质的专业人员数量达到相关要求的证明材料；

6、其他证明材料。

二、合规评估师申请材料清单

（一）首次申请

1、银联卡账户信息安全合规评估师资质申请表；

2、个人简历；

3、毕业证和学位证书原件和复印件一份；

4、与合规评估机构雇佣关系的证明材料；

5、具备 2 年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面工作经验的证明材料；

6、注册信息系统安全专业人员证书（CISSP）、注册信息系统审计员证书（CISA）、注册信息安全经理人证书（CISM）、国际注册风险与信息系统安全控制认证(CRISC)、Cisco 认证网络或安全等专业人员证书（CCNA、CCNP、CCSP、CCDP、CCIE 等）、注册信息安全专业人员证书（CISP）等证书原件和复印件一份；

7、无犯罪记录或不良信用记录；

8、其他证明材料。

（二）例行资质确认申请

1、银联卡账户信息安全合规评估师资质申请表；

2、已获得合规评估师资质的证书复印件；

3、个人简历；

4、与合规评估机构雇佣关系的证明材料；

5、最近两年内参加银联风管委或相关信息安全评估培训的证明；

6、无犯罪记录或不良信用记录；

7、其他证明材料。

三、高级合规评估师申请材料清单

（一）首次申请

1、银联卡账户信息安全高级合规评估师资质申请表；

2、已获得合规评估师资质的证书复印件；

3、个人简历；

4、毕业证和学位证书原件和复印件一份；

5、与合规评估机构雇佣关系的证明材料；

6、具备 4 年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面工作经验的证明材料（学历为硕士及以上的，工作年限要求可放宽至 3 年）；

7、注册信息系统安全专业人员证书（CISSP）、注册信息系统审计员证书（CISA）、注册信息安全经理人证书（CISM）、国际注册风险与信息系统安全控制认证(CRISC)、Cisco 认证互联网专家证书（CCIE）等证书原件和复印件一份；

8、无犯罪记录或不良信用记录；

9、其他证明材料。

（二）例行资质确认申请

1、银联卡账户信息安全高级合规评估师资质申请表；

2、已获得高级合规评估师资质的证书复印件；

3、个人简历；

4、与合规评估机构雇佣关系的证明材料；

5、最近两年内参加银联风管委或相关信息安全评估培训的证明；

6、无犯罪记录或不良信用记录；

7、其他证明材料。

四、见习合规评估师参与培训及笔试考核需提交材料清单

1、个人简历；

2、毕业证和学位证书原件和复印件一份；

3、与合规评估机构雇佣关系的证明材料；

4、具备 1 年以上从事与银行卡相关的数据安全，或金融数据安全、网络安全、数据库或应用程序安全等任一方面工作经验的证明材料。

银联卡账户信息安全合规评估机构工作指引

（银联风管委〔2010〕3 号）

第一章　总则

第一条 为保障银联卡账户信息安全合规评估质量，规范银联卡账户信息安全合规评估机构服务行为，落实《银联卡账户信息安全合规评估机构管理暂行办法》相关规定，特制定本指引。

第二条 本指引所称银联卡账户信息安全合规评估机构（以下简称“合规评估机构”），是指由中国银联风险管理委员会（以下简称“银联风管委”）授予合规评估服务资质，能够向银联卡业务机构提供账户信息安全合规评估服务的专业化机构。

银联卡账户信息安全合规评估师（以下简称“合规评估师”），是指由中国银联风险管理委员会授予合规评估服务资质，能够向银联卡业务机构提供账户信息安全合规评估服务的专业人员。

第三条 银联卡账户信息安全合规评估机构应遵循独立、客观、公正原则开展银联卡账户信息安全合规评估，协助银联卡业务机构提升账户信息安全管理水平。

第四条 本指引适用于已获得银联卡账户信息安全合规评估服务资质的机构及专业人员。

第二章　合规评估营销管理

第五条 合规评估机构应定期组织本单位从事账户信息安全合规评估营销活动的有关人员开展业务培训，确保营销人员具备并保持以下业务能力：

（一）了解银行卡基本概念、业务原理、主要业务流程等基础知识；

（二）熟悉银联卡账户信息安全管理及合规评估制度基本规定；

（三）熟悉银联卡收单机构账户信息安全管理标准（ADSS）基本要求；

（四） 熟悉银联卡账户信息安全合规评估操作必备流程、常规评估工具和手段。

第六条 合规评估机构应维护银联卡品牌声誉及合法权益，在营销银联卡账户信息安全服务过程中，不得出现以下违规行为：

（一）宣传与银联卡具有竞争关系的其他银行卡品牌相关安全标准及评估服务；

（二）捆绑销售除中国银联各专家委员会授权评估服务以外的，与银联卡账户信息安全合规评估无关的检测、评估或认证服务；

（三）捆绑销售与银联卡账户信息安全合规评估无关的软、硬件安全设备、产品或产品组件；

（四）利用已获得的银联卡账户信息安全合规评估资质，营销推广与本资质授权内容无关的其他服务。

第七条 合规评估机构之间应倡导公平竞争，不得采取不正当手段扰乱账户信息安全合规评估正常秩序。不正当竞争手段包括但不限于：

（一）声明或暗示与本机构基本资质、服务范围、从业经验等情况不符的信息；

（二）声明或暗示本机构在银联卡账户信息安全合规评估资质方面拥有其他合规评估机构不具备的排他性优势；

（三）声明或暗示本机构成为国家行业主管部门，或银联风管委唯一指定、认可或推荐的账户信息安全合规评估专业机构；

（四）采用财物或者其他手段贿赂被评估单位有关人员；

（五）捏造、散布虚假事实，损害其他合规评估机构商业信誉；

（六）其他影响账户信息安全合规评估公平竞争的行为或手段。

第八条 合规评估机构应建立银联卡账户信息安全合规评估服务价格形成机制及最高报价标准，并保持价格形成机制及最高报价标准的稳定性，不得随意修改或调整。

合规评估机构应在取得银联卡账户信息安全合规评估资质的 60 个工作日内将账户信息安全合规评估价格形成机制及最高报价标准报备银联风管委。如因业务需要进行调整的，应及时就调整内容向银联风管委提交书面说明。

第九条 合规评估机构向被评估单位提交银联卡账户信息安全合规评估服务报价，应遵守以下要求：

（一）服务报价不得高于本单位向银联风管委报备的最高报价标准；

（二）不得违背被评估单位意愿附加不合理条件；

（三）不得通过缩小合规评估范围、简化评估流程、缩短评估必要周期、降低评估质量等方式，取得合规评估服务价格优势。

第十条 合规评估机构应指派至少 1 名合规评估师协助被评估单位编写合规评估方案、明确合规评估范围、制定合规评估计划等工作。

第十一条 合规评估机构与被评估单位签订的账户信息安全合规评估书面协议以及附件中，应明确合规评估内容、实施计划、评估师人员安排等必备信息。

第三章 合规评估质量管理

第十二条 合规评估机构应定期组织本单位银联卡账户信息安全合规评估师业务培训，确保合规评估师具备并保持以下业务能力：

（一）熟悉与银联卡账户信息安全相关的各项业务规则、技术规范、风险管理要求；

（二）精通银联卡账户信息安全管理及合规评估各项制度规定；

（三）深刻领会银联卡收单机构账户信息安全管理标准（ADSS）各项要求及管理重点；

（四）熟悉银联卡账户信息安全合规评估操作流程，熟练运用各项合规评估工具和手段；

（五）熟悉账户信息安全常见保密方法及合规评估应急处置措施；

（六）了解当前银联卡各类业务参与方主要业务模式的账户信息安全风险隐患，并能提出针对性的风险防范解决方案。

第十三条 评估过程中，对于被评估单位有关应用服务器、网络设备、交易终端，或网络符合相似原则的，可实行抽样评估；不符合相似原则的，应进行逐一评估。

第十四条 对于采取抽样方式开展合规评估的，合规评估机构应在签订银联卡账户信息安全合规评估书面协议之前，协助被评估单位对抽样评估适用条件及范围进行确认，并共同制定账户信息安全合规评估方案。需确认内容包括但不限于以下方面：

（一）被评估单位应纳入银联卡账户信息安全合规评估范围的各类应用服

务器、网络设备、以及交易终端的情况；

（二）被评估单位符合抽样评估条件的有关应用服务器、网络设备，以及交易终端的情况。

第十五条 合规评估机构可就银联卡账户信息安全合规评估适用范围、抽样评估界定标准等事宜向银联风管委办公室进行咨询，并应以银联风管委最终解释为准执行。

第十六条 合规评估机构应协助被评估单位在收到账户信息安全合规评估通知的 90 个工作日内完成评估工作，并落实以下要求：

（一）问卷自查环节。协助被评估单位如实填写《银联卡账户信息安全管理调查问卷》、《银联卡账户信息安全检查点列表》；

（二）制度审查环节。对被评估单位账户信息安全管理规定、操作流程、权限管理、应急预案、合规审计等制度规定的完备性和合理性进行审查；

（三）人员访谈环节。向被评估单位业务、技术、风险管理相关人员了解账户信息安全管理现状，检查账户信息安全管理要求执行情况；

（四）现场检查环节。应运用弱点扫描、渗透测试、穿行测试、手工检查等必要手段，实地验证被评估单位账户信息安全管理规定执行情况；

（五）出具风险点清单环节。应在完成现场检查的 5 个工作日内，出具《银联卡账户信息安全合规评估风险点清单》（以下简称《风险点清单》），识别被评估单位账户信息安全管理风险隐患，并提出改进建议；

（六）协助整改环节。自出具《风险点清单》之日起，应至少预留 30 个工作日协助被评估单位实施账户信息安全整改，并对整改情况进行确认核实；

（七）出具报告环节。根据被评估单位账户信息安全整改实际情况，出具《银联卡账户信息安全合规评估报告》。

第十七条 合规评估机构应指派至少 2 名合规评估师全程负责问卷自查、制度审查、人员访谈、现场检查、出具风险点清单、协助整改、出具报告等必备环节的评估工作。

其中，对于人员访谈、现场检查环节，2 名合规评估师必须同时在场进行评估。

第十八条 合规评估机构应根据被评估单位对《风险点清单》中有关风险问

题的整改情况，出具《银联卡账户信息安全合规评估报告》，并落实以下要求：

（一）对于《风险点清单》中列示的风险问题，如被评估单位已完成整改并确认达标的，合规评估机构应在《合规评估报告》中对上述风险问题的整改情况进行说明。

（二）对于《风险点清单》中列示的风险问题，如被评估单位未完成整改，合规评估机构应在《合规评估报告》中对未完成整改的有关问题进行说明，并协助被评估单位制定整改计划。

（三）合规评估机构应对《合规评估报告》负责，加盖公章并由负责本项目的 2 名评估师签字确认。

第十九条 合规评估机构应设计《银联卡账户信息安全合规评估证书》，并在取得银联卡账户信息安全合规评估资质的 30 个工作日内向银联风管委办公室报备证书设计方案及中英文对照的证书模版。证书基本要素包括但不限于：

（一）被评估单位基本信息，包括：被评估单位名称、代码、单位类型等；

（二）证书资质信息，包括：评估依据、评估完成时间、评估结论、资质效力有效期，证书编号，证书发放日期，有关声明等；

（三）合规评估机构基本信息，包括：合规评估机构名称、代码及公章，合规评估师姓名、代码及签名等。

第二十条 对于通过账户信息安全合规评估，达到 ADSS 标准要求的被评估单位，合规评估机构应向其颁发《银联卡账户信息安全合规评估证书》，并对证书效力负责。

合规评估机构在发放证书之前，应向银联风管委办公室申请证书编号，并报备证书副本。

第二十一条 合规评估机构应建立账户信息安全合规评估文档管理机制，妥善保管合规评估有关文档及过程记录。需保存的文档包括但不限于：

（一）银联卡账户信息安全合规评估合同及保密协议；

（二）银联卡账户信息安全合规评估报告；

（三）银联卡账户信息安全合规评估风险点清单；

（四）银联卡账户信息安全管理调查问卷；

（五）银联卡账户信息安全检查点列表；

（六）制度文审、人员访谈、现场检查等环节使用的过程文档、原始工作底稿等记录文件；

（七）评估过程中向被评估单位获取的各项文档、记录等辅助资料。

第四章　附　　则

第二十二条　本指引经中国银联风险管理委员会制订、修改、解释。

第二十三条　本指引自中国银联风险管理委员会审议通过后发布之日起实行。

银联卡密钥安全管理规则【磁条卡部分】V1.0

（银联风管委〔2004〕2 号）

第一章　总　则

1. 目的

提升磁条卡跨行交易的安全性和管理水平，确保持卡人个人标识代码（PIN）与敏感信息在跨行交易过程中的安全传输与转接，维护通过跨行网络开展银行卡交易的银联卡网络参与方的整体利益。

2. 适用范围

《银联卡密钥安全管理规则》（以下简称《密钥规则》）适用于通过跨行网络进行银行卡交易的中国银联、成员机构、所有受理银联卡的联网机构及其他关联机构（本规则统一简称为银联卡网络参与方）。

本着循序渐进的原则，在现阶段《密钥规则》提出基于传统交易终端（如 ATM、POS）发起的跨行磁条卡敏感交易信息加解密的基本规定，主要适用于对称算法的密钥管理。

本规则分章节叙述密钥生命周期各环节应达到的基本要求，对银联卡网络内的终端机具、硬件加密设备的安全管理做出基本规定；对人员管理及制度监督提出原则意见；附录列出安全管理工作表格的基本要素。

本规则与 VISA、MASTERCARD 等境外信用卡公司的相关规定基本一致。境外卡在银联卡网络的交易同样适用于本规则；银联卡在境外使用时参照本规则执行。

3. 遵循标准

在实际应用当中，密钥按照体系和使用范围划分为不同类别，每个类别具有相应的功能与特点，遵循不同的标准与要求。《密钥规则》规定：在有国内标准的情况下应首先遵循国内标准，如国内标准尚未明确，一般应遵循 ISO 颁布的相关国际标准。

4. 与现有规范的关系

现有规范是指由国家主管部门及中国银联制定颁布的，在金融机构范围内

实行，涉及银行卡信息交换密钥安全的有关规范，主要包括：

《银行卡联网联合技术规范》V1.0　2001（简称 1.0 版《技术规范》）第三部分“公共接口说明”的第八章“数据传输安全说明”。

《银行卡联网联合安全规范》（简称《安全规范》）第五部分“联网联合安全技术应用”。

《银行卡联网联合技术规范》V2.0　2004（简称 2.0 版《技术规范》）第四部分“数据安全传输控制规范”。

上述规范主要从技术实现的角度阐述了信息交换系统中密钥正确和安全使用的相关规定。本规则重点从管理角度出发规定密钥生命周期各环节的操作规则，与现有规范互相补充、配套。

5.生效说明

本规则适用于当前及今后一段时期内的安全管理，其内容随着业务发展变化的具体情况做相应调整和修订。

鉴于目前不同银联卡网络参与方的制度要求与操作方法存在一定差别，为全面实现本规则的要求，现确定实施过渡期（具体期限另行确定）。过渡期间，各银联卡网络参与方应对照要求整章建制，更新相关设备和系统，落实人员，规范操作。过渡期末应达到本规则的基本要求：

- 涉及密码的交易必须采用硬件加密。硬件加密设备的要求必须符合本规则第三章的相关规定；
- 凡有条件的银联卡网络参与方必须使用 128bit 或 128bit 以上的密钥；
- 涉及密钥生命周期的各项操作均应执行双重控制、信息拆分、严密交接、妥善保管、及时更新的基本要求，建立并履行权限划分、严格审批、详细记录、实名操作的规章制度；
- 建立并严格执行自查与监督机制，实施业务准入评估与违规处罚。

6.与本规则配套的相关文档

中国银联同步制定了《银联卡密钥安全管理指南》和《中国银联密钥安全管理暂行办法》。前者详细阐述各类密钥及其组件生命周期安全管理的推荐做法。后者主要适用于中国银联银行卡信息交换总中心和各分公司，银联商务总

公司及其分支机构、银联卡网络参与方应比照这一办法制定相应的实施细则。

第二章 个人标识代码（PIN）与密钥管理的基本规定

本章概要叙述实际应用当中的密钥体系，按照使用范围划分为不同类别，每个类别都具有相应的功能与特点，须遵循不同的标准与要求。

1.银联卡个人标识代码（PIN）加解密基本规定

1.1 发卡机构发行带个人标识代码（PIN）的银联卡必须遵循如下规定：

- 校验密码的真实性；
- 个人标识代码（PIN）未经加密而传输的交易必须拒绝。

1.2 联机受理凭个人标识代码（PIN）使用的银联卡跨行交易应遵守如下基本要求：

- 必须在专用的个人标识代码（PIN）输入设备中输密；
- 个人标识代码（PIN）加解密必须在专用的硬件加密设备中进行；
- 在包括受理方、转接方在内的整个传输过程和主机设备中必须对个人标识代码（PIN）加密；
- 加解密必须使用对称算法；
- 对 MAC 的要求视应用按照相关规范而定。

2.密钥体系

银联卡网络的密钥根据实际使用情况划分成三层，三层密钥体系根据密钥的使用对象而形成，上层对下层提供保护和一定的维护功能，不同层的密钥不许相同，不能相互共享。

同一密钥只能用于其生成时所定义的目的，不能用于其他用途；

不同的银联卡网络参与方、不同的地区、不同的终端设备不得使用相同的密钥，必须确保密钥的唯一性。

2.1 第一层密钥（MK）

加密机主密钥，即本地主密钥，是最重要的密钥，用于加、解密本地存放的其他密钥数据。MK 长度规定为 128bit 或以上，在硬件加密机以外的地方保管时必须采取严格的安全保管措施。MK 一般不更换。

2.2 第二层密钥（MMK）

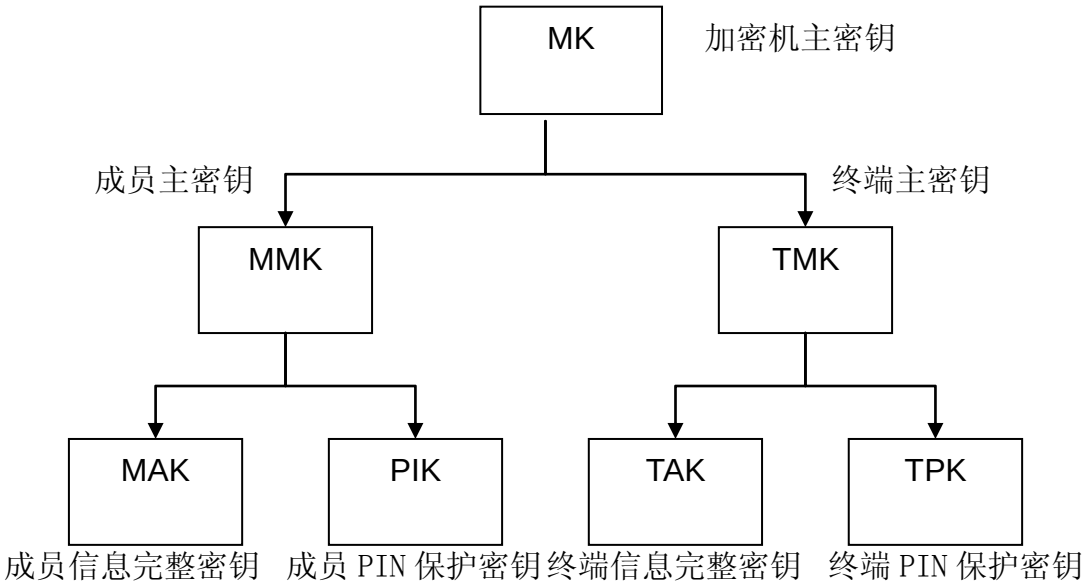
加密机主密钥的下一层为成员主密钥（MMK）[或终端主密钥（TMK）]，作用是加、解密需传递的工作密钥，实现工作密钥的联机实时传输或其他形式的异地传输。成员主密钥在硬件加密机以外的系统中存放和使用时，处于本地 MK 的保护之下。两组不同的银联卡网络参与方之间不得使用相同的成员主密钥。一般情况下，MMK 最长 2－3 年更换一次。

2.3 第三层密钥（PIK、MAK、TPK、TMK）

工作密钥为最底层的密钥，包括银联卡网络参与方之间使用的成员信息完整性密钥（MAK）和成员 PIN 保护密钥（PIK）、终端到银联卡网络参与方之间使用的终端信息完整性密钥（TAK）和终端 PIN 保护密钥（TPK）等，用于加密各种数据，保证数据的保密性、完整性、真实性。第三层密钥一般称为工作密钥（也称数据密钥），是使用最频繁的密钥，在本地存放时，受相应的 MK、成员主密钥或终端主密钥的保护。在银联卡网络参与方之间进行传输时受成员主密钥的保护，在终端与银联卡网络参与方主机之间传输时受终端主密钥的保护。工作密钥采用定期（原则上每天更换一次），或人工触发方式，或按每隔一定交易笔数申请更换。

三层密钥体系结构如下图所示：

密钥体系结构图



2.4 各类密钥的基本要求

各类密钥及其组件的基本要求如下表所示。

通用三级密钥结构表

	缩写	密钥组件段数	长度	存储方式	备份方式	更新频率
加密机主密钥	MK	3 段	128bit 或以上	HSM 内部或外部明文组件存储	IC 卡保存或纸质	一般不更新
成员主密钥 终端主密钥	MMK/TMK	2 段	128bit 或以上	明文 HSM 存储，外部密文存储	主机密文或外部密文存储	一定的更换周期，更新频率低
工作密钥	PIK/MAK TPK/TAK	与应用相关	128bit 或以上	外部密文存储	外部密文存储	定期更新，更新频率高

其中，凡有条件的银联卡网络参与方必须使用 128bit 或以上的密钥；条件不具备的银联卡网络参与方应在过渡期末更新过渡到 128bit 或以上。

第三章　密钥生命周期安全管理

本章详细规定密钥的生成、注入和启用、传输、保管、泄漏与重置、删除与销毁等生命周期各环节应遵循的基本规定。

1.密钥的生成

1.1 基本要求

1.1.1 生成原则

各类密钥及其组件必须遵循随机或伪随机生成的原则。密钥生成工具中随机数的产生必须遵循国家或国际标准中规定使用的算法。

1.1.2 生成方式及使用工具

- 应使用硬件加密机生成各种密钥。各种密钥生成工具，必须通过国家主管部门的认证。

- 使用其他符合本规则规定，经必须程序认定安全的生成工具生成。
- 在无条件使用工具，只能用人工方式生成密钥时，应规定人工生成密钥的具体步骤及辅助工具的使用方式。人工生成允许采用丢硬币、摸彩球、掷骰子等方法；不允许采用随便用想象的方式或使用计算机语言中固有随机函数产生。

1.1.3 生成记录

各类密钥生成过程必须履行严格的操作审批手续，详细记录，相关人员签名确认，文档资料必须妥善保管（相关工作表格要素详见附录），保存期限应不低于记录对象的生命周期，确保各类密钥生成的安全性与规范性。

1.2 各类密钥的生成

1.2.1 加密机主密钥（MK）

加密机主密钥必须由三个组件组成，每个组件的长度为 128bit 或以上。

1.2.1.1 使用硬件加密机生成

由加密机主密钥的三名生成人员在接受监督的情况下，通过硬件加密机分别独立生成三段主密钥组件，分别记录（或写入 IC 卡、或打印密封信封）后密封入三个信封，生成、监督人员分别加盖名章（或骑缝签名），由组件生成人员分别保存到各自的保险箱内，负责该密钥组件的注入和保管。

1.2.1.2 人工生成

三个加密机主密钥生成人员在接受监督的情况下，按照指定的人工生成方法各自生成一段密钥组件，分别记录（或写入 IC 卡、或打印密封信封）后密封入三个信封，生成和监督人员分别加盖名章（或骑缝签名），由组件生成人员分别保存到各自的保险箱内，负责该密钥段的注入和保管。

1.2.1.3 采用其他工具生成

按照本规则规定，根据生成工具的具体使用方法生成。

1.2.2 成员主密钥（MMK）

成员主密钥一般由两段密钥组件组成，可由对应银联卡网络参与方各自生成其中一段密钥组件，并以安全方式传递合成；也可由银联生成全部两段密钥组件后生成。

成员主密钥在双方注入并投产试运行成功后，明文组件应及时销毁。

终端主密钥的生成比照上述要求执行。

1.2.3 工作密钥（PIK、MAK、TPK、TAK）

工作密钥一律采用联机方式由硬件加密机生成。

密钥生成后在硬件加密机中用相应的成员主密钥加密后送到主机，再通过相应的联机报文发送到有关银联卡网络参与方及终端设备。

加密后的工作密钥，可存放在主机上供系统使用，存放在主机上的工作密钥必须用加密机主密钥或成员主密钥加密保护；也可存放在终端上使用，存放在终端上的工作密钥必须用终端主密钥（TMK）加密保护。

2.密钥的传输

2.1 基本要求

密钥明文传输应采用信息拆分、分人分段负责的方法。传输时须分为两个及以上组件，并使用多种渠道不在同一天运输。

密钥可采用以组件的硬拷贝、内含密钥组件的安全芯片等方式传输；不得以内含完整密钥明文的硬拷贝或内含完整密钥的芯片方式传输。

各类密钥传输交接过程必须履行严格的操作审批手续，详细记录，相关人员签名确认，文档资料必须妥善保管（相关工作表格要素详见附录），保存期限应不低于记录对象的生命周期，确保各类密钥传输的安全性与规范性。

2.2 传输过程

2.2.1 同城传输

向同城银联卡网络参与方分发密钥时，每一段密钥组件接收机构必须分派专人领取，不得由一人领取多段密钥；不同领取人员不得乘坐同一交通工具。

2.2.2 异地邮寄

应使用机要方式或邮政系统的特快专递邮寄，每一段密钥组件必须单独邮寄，分别在不同日期寄出。

2.2.3 工作密钥的传输

成员机构间的工作密钥必须经对应的成员主密钥加密传输与转接，行内联机方式可采用或比照《银行卡联网联合技术规范》中有关密钥切换的报文进行。

2.2.4 禁止方式

密钥明文及其组件不得采用电子邮件（E-mail）、传真、电传、电话、短

信等方式直接传递。

2.3 接收要求

接收时接收机构的接收、保管、监督等相关人员在场，审核密封信封的完整性和安全性，当场签名盖章，由接收人员或交给保管员存入安全容器内保管，存入过程应记录相应文档。

3.密钥的注入和启用

3.1 基本要求

密钥组件必须采用双重控制和信息拆分的原则注入。注入数据不得被无关人员以任何方式非法或无意获得，不得被人为窥视、摄像头监控以及网络截取等方式获取。

各类密钥注入过程必须履行严格的操作审批手续，详细记录，相关人员签名确认，文档资料必须妥善保管（相关工作表格要素详见附录），保存期限应不低于记录对象的生命周期，确保各类密钥注入的安全性与规范性。

3.2 加密机主密钥的注入与启用

3.2.1 密钥启用前的审核

审核密钥组件信封是否有破损或被干预迹象，密封章是否完整。

3.2.2 密钥注入过程

注入密钥组件时，由注入人员分别在现场单独操作，其他人员必须退出到看不到密钥存储设备操作面板的地方。注入完毕后，操作面板上不得留下任何密钥内容。

3.2.3 密钥注入后的工作

原已开封的密钥保管信封需重新封装，并加盖密封章和密钥监督人员的名章，交由原来的保管员保管并做相应文档记录。保管方法须遵守本章 4.要求。

3.3 成员主密钥的注入与启用

成员主密钥的注入要求与加密机主密钥的注入过程基本一致。

注入完成并投产试运行成功后，凡记录在纸质上的密钥明文必须销毁，销毁方法须遵守本章 5.要求。原密钥必须至少保留两个副本，副本保存可采用主机密文文件或机外密文文件的方式。

3.4 工作密钥的启用

比照本规则 1.2.3 的相关规定进行。

4. 密钥的保管

4.1 基本要求

- 每一段密钥组件必须独立存储。
- 密钥存储介质要求用信封密封，加盖密封章（或骑缝签名）后置入保险容器妥善保管；只有指定的密钥组件的生成人员或注入人员才有权打开容器启用该组件。
- 保管地点应在安全区域内的保险容器中。
- 保管人员调离时，应按照规定办理交接手续。

4.2 各类密钥组件的保管

4.2.1 加密机主密钥组件

存储加密机主密钥各段组件的密封信封应在监督下，加盖名章（或骑缝签名）后存入保险容器，且只能由生成人员（或授权人员）在监督下取用各自生成的加密机主密钥组件。

4.2.2 成员主密钥组件

各银联卡网络参与方不保存成员主密钥明文，除主机密文或机外密文留存外，机外不允许有明文出现。

4.2.3 工作密钥

不应出现在应用系统、终端、注入设备等相关设备以外的任何介质上。

4.3 保管或接收保管

4.3.1 由本机构自己生成的密钥组件的保管

密钥组件生成后用信封密封，注明密钥名称、用途、长度、密封日期；生成人员、监督人员与保管人员分别签名确认，加盖密封章，当场交保管人员置入不同的保险容器保管。

4.3.2 由对方分发的密钥组件的保管

接收机构的领取人员、密钥监督人员和保管人员同时在场办理交接手续，保管人员应审核信封及其名章的合法性和有效性，当场存入安全容器内保管。

4.4 与密钥安全有关的机密设备及密码的保管

4.4.1 存放密钥的保险容器

根据密钥保管方式的不同相应配备保险容器。

4.4.2 硬件加密机钥匙

硬件加密机钥匙可由设备管理人员负责保管，但密钥保管员不能开启密钥注入设备。

4.4.3 与密钥有关的密码

硬件加密机的安全密码、操作窗口密码（或授权操作密码）应分别由设备管理人员、设备操作人员掌管。

上述钥匙和密码应在保险容器保留一份，以备急用。

4.4.4 与硬件加密机相连的计算机设备（PC）

用于密钥维护的计算机设备（PC）必须专机专用，不得另做他用。

5.密钥的删除与销毁

5.1 基本要求

- 失效、作废或泄漏的密钥应及时采用安全可靠的方法删除或销毁；
- 各类密钥销毁过程必须专人监控和记录，相关人员签名确认，文档资料必须妥善保管（相关工作表格要素详见附录）；
- 执行删除操作时必须有监督员在场，经验证确认删除操作完整地执行后，才可认定密钥已被完全删除。

5.2 处理要求

5.2.1 主机系统中的密钥

在主机系统中找出存放待删除密钥的数据库表或密钥索引文件，经授权后由指定的操作员执行删除操作。

5.2.2 硬件加密机中的密钥

硬件加密机应具有密钥销毁功能，当加密机送检、维修或运输时应启动毁钥功能，保证硬件加密机中的所有密钥被彻底删除。

当需要删除加密机中的某个密钥时，应首先确定待删除的密钥在硬件加密机中相应的索引值，然后对该密钥进行删除操作，对无删除密钥功能的加密机可采用重写的方式覆盖需删除的密钥。若需删除加密机中所有的密钥时，可利用加密机提供的毁钥功能来操作。

5.2.3 终端设备中的密钥

设备中存放的密钥报废不再使用时可采用物理销毁的方法来删除密钥。对仍将继续使用的设备可采用覆盖的方法删除密钥。

5.2.4 存放密钥组件的介质

- 纸介质：采用“十字”粉碎、焚毁、溶化的方式，确保不可辨认、不能恢复；
- IC 卡：对可重复利用的介质，执行写卡操作，覆盖旧密钥，确保不可恢复。对于不再利用的介质采用芯片毁损的方式进行物理毁卡，确保不可恢复。
- 密钥传输及注入设备类：启动密钥枪或母 POS 等设备的毁钥功能销毁。

5. 2.5 相关机构的成员主密钥

当一方销毁密钥涉及另一方的成员主密钥时，应书面通知对方机构删除和销毁成员主密钥，对方机构删除和销毁后需书面返回回执并由相关人员签字确认。

6.密钥的泄漏与重置

一旦发生密钥泄漏，应立即更换被怀疑或确认泄漏的密钥及所有由该密钥保护的密钥，并重置已更新的密钥，密钥更新和重置后需向主管部门报告。

6.1 密钥泄漏情况的界定

- 有两段或两段以上密钥明文被盗或同时丢失；
- 有两段或两段以上密钥明文同时存放在同一台可被人读取的设备上；
- 系统内大量密钥泄漏或被攻破；
- 系统内大量持卡人 PIN 被泄漏；
- 严重违反本管理规则的操作要求，导致有人掌握完整密钥；
- 其他由密钥安全管理组织认定的情况。

6.2 审核程序

密钥泄漏和被攻破需经成员机构密钥安全管理的相关部门认定。

对于无法认定的情况，可聘请有关专家和管理人员进行审核，对于情况比较复杂的事件需专题报告中国银联，必要时可报公安部门协查。

6.3 密钥泄漏后应采取的措施

6.3.1 主密钥泄漏

主密钥泄漏后，应重新生成新密钥并马上启用，需生成的密钥包括加密机主密钥，成员主密钥和终端主密钥，以及各类工作密钥。

6.3.2 成员主密钥泄漏

成员主密钥泄漏后，应重新生成相应成员主密钥并立即启用，并对该成员主密钥所涉及的所有工作密钥予以更新。

6.3.3 终端主密钥泄漏

终端主密钥泄漏后，应重新生成相应的终端主密钥并立即启用，并对该终端的工作密钥予以更新。

6.3.4 工作密钥的泄漏

工作密钥泄漏后，应立即联机更换。

6.4 其他需要重置的情况

如发生硬件加密机无法正常工作或更换新的硬件设备等情况，可根据具体要求进行密钥重置。重置过程比照上述规定执行。

6.5 加强系统用户权限和操作密码的管理

对受理银联卡的各类系统应设置严格的用户管理权限，按级别分别设置各自不同的操作密码，各类密码只有相关人员本人掌握，不得共用密码。

如密码发生泄漏或人员离职，应及时更换或更改。

6.6 情况记录

详细记录各类密钥泄漏与处理情况，相关人员签名确认，文档资料必须妥善保管（相关工作表格要素详见附录）。

第四章　设备安全管理

本章对银联卡网络的终端机具、硬件加密设备的运行安全做出基本规定。

1. 基本要求

- 银联卡网络参与方使用的硬件加密设备必须经过国家密码管理委员会办公室审核通过。终端设备内的密钥安全模块应符合国家密码主管部门的规定和相关标准并经过国家认可的权威机构检测通过；对于未通过审核和批准使用的设备不得在受理银联卡的网络系统中使用，已经使用的应予以更换。

- 设备应满足中国人民银行颁布的《银行卡联网联合技术规范》、《银行卡联网联合安全规范》以及中国银联颁布的有关规范中规定的基本功能和安全要求。
- 对个人标识代码（PIN）的加、解密以及报文鉴别等操作必须在硬件加密设备中完成，完整的密钥和个人标识代码（PIN）的明文不得出现在加密机之外的任何地方。
- 管理或维护人员应经常对安全设备的物理情况、监控效果和安全状况进行检查，发现问题应立即纠正。

2.硬件加密设备安全的管理要求

2.1 设备操作

- 根据不同的操作权限，设置不同的操作密码；至少双人控制钥匙或密码来执行对设备的操作；
- 不能从硬件加密机的外部用任何形式读取密钥的明文；
- 硬件加密设备的外壳一旦被强行打开，设备内的密钥应全部自毁；
- 具有打印功能的硬件加密机只能在生成新的密钥时才可打印密钥内容，必须打印在密封信封内，由专用打印接口提供，不得通过网络方式提供。

2.2 设备运行

- 应采用双机热备，避免单机故障造成密钥丢失，影响正常交易；
- 应存放在带锁机柜中，机柜背板应固定，安放在严格进出管理的机房内；
- 应配备摄像系统监控对硬件加密机的操作，但不得监控到注入内容；
- 配备摄像监控系统的地方，不得将监控器对准加密设备的操作面板；
- 与外部网络连接的加密设备必须设置防火墙隔离措施。

2.3 设备启用及报废

- 硬件加密机启用前应确定机壳未被拆卸过；
- 新购买的加密机应修改加密机相关的缺省口令，并执行毁钥操作；
- 若使用 IC 卡保存加密机的密钥，应首先更换 IC 卡的缺省密码。
- 硬件加密机报废时，存贮在该设备中的密钥必须按要求及时删除。

3.终端设备安全管理

3.1 操作与监控

- 终端设备技术维护人员与日常业务管理人员应分离，职责明确；
- 每次对终端设备的操作，需严格按照操作手册、操作规程进行；
- 指定专人管理或通过监控系统实行 24 小时有效监控。

3.2 启用及报废

3.2.1 在终端设备初始化或更新配置之前，应确定：

- 机壳未被拆卸、密码键盘（PIN PAD）粘贴封条、密码模块未被非授权修改或替换；
- 终端主密钥生成、注入过程是否符合本规则要求；
- 主管密码、操作员密码是否为缺省值。

对不符合安全要求的情况，应立即采取措施，消除安全隐患。

3.2.2 在终端设备报废时，必须立即删除或销毁存储在该设备中的所有密钥。

第五章　制度监督

本章对密钥维护人员的岗位配置、工作职责、审批制度和监督机制做出基本规定。

1.组织管理

银联卡网络参与方均应指定专门部门或人员负责密钥安全管理工作。

1.1 主要工作职责

- 结合本单位实际状况，制定严格而有效的实施细则，落实岗位责任制；
- 负责密钥生命周期，包括生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置等各环节全方位、全过程的规范操作与安全管理。
- 根据密钥特性，妥善保管密钥组件、密码函、IC 密码卡、软件、源代码、涉及密钥安全管理的各种文档。
- 制订其他有关的安全专项管理制度，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。

- 涉及密钥生成、传输、保管各个环节的设备安全管理。
- 定期对本单位密钥安全管理状况进行自查，填报有关表格、报送报告。

1.2 密钥维护人员的基本配备要求

根据密钥安全管理的要求，需配备专职或兼职人员负责密钥生命周期各环节的具体工作，所有的审批和操作必须指定专人负责，各专管人员均有自己的业务主管权限，未经批准，不得擅自互换或代替。

各单位具体配备的人员为：

密钥监督员：负责监督整个密钥生成过程的规范性。

设备管理员：负责相关设备的安全管理工作。

设备操作员：负责相关安全设备的操作工作。

密钥生成员（一般应由硬件加密机使用单位三个不同部门的负责人担任）：负责或授权专人负责密钥的生成、分发、保管及销毁等工作。

档案管理员：负责密钥档案资料的保管工作。

密钥销毁员：负责密钥资料的销毁。

上述人员必须相对固定，均应指定候补人员。相关工作可以兼职，但兼职必须按照本规则第二、三章的相关规定，遵循分隔操作、双重控制的原则，不允许任何一个人具有全部加密资料和加密设备钥匙的控制权。

密钥维护人员调离时，应办理交接手续，并由密钥监督人员审核认可。

2. 审批与操作制度

银联卡网络参与方应遵循本规则规定，根据具体应用环境，对各类密钥生成、注入和启用、传输、保管、泄漏与重置、删除与销毁等生命周期流程制定专门的操作规程，建立并履行严格的操作审批手续登记制度（相关工作表格要素详见附录），每一过程必须详细记录，相关人员签名确认，文档资料必须妥善保管，保存期限应不低于记录对象的生命周期，确保各类密钥的安全性与规范性。

未履行审批手续的操作一律视同违章操作，应严格禁止。

3. 自查与监督

银联卡网络参与方共同建立监督机制，进行自查与监督，确保密钥生命周期过程操作和管理的规范性，维护持卡人个人标识代码（PIN）及相关敏感信息

在银联卡网络的安全传输。

3.1 业务开办前对个人标识代码（PIN）及密钥安全进行资格审查

银联卡网络参与方在开办与个人标识代码（PIN）关联的业务品种前，需向中国银联说明 PIN 安全管理的有关情况，在规定时间内填报专题调查问卷；填报问卷的银联卡网络参与方应对问卷的真实性负责（下同）。

审核结果作为业务开通的必要条件。

开办外卡收单业务的银联卡网络参与方须按照国际组织的相关要求，在规定时间内完成调查问卷的填报。

3.2 自查

银联卡网络参与方应定期或不定期对本单位密钥安全管理状况组织检查。自查工作由分管负责人统一组织，技术、业务部门的负责人与密钥维护人员参加。

3.2.1 自查内容

结合当前工作实际确定自查提纲和重点；重点检查密钥资料归档情况是否严密、规范，是否存在未经授权操作，是否存在表格要素填写不全或档案缺失现象，密钥组件明文备份介质与存放情况是否符合要求。

针对上次自查报告中存在的问题，重点检查整改落实情况。

3.2.2 自查方式

3.2.2.1 调阅档案

全面审核所有自上次检查以来的申请表、登记表、审批手续等书面记录。首次自查应审核全部密钥档案资料。

通过查阅申请表、登记表的处理流程，核查密钥操作流程是否符合本规则中关于密钥生命周期安全管理的要求。

3.2.2.2 上机检查

模拟生成密钥的全过程。

3.2.2.3 工作记录

针对检查情况设计并填写工作表格；所有检查过程均应记录在册，相关人员现场签章。

3.2.3 情况处理

对自查工作中发现的问题，按照严重程度提出相应整改意见，分别处理：

- 对存在泄漏风险隐患、违反规则，如未执行分人操作、保管、档案缺失等原则性问题，应立即责成技术、业务等相关部门立即改正，视情况采取销毁、删除、重置等措施；
- 对轻微违反，如保管不善、密钥审批表格要素填写不全等情况同步提出书面改进意见；
- 对违反其他规定，如存放加密设备的机柜未上锁、机房出入登记制度执行部严格等情况，责成有关人员纠正。

3.2.4 自查报告

自查结束后，应完成工作报告，其主要内容包括：单位的基本情况、密钥生命周期安全管理、维护状况、存在问题及整改意见。

在规定时间内向中国银联报送调查问卷，作为自查报告附件，留底备查。

3.3 监督

中国银联风险管理委员会代表全体银联卡网络参与方履行监督职能，以维护共同利益。

3.3.1 调查对象

中国银联将定期或不定期组织对银联卡网络参与方开展调查。其中，重点对象明确如下：

- 申请加入银联网络或开办新的与个人标识代码（PIN）关联的业务品种的；
- 发生个人标识代码（PIN）泄漏等风险事件，给其他银联卡网络参与方带来业务损失或潜在风险隐患的；
- 报送的自查报告存在较为严重问题的；
- 涉及被相关银联卡网络参与方投诉或提起争议裁定，与个人标识代码（PIN）相关事件中的；
- 限期整改未达标的；
- 国际组织通报存在风险隐患的；
- 其他信息安全管理不严的。

3.3.2 监督流程

3.3.2.1 确定监督重点

对照本规则基本要求，确定监督重点；

针对自查报告中存在的问题，重点抽查落实整改情况。

3.3.2.2 发送监督通知

在监督日前一周以函件形式通知被查单位，并将本次监督重点和要求填报的表格发送给被查单位。

3.3.2.3 书面反馈监督情况

具体监督方式参照本章 3.2.2“自查方式”执行。

基本监督情况、存在问题、改进意见以书面形式反馈并限期改进。

3.3.2.4 申诉与反馈

被查单位可以对存在问题提起申诉。申诉应在监督日后 7 个工作日内提交中国银联。

中国银联将核实申诉内容，结果于 7 个工作日内回复。

3.3.3 监督内容

3.3.3.1 密钥生命周期的安全管理

对密钥生成、保管、启用、更新、销毁操作等过程进行监督，杜绝违规或超权限操作，禁止发生以下情形：

- 未使用专用加密设备，密钥的明文出现在系统或程序中；
- 加密机主密钥、成员主密钥以单个密钥形式出现，或密钥组件在权限范围外可以被合成；
- 密钥未按规定动态更新，长时段呈静态状况，导致被非法穷举攻破；
- 废旧密钥未及时销毁，随意丢弃或放置；
- 在测试系统和生产系统使用同一密钥，或在测试系统出现生产系统密钥的明文；
- 同一密钥在多个地方使用；
- 不同银联卡网络参与方使用相同的加密机主密钥；
- 其他。

3.3.3.2 与 PIN 及密钥相关的机具设备、系统运行的维护管理状况

- 设备的物理环境如电源电流及电压、温湿度、是否变化；

- 照明、消防及监控设施是否完好，摄像头是否清晰有效，摄像头不能对准键盘或屏幕；
- 设备的外壳是否完好，是否有被拆卸、破坏的迹象；
- 设备有无多余的连接线或外接电缆；
- 终端设备（如 ATM）周围是否张贴有关操作提示；
- 其他各项安全监督指标是否符合要求。

3.3.3.3 对终端定期进行安全监督

- 终端硬件（包括 PIN PAD）是否完好
- 密码键盘（PIN PAD）封条是否损坏
- 终端软件是否更新过
- 终端操作是否正常

3.3.4 情况处理

对密钥安全管理监督工作中发现的问题或自查中的遗留问题，按照性质的严重程度和是否能现场定性进行分别处理。

3.3.4.1 现场纠正

对违反本规则并能够现场定性的问题，应向被监督单位有关负责人及其技术、业务等相关部门提出改正意见，视情况口头提出如销毁、删除、重置等针对性措施建议。

3.3.4.2 事后处理

对现场不易总结或问题性质严重甚至有可能发生案件的情况，事后立即向被监督单位有关部门负责人提出针对性意见。

3.3.4.3 违规处罚

被监督单位违反本规则操作，并给银联卡网络参与方带来损失的，报经风险管理委员会同意，视严重程度向其分别给予承担相应损失责任并限期整改、增加监督力度、限制业务运营种类、罚款以至网络退出等处罚。

附录 A：术　语

ATM 自动柜员机（Automatic Teller Machine）

一个有电子功能,接受密码，提供取现和支票的终端自行处理的机器。

密钥校验值（Check value）

用于校验密钥输入时的正确性。分为密钥组件的校验值和密钥合成后的总校验值。

密文（Cipher text）

数据的加密形式，即已加了密的明文。

分裂学（Cleavage）

将密钥信息分裂为两个及两个以上的组件，单个人员凭掌握的单个组件无法获得足够的信息来了解实际密钥的方法。

数据加密算法（Data Encryption Algorithm，DEA）

一个发布的加密算法，把基于可变密钥的数据译成密码，用来保护重要信息。

解密（Decrypt）

将密文转换成明文的过程。

双重控制（Dual control）

单个人员不能控制保护项的过程。

加密（Encrypt）

通过一种加密算法（可逆的）将数据转换成密文。

硬件加密机（HSM）

由国家指定生产厂商研制开发的，专门应用于内部网络系统中，以规定的协议通讯，直接与主机相连接，实现对网络上传输的信息进行保护或鉴别，以保证信息的正确性，防止内部重要的数据被非法篡改或窃取的设备。

密钥（Key）

一种与密码算法联系起来使用的参数。

密钥分量（Key component）

见密钥组件。

密钥交换密钥（Key encryption key，KEK）

包含两类，成员主密钥（MMK）和终端主密钥（TMK），密钥交换密钥是在传输过程中对工作密钥进行加密的密钥。

密钥生命周期（密钥生存期）（Key lifecycle）

密钥从生成开始到被销毁为止，密钥存在的过程，包括生成、存储、分发、注入、使用、删除、销毁和存档等。

密钥管理（Key management）

在整个密钥生命周期内的对密钥及相关参数（初始向量、计数值）的操作，包括生成、存储、分发、注入、使用、删除、销毁和存档等。

加密机主密钥（MK）

在密钥加密密钥和处理密钥中，最高级别的密钥加密密钥称为加密机主密钥，用于加密下一层（MMK）密钥的密钥，受硬件加密机保护。

成员主密钥（MMK）

在密钥加密密钥和处理密钥中，处于第二层的密钥加密密钥称为成员主密钥，用于加密下一层（WK）密钥的密钥，受 MK 加密保护。

消息鉴定码（Message Authentication Code, MAC）

MAC 是用来完成消息来源正确性鉴别，防止数据被篡改或非法用户窃入的数据。

MAC 密钥（MAK）

用于生成交易报文合法性的认证数据(MAC)的密钥称为 MAC 密钥(MAK)。

个人标识代码（Personal Identification Number, PIN）

个人识别码是在联机交易中识别持卡人身份合法性的数据信息，在计算机和网络系统中任何环节都不允许 PIN 以明文的方式出现。

PIN 加密密钥（PIK）

用于加密 PIN 的密钥称为 PIN 加密密钥。

POS 销售点终端（Point Of Sale）

能够接受磁条卡信息，有通讯功能，接受指令而完成金融交易信息和有关信息交换的设备。

伪随机（Pseudo-random）

指由算法产生，生成结果是一系列可以转换成二进制的数字。

随机（Random）

指无法预知和重复。

对称密钥（Symmetric key）

用于对称加密算法中，加密和解密过程中使用相同的对称密钥。目前通用的对称密钥算法为 DES 算法。

终端（Terminal）

指用于读取银行卡信息，发送交易指令的设备。包括银行磁条卡销售点终端（POS）、商户收银系统（MIS）、自动柜员机（ATM）等。

终端 MAC KEY（TAK）

用于终端上对报文进行 MAC 生成和检验。

终端管理密钥（TGK）

用于传输和保存终端主密钥的密钥。

终端主密钥（TMK）

用于加密终端工作密钥（TPK、TAK）。

终端 PIN KEY（TPK）

用于加密客户输入的 PIN。

终端工作密钥（TWK）

是指在终端上对 PIN 进行加密保护的 PIN 加密密钥（TPK）和用于终端报文合法性认证的密钥(TAK)。

工作密钥（Working key, WK）

工作密钥是对 PIN 加密、参与认证码（MAC）计算的密钥。工作密钥必须经常更新。在联机更新的报文中对工作密钥必须用相应的密钥加密，形成密文后进行传输。

密钥组件（Key component）

建立和维持密钥加密联系的数据（如密钥、初始向量）。

附录 B：遵循标准

1.国内标准

BG 4943-1995 信息技术设备（包括电气事务设备）的安全（IEC 950）

BG 9361-88 计算机场地安全要求

GB/T 15277-1994 信息处理 64 位块加密算法操作方式（ISO 8372:1987）

GB 15852-1995 信息技术-安全技术-用块加密算法作校验函数的数据完整性机制（ISO/IEC 9797:1994）

GB 15853.1-1995 信息技术-安全技术-实体鉴别机制第 1 部分： 一般模型（ISO/ICE 9798-1:1991）

GB 15853.2- 信息技术-安全技术-实体鉴别机制第 2 部分： 使用对称加密算法的实体鉴别（ISO/IEC 9798-2:1994）

GB/T18789-2002《自动柜员机（ATM）通用规则》

JR/T 0001-2001《银行磁条卡销售点终端规则》

2.国际标准

ANSI X3.92 数据加密算法 （生成）

ANSI X9.17 金融机构的密钥管理（生成）

ANSI X9.19-1986 金融机构零售消息鉴别

ANSI X9.24 金融服务零售密钥管理（生成）

ANSI X9.42-2001 金融机构公开密钥加密：使用离散对数加密对称密钥协议（Key Exchange）

ANSI X9.44-200x 金融机构使用可逆算法公开密钥加密：RSA 对称密钥管理（Key Exchange）

ANSI X9.52-1998 TDES：操作方式

ANSI X9.63 ECC （密钥交换）

ANSI X9.66-200x 加密模块的安全必备

ANSI X9.8 标识号的管理和安全 （个人标识码 PIN）

ANSI X9.82 随机数产生 （生成）;

ANSI X9.86 电子商务 PIN 安全;

ANSI X9.87 磁条卡 PIN 安全;

ANSI X9.9-1986 金融机构的消息鉴别（批量）（消息鉴定码 MAC）

ISO 9564-1:1991 银行业务-个人标识号管理和安全 第 1 部分：PIN 保护原则和技术

ISO 9564-2:1991 银行业务-个人标识管理和安全 第 2 部分：认可 PIN 加密算法

ISO 11568-1:1994 银行业务-密钥管理（零售） 第 1 部分：密钥管理引言

ISO 11568-2:1994 银行业务-密钥管理（零售） 第 2 部分：对称密码用的密钥管理技术

ISO 11568-3:1994 银行业务-密钥管理（零售） 第 3 部分：对称密码的密钥生存期

ISO 11568-4:1994 银行业务-密钥管理（零售）第 4 部分： 使用公开密钥加密的密钥管理技术

ISO 11568-5:1994 银行业务-密钥管理（零售）第 5 部分：公开密钥加密系统的生存期

ISO 11568-6:1994 银行业务-密钥管理（零售）第 6 部分：密钥管理方

ISO/IEC 11770-2 1996 信息技术-安全技术-密钥管理 第 2 部分：使用对称技术的机制

ISO/IEC 11770-3 1998 信息技术-安全技术-密钥管理 第 3 部分：使用非对称技术的机制（RSA 和 Diffie-Hellman）

ISO/WD 13491-1 1998 保密加密设备-第 1 部分：概念、特性、管理和依赖性

3. 银联卡个人标识代码（PIN）应遵循的标准

涉及的密码及其保存与密码输入设备均须符合 ANSI X9.8 或 ISO9564 标准。

密码的加密必须符合 ISO FORMAT 0 的方式标准，同时符合 ANXI X9.87 标准或 ISO9564-1 标准。

附录 C：密钥生命周期各阶段工作表格基本要素

密钥生命周期阶段		基本要素
密钥生成	本方生成	生成时间、地点，密钥类型、长度、生成设备及方法，密钥使用机构、机构编号、使用设备名、设备编号；密钥监督、设备操作、每个密钥生成人员的签名栏等。
	提供给对应银联卡网络参与方密钥生成表格(对方生成 B 段密钥的回复表)	对应的银联卡网络参与方名称、地址、接收人姓名，密钥名称、长度、奇偶校验要求、密钥组件段号、密钥用途、使用机构名称、机构编号、密钥内容、密钥检验值（Check Value）
分发和传输	密钥分发	使用方名称、机构编号、接收方名称、地址、领取时间、地点、密钥类型、长度、密钥使用设备名称、设备编号、密钥监督、保管、分发（如有）、接收（或每个领取）人员签名栏、分发机构分发、保管、监督人员签名栏等。
	密钥接收	传送机构联系人姓名、地址、机构名称，密钥长度、奇偶校验、密钥组件段号、本方接收及保管人员、密钥监督人员签名栏等。
密钥注入		使用单位、密钥类型、长度、注入时间、地点、使用设备名、设备编号、注入设备、密钥监督员、设备操作员、注入人员签名栏等。
泄漏和被攻破		泄漏或被攻破的时间、地点和方式，密钥类型、使用单位、使用设备名称和编号，泄漏造成的损失和补救措施等。
密钥删除销毁		密钥类型、密钥编号、销毁时间、介质是否重用、密钥销毁、监督人员签名栏等。

银联卡账户信息泄漏点损失补偿流程

（中国银联第四届风险管理委员会第五次会议审议通过）

第一章　总则

第一条 为加大对银联卡账户信息泄漏点（以下简称“CPP 点”）损失补偿力度，快速高效地界定账户信息泄漏事件责任，保障发卡机构的合法权益，根据《银联卡账户信息与交易数据安全管理规则（修订）》（银联风管委[2006]6号），《银联卡风险事件报送及协助调查规则（修订）》（银联风管委[2012]4 号）和《银联卡账户信息安全事件调查处理流程》（银联风管委[2007]8 号）制订本流程。

第二条 本流程是对《银联卡账户信息与交易数据安全管理规则（修订）》（银联风管委[2006]6 号）中确定的账户信息安全泄漏事件损失补偿标准及流程的细化实施。

第三条 本流程适用的 CPP 点范围包括公安司法机关或监管机构查实的 CPP 点。

第四条 本流程适用的责任主体为 CPP 点的收单机构，适用的补偿对象为在 CPP 点发生账户信息泄漏的发卡机构。

第二章　参与各方的职责分工

第五条 CPP 点损失补偿工作参与方为中国银联风险管理委员会办公室（以下简称“风管委办公室”）、在 CPP 点发生账户信息泄漏的发卡机构、CPP 点的收单机构等。

第六条 风管委办公室负责根据本流程确定的处理补偿标准和措施进行操作，包括对 CPP 点信息的整理，损失补偿措施的通知和执行等。

第七条 在 CPP 点发生账户信息泄漏的发卡机构需配合进行损失补偿等信息的确认。

第八条 CPP 点的收单机构负责做好 CPP 点调查配合、确认损失补偿措施、落实整改要求等。

第三章 CPP 点损失补偿流程

第九条 对于公安司法机关或监管机构查实的 CPP 点，风管委办公室依据本流程直接启动损失补偿。

（一）损失补偿标准

根据公安司法机关或监管机构查实的 CPP 点案件情况，按照以下标准确定损失补偿金额。

1、根据泄漏卡片数量及欺诈损失金额[5]，补偿金额标准如下：

（1）泄漏卡片数量达到 1000 张以上（含）或欺诈损失金额达到 500 万元人民币以上（含），补偿金额为欺诈损失金额的 25%，最高不超过 50 万元；

（2）泄漏卡片数量达到 600 张以上（含）1000 张以下，或欺诈损失金额达到 100 万元人民币以上（含）500 万元人民币以下，补偿金额为欺诈损失金额的 25%，最高不超过 30 万元；

（3）泄漏卡片数量达到 200 张以上（含）600 张以下，或欺诈损失金额达到 30 万元以上（含）100 万元以下，补偿金额为欺诈损失金额的 25%，最高不超过 20 万元；

（4）泄漏卡片数量低于 200 张，或欺诈损失金额低于 30 万元，补偿金额为欺诈损失金额的 25%。

2、除以上补偿费外，根据泄漏卡片数量，按照每张卡 10 元人民币的标准补偿换卡费，补偿总额不超过 40 万元。

（二）损失补偿的操作流程

1、补偿金额计算：风管委办公室获得公安司法机关或监管机构查实的 CPP

[5] 本流程中欺诈损失金额是 CPP 点发生账户信息泄漏的卡片发生后续伪卡盗刷欺诈的损失金额。

点案件情况后，根据发卡机构数量、对应的泄漏卡片数、欺诈损失金额，按比例计算损失补偿金额。对于 CPP 点信息中包含欺诈损失金额的，以各发卡机构损失金额占比计算补偿比例，未包含欺诈损失金额的，以卡片数占比计算补偿比例。

2、补偿通知：风管委办公室向 CPP 点涉及的发卡机构发送“CPP 点损失补偿通知”（见附件 1），要求各方于 10 个工作日内回复确认，收到回复确认之后向收单机构发送“CPP 点处理通知”（见附件 2）。

3、补偿操作：风管委办公室在回复期满制定“CPP 点损失补偿金额一览表”（附件 3），于 5 个工作日内从 CPP 点收单机构清算账户中扣除，并向 CPP 点涉及的发卡机构清算账户中划拨补偿款项。

4、追偿操作：完成损失补偿流程之后，若公安司法机关或监管机构进一步查实 CPP 点泄漏的更多银联卡账户信息，风管委办公室可依据本流程规定的补偿标准追加损失补偿。

第十条 公安司法机关或监管机构在调查确认欺诈损失的过程中，发卡机构应配合提交相关欺诈交易明细、欺诈损失金额等信息，并在提交欺诈损失相关信息之前已向中国银联报送欺诈交易。在损失补偿金额确定之前，相关欺诈交易如已通过退单或争议等渠道获得补偿，则不纳入损失补偿范围。

第十一条 风管委办公室针对中国银联风险系统侦测的疑似 CPP 点，以及发卡机构报送的疑似 CPP 点，推动公安司法机关立案调查，或推动发卡机构主动报案，确认 CPP 点信息之后启动损失补偿流程。

第十二条 风管委办公室定期整理公安司法机关或监管机构查实的 CPP 点，以及成员机构调查反馈的 CPP 点，对于问题比较突出的 CPP 点的收单机构，可采取向风管委委员行通报、敦促检查整改等措施。

第四章　附则

第十三条 本流程经中国银联风险管理委员会审定后发布。

第十四条 本流程自发布之日起实施。

附件 1：

CPP 点损失补偿通知

（单位名称）：

经公安司法机关/监管机构查实，XX 机构--------(收单特约商户名称或自助终端布放商户)被确认为 CPP 点，涉及被泄漏信息卡片数共----张，已确认欺诈损失----元，其中贵单位涉及被泄漏信息卡片数为----张，欺诈损失----元。根据《银联卡账户信息泄漏点（CPP）损失补偿流程》相关规定，贵单位获得补偿的金额为----元，补偿金额将由中国银联风险管理委员会办公室从该 CPP 点收单机构清算账户扣减后划拨至贵单位清算账户。

附： CPP 点信息

联系人：

电话：

中国银联风险管理委员会办公室

年 月 日

CPP 点信息

★注意保密

CPP 点 1 信息			
商户名称		发生欺诈卡片数	
商户代码		涉及发卡机构数量	
收单机构代码		损失金额	
泄漏期			
CPP 点 2 信息			
商户名称		确认发生欺诈卡片数	
商户代码		涉及发卡机构数量	
收单机构代码		损失金额	
泄漏期			
联系人方式			
姓名	电话	传真	邮箱

附件 2：

CPP 点处理通知

（单位名称）：

经公安司法机关/监管机构查实，贵单位--------(收单特约商户名称或自助终端布放商户名称)为 CPP 点，涉及泄漏信息卡片数为----张，欺诈损失金额为------元，涉及发卡机构----家。

根据《银联卡账户信息泄漏点（CPP）损失补偿流程》相关规定，贵单位需承担损失补偿费用----元。补偿费用将于中国银联风险管理委员会办公室发送本通知后 5 个工作日内从贵机构清算账户中扣除，并向遭受卡片信息泄漏损失的发卡机构进行费用补偿。

附：CPP 点信息

联系人：

电话：

中国银联风险管理委员会办公室

年　月　日

CPP 点信息

★注意保密

CPP 点 1 信息			
商户名称		发生欺诈卡片数	
商户代码		涉及发卡机构数量	
收单机构代码		损失金额	
泄漏期			
CPP 点 2 信息			
商户名称		发生欺诈卡片数	
商户代码		涉及发卡机构数量	
收单机构代码		损失金额	
泄漏期			
联系人方式			
姓名	电话	传真	邮箱

附件 3：

CPP 点损失补偿金额一览表

对 CPP 点收单机构的处理				对 CPP 点涉及发卡机构的补偿		
商户代码	商户名称	收单机构代码	金额	发卡银行代码	补偿金额	补偿日期
********	********	********	人民币 XX 元	********	人民币 XX 元	********
				********	人民币 XX 元	********
				********	人民币 XX 元	********
********	********	********	人民币 XX 元	********	人民币 XX 元	********
				********	人民币 XX 元	********
				********	人民币 XX 元	********

中国银联风险管理委员会办公室
XX 年 XX 月 XX 日

关于双倍长密钥算法加解密迁移时间进度的要求

（银联风管委〔2006〕1 号）

为明确国内双倍长密钥算法加解密迁移时间，结合各成员机构的实际情况，现提出如下关于双倍长密钥算法加解密迁移时间进度的要求：

- 所有通过银联卡网络进行银行卡交易的成员机构、受理银联卡的联网机构及其它关联机构接入银联卡网络时，其系统必须支持双倍长密钥算法加解密；
- 从 2005 年 11 月 1 日起，所有新配置的 PIN 接收设备（包括 ATM、POS 及自助终端等）须支持双倍长密钥算法加解密；
- 从 2007 年 7 月 1 日起，所有 ATM 须支持双倍长密钥算法加解密，且所有由支持双倍长密钥算法加解密的设备发起的交易从交易接受端到发卡端须经双倍长密钥算法加解密；
- 从 2008 年 7 月 1 日起，所有自助终端须支持双倍长密钥算法加解密；
- 从 2010 年 7 月 1 日起，所有 PIN 接收设备（包括 ATM、POS 及自助终端等）等须支持双倍长密钥算法加解密。

第二部分 银联卡账户信息安全管理指南及工具

银联卡账户信息与交易数据安全管理指南

（银联风管委〔2004〕9 号）

前言

成员机构、成员机构的代理机构、商户以及他们的上一级管理机构应当采取有效的措施来保护账户信息和交易数据的安全。保证账户信息与交易数据的安全性、完整性和可用性是银行卡行业的首要工作，因而这些信息资产必须受到保护以防未授权的篡改、泄漏和销毁。目前，由于越来越多的代理机构和非成员机构能够访问到账户信息和交易数据，这使得对于各成员机构而言，确保这些信息的安全变得越来越重要。

《银联卡账户信息与交易数据安全最佳指南》（以下简称“指南”）是《银联卡账户信息与交易数据安全管理规则》（以下简称“规则”）的辅助性文件。《规则》和《指南》为成员机构、成员机构的代理机构和商户如何保护账户信息和交易数据安全提供了标准和指导方针。总体而言，《规则》表述了用以保护账户信息和交易数据安全的标准和规范，而《指南》则提供了更多具体的实施细节，以协助成员机构更有效地实施《规则》。《指南》并没有涵盖所有的安全需求，指南中的信息仅用于辅助各机构实施《规则》中的条款，因此并不是所有机构必须遵守的，而仅作为参考。

本指南的目标读者是：成员机构，成员机构的代理机构以及能够访问到账户信息和交易数据的商户。

《指南》中的内容基于下列文献：《ANSI Information Security for Financial Organizations Guidelines, X9/TG-5 (1992)》，《ISO/TR 13569 Banking and Related Financial Services Information Security Guidelines, Second Edition》。

第一章 政策制定

为了有效地保护账户信息和交易数据，成员机构在制定相关政策、管理办法时应当遵循《规则》中的要求，并注意以下几个方面：

- 全盘考虑与账户信息和交易数据相关的各种风险以及控制这些风险的措施；
- 明确不同岗位（如管理人员，工作人员等等）的员工各自在保护账户信息与交易数据安全方面的责任；
- 由专人负责保护信息资产和确定安全等级；
- 建立相关的培训机制，以确保各类雇员知道他们在账户信息与交易数据安全方面应当承担的责任；
- 明确发生数据安全事故时的报告机制和处理措施；
- 根据本机构的实际情况，制定具体的安全管理实施办法，但不得与《规则》相抵触；
- 政策的制定应当鼓励和其他相关部门， 如审计、监察部门的合作；
- 制定相关考核标准，用于监督信息安全项目实施的有效性和具体执行情况；
- 制定并及时调整在采用新技术和出现新的安全隐患时的数据安全应对措施；
- 制定检查代理机构和商户遵守《规则》要求的具体措施。

第二章 组织管理

为了确保账户信息与交易数据的安全和完整，成员机构、成员机构的代理机构及商户应当加强各机构内部的组织管理。组织管理主要包括机构各级领导和雇员职责的划分、人事制度和安全审计管理、数据安全教育等内容。

2.1 岗位职责

以下部分描述了机构中各级管理岗位在账户信息与交易数据安全管理中的职责。由于各机构管理层的组织结构不尽相同，因而对各种职位的称谓也可能不同。本《指南》仅按照一般惯例中采用的称谓来界定岗位职责，各机构可

根据具体情况作相应的调整。

机构管理高层

机构内部最高管理层官员肩负着机构正常运营的重任。管理高层官员应授权并支持账户信息和交易数据安全项目的建设，并向机构内部各级员工强调账户信息与交易数据安全管理的重要性。

业务主管

由于各级业务主管具体负责机构的运营和指导、监督雇员的工作，因此主管经理在实施账户信息和交易数据安全项目中起着至关重要的作用。业务主管在账户信息与交易数据安全管理工作中的职责包括：

- 理解，支持和遵守《规则》的各项条款，并负责组织与这些规则相适应的相关程序的实施；
- 确保雇员、供应商和承包商理解、支持和遵守《规则》中的条款；
- 创造良好的工作氛围，以鼓励雇员、供应商和承包商及时报告与账户信息和交易数据安全相关的事宜；
- 负责就与账户信息和信息安全有关的事宜与信息安全管理官员进行沟通；
- 参与并组织与账户信息和交易数据安全管理相关的交流和培训活动；
- 定义具体业务中“权限”的标准，以实施和维护适当的访问控制；
- 整合实施账户信息与交易数据安全管理项目所需要的各种资源；
- 按照内部安全管理政策、规章，或者是涉及账户信息和交易数据安全注意事项的要求，更新、检查各项安全措施。特别在发生以下情况时：

— 由于安全疏漏造成巨大损失；

— 购买新的电脑系统和软件或者进行系统升级；

— 采用新的通讯服务；

— 引进新的业务处理服务。

— 发现新的安全隐患。

信息安全管理经理

信息安全管理经理是指负责开发、实施和推广安全管理项目以保护账户信息和交易数据的高级官员。信息安全经理主要承担以下工作：

- 负责制定适用于整个机构的所有信息安全管理政策和标准，这些政策和标准应当适应技术更新和防范潜在安全隐患的需要；
- 协助各业务单位制定安全管理标准和实施标准的指导方针，包括和业务经理合作，制定安全控制流程；
- 对需要访问账户信息和交易数据的业务合作伙伴进行审查以确保合作伙伴符合《规则》要求；
- 向成员机构解释并确保他们知道规则中的例外情况；
- 了解对账户信息和交易数据资产产生威胁的要素并跟踪其最新发展（比如，参加信息安全会议，阅读相关资料和出版物等等）；
- 通过参加内部培训、信息安全研讨会和在职培训等方式掌握当前信息处理技术和最新的信息保护和控制方法；
- 在履行职责时，积极应用管理和组织技能、业务知识开展工作，积极参加职业资格考试；
- 审核与账户信息和交易数据安全相关的各类报告，并及时将审核结果和内容通知相关的管理部门。信息安全官员负责回复审计中提出的疑问，并负责跟踪改进措施，以确保在规定的时间内提高安全管理水平；
- 及时预测、发现账户信息和交易数据安全隐患，并向管理高层报告；
- 负责发布严重或者紧急账户信息与交易数据安全隐患报告（如电脑病毒）；
- 协助调查攻击或威胁账户信息和交易数据安全的行为；
- 协助处理系统被攻击后的恢复工作。

信息系统安全管理员

信息安全管理员负责具体执行、实施账户信息及交易数据安全管理。每个业务部门和信息安全经理在决定其各自业务部门使用者的访问权限后，书面通知信息系统安全管理员，由系统安全管理员设置访问权限。信息系统安全管理员要定期审核这些访问权限并在适当的时候进行修改。每个信息访问控制系统应该配备至少一名信息系统安全管理员，以保证有效地监控和实施访问控制流程。信息系统安全管理员的责任如下：

- 根据信息资源控管人员的指示和内部政策、规章和标准，准确地控制

访问权限；

- 及时掌握雇员被解雇、调动或工作职责改变等状况；
- 密切监控有高级访问权限的用户。对这些用户，当他们不再需要这些权限时，应迅速将他们的权限终止。
- 检查每日的访问日志，以监控是否有可疑行为发生，比如重复性非法访问企图，因为这些行为将威胁到系统的完整性、保密性和实用性。信息系统安全管理员应把发现的可疑行为及时报告给数据信息的拥有者，并协助他们进行调查和采取防范措施。
- 确保每一个用户只能使用已注册过的有效用户名（USERID）访问系统。在访问系统时，系统应通过密码、生物识别、数字认证等方法验证访问者的身份。
- 收集、保护审核记录信息。

雇员、供应商和承包商

雇员，供应商和承包商应承担下列责任：

- 理解，支持和遵守《规则》中的各项条款，并执行各机构的具体实施步骤；
- 知道他们的行为是否影响到账户信息与交易数据的安全；
- 及时报告威胁账户信息和交易数据资产或处理设施安全、完整的任何可疑行为和状况。

法律顾问

法律顾问应该负责审阅成员机构与雇员、客户、服务提供商、项目承包商和供应商签订的各类合同，以确保合同中有关账户信息和交易数据安全的条款表述完整。注意所有的合约都不能与《规则》中的条款相抵触。法律顾问需要对储存和处理账户信息与交易数据的机构进行背景调查，背景调查包括审核机构的法人代表或拥有者的背景。同时，由于一个机构的财务状况会直接影响到公司在信息安全控制方面的投入，因而对财务状况的审核至关重要。

2．2 人事管理

人力资源是一个机构最重要的资产。一方面，机构的雇员工作在安全防御的一线，他们帮助实现技术功能、发现安全隐患、协助构建安全体系；另一方

面，人也能进行欺诈犯罪、利用现代高科技技术进行作案。因此各机构既应当考虑如何调动人力资源的能动性来保证公司内部安全，也应当运用高科技手段来减少少数分子趁机犯罪的机会。

各机构在人力资源管理方面应该做到：

- 确保所有员工包括正式雇员、合同制员工和临时雇员在访问账户信息和交易数据时遵守《规则》中有关“访问权限”的条款。
- 当员工的雇佣合同被中止或者工作调动时，及时通知信息系统安全管理员。

2．2．1 安全教育

为了加强对雇员在信息安全意识方面的教育，应该做到：

- 明确告知所有雇员，包括各级领导和员工，账户信息和交易数据是公司的资产，只可以用于与公司相关的业务。
- 作为实施账户信息和交易数据安全项目的一部分，制定安全意识培养和交流的计划，让雇员知道加强信息安全的重要性和必要性。
- 制订相关政策并将账户信息和交易数据安全事项责任化，使员工认识到违反安全规定可能导致的后果。
- 鼓励加强对员工的教育，以使员工知道他们工作中所访问信息的敏感性；
- 鼓励经理了解雇员的不正常行为，并积极寻求人事部门的协助；
- 在制定雇佣和管理政策时考虑这些政策对员工行为的影响。

2．2．2 招聘政策

除非法律禁止，应该对有权访问账户信息和交易数据的员工进行背景调查，一旦发现员工有任何犯罪记录或者明显的经济、财务问题，就应当取消该员工访问系统的权限。

对于从事机密性较强的工作的员工要定期进行检查，及时发现他们的可疑行为。

犯罪行为记录应包括 7 年内发生的以下行为，但不仅限于此：

- 严重的经济犯罪；
- 参与组织与犯罪团伙有关的违法行为；

- 多起一般经济违法行为；
- 对于有权访问电脑设备、软件和数据的员工所发生的电脑犯罪。
- 重大的经济、财务问题包括 5 年内发生的以下行为，但不仅限于此：
- 出现三次欠债不还；
- 根据各地的相关标准，有过多的债务。
- 根据员工个人访问账户信息和交易数据的权限的不同，可采用不同的犯罪和经济问题记录标准。各机构还可以通过对雇员其他背景情况的调查来权衡该雇员是否满足机构对安全性和工作技能方面的要求。

2．2．3　道德标准

为了避免利益的冲突，并确保公司的道德水准，应当建立一套符合机构账户信息与交易安全管理相符的道德标准。同时，要对工作在重要敏感位置的雇员进行监控，以确保他们遵守道德标准。

2．2．4 对在职员工的管理

帮助在职员工解决可能导致潜在信息安全危害的个人问题，在发现员工出现赌博、经济困难等问题时，为他们提供帮助。

2．2．5 对前雇员的管理

为了防范前雇员对账户信息与交易数据的非法访问，要做到：

- 在雇员被开除、退休、辞职或以其他任何方式离职时，应立即停止雇员的所有访问的权限。不要将该人的用户名转给别人使用。
- 收回该雇员的所有门禁卡、胸章、钥匙、访问控制标识和其他与安全相关的物品，包括其他公司或机构提供的设备。

2．3 审计

审计是根据以往的经验来发现安全隐患，并对相应的风险控制手段进行评估以降低损失的一种措施。成员机构的内部审计是指在机构内部建立的一种独立的评估体系，该体系用于检查和评价机构的服务行为。内部审计的目的在于协助各成员机构有效的履行其职责。最终，内部审计将向相关机构提供一系列的分析、评价、建议、和审核报告。信息安全审计人员应该：

- 评估检查某机构账户信息和交易数据安全管理控制措施；
- 随时和信息安全官员及其他相关人员就安全隐患和风险的识别、现存

和新的产品风险控制措施是否完善等问题进行沟通；

- 在权衡需求与成本的前提下，向管理层提出客观的安全管理措施和改良建议；
- 检查审核记录的保留与信息记录是否完整。

2．4　数据安全知识的普及教育

进行数据安全知识普及教育的目的在于更有效地保护账户信息和交易数据安全。各机构的管理层应不断加强安全普及工作，从正面影响雇员对账户信息和交易数据安全的态度。数据安全教育应考虑不同层面的员工的具体情况和工作上的不同需要。为了有效地普及信息安全知识，信息安全官员可采用多种途径，如影像宣传（电影，预先录制的录像，张贴画），内部通讯或研讨会，一对一的交谈等适当的方式。注意正面的教育通常是最有效的。

第三章 访问控制

访问控制主要包括逻辑访问控制和物理访问控制。

3．1 逻辑访问控制

3．1．1 用户名（USER ID）管理

建议使用以下措施管理用户名：

- 如果某用户名连续 90 天未被使用，应将其冻结；连续冻结 30 天后应删除这一用户名.但是如果用户名只需要每隔几个月才使用一次，可以适当延长冻结的期限。
- 注意对预设用户和密码的管理。多数操作系统和安全管理软件中带有软件开发商预先设定好的用户名和默认密码，以便于安装、更改或删除软件的一些功能，也便于对其他用户的访问授权。成员机构、成员机构的代理机构或商户必须指定专人进行预设用户的操作和管理，并在使用预设用户时更改其默认密码。
- 根据持卡人是否会再次使用 USERID 来决定是冻结还是终止已注册的用户名。

3．1．2 静态密码管理

为了减少获取或者猜出密码的机会，建议使用以下规则来管理静态密码：

- 密码长度不少于 6 位
- 密码必须在 90 天内更改一次。如果密码没有在 90 天内更改，应将该用户名冻结。持卡人的密码不需要作周期性更改；
- 密码不可共享，或被他人，包括管理人员在内的人知道；
- 使用者不能选择容易被他人猜测到的密码（如名字或者与名字相关的代码、电话号码、日期、常用词汇或数字等等）。访问系统时使用的密码必须同时包括数字和字符；
- 禁止记录密码；
- 密码在传输时必须进行加密。
- 为保证静态密码的完整性：
- 在新的密码生效前使用用户的当前密码；
- 对密码的保存要进行不可逆加密；
- 禁止在输入，报告密码时，或在其它任何媒体上显示密码；
- 在收到更改密码的请求后，如果使用者不知道原始密码，需要采用强鉴别法对用户进行识别。

3．1．3 动态密码管理

确保在使用动态密码系统时进行合理的验证：

- 选择适当的需要激活的身份验证标识，这样的身份标识可以是可更改的个人识别码（PIN），也可以是生物识别数据。
- 用户的个人识别码（PIN）和用户名（USERID）不能相同；
- 严禁共享个人识别码验证标识；
- 个人识别码的长度至少为 4 位；
- 产生的密码长度至少为 6 位；
- 随机产生的密码只可以使用一次；
- 产生的密码不能被轻易地猜出；
- 密钥及其他验证用的重要信息应在标识上加密，并存在相应的系统中；
- 安全标识不能被复制和篡改；
- 做好对安全标识的库存管理；

- 当雇员工作职责发生变化或雇佣关系解除时，要及时收回安全标识，或者终止赋予该安全标识的准入权限。

3．1．4 登录系统（Sign on）的限制

为了及时发现未授权的登录企图，应当对每个授权人最后一次登入的时间和日期及不成功登入的次数进行记录。

为了防止未授权登录，应该：

- 在最多 3 次连续失败登录后，冻结该用户名.
- 将验证的最长时间设置为 5 分钟，如果超过设定时间，系统自动中止用户的登录。

3．1．5 工作暂停保护

为防止非法使用已和系统连接的终端，在出现一定时间的工作暂停时，如果要继续执行操作，需要对使用者进行重新识别和验证。

3．1．6 警告信息显示

为了警告未经过授权的使用者的行为可能导致的后果，应在使用者登录后显示警告页面，以指明未授权登录的行为需要承担的法律责任。

3．2 审核记录

审核记录是用来重新整合案件和确定责任的访问活动的记录。审核记录中信息对于问题的调查至关重要，它主要包括以下内容：

- 企图非法登录；
- 企图同时登录；
- 更改安全要素；
- 各机构应及时调查和报告可疑的行为，并：
- 定期检查审核记录信息；
- 调查和报告异常情况；
- 根据业务需求保留审核记录，保留时间不少于 6 个月。

3．3 访问权限的变更

为了保证信息处理系统的完整性，必须加强对访问权限变更步骤的管理。访问权限变更的步骤包括对访问硬件权限的更改、访问系统权限的更改、使用软件权限的更改、对手工处理程序的更改以及应急更改。

为了防止未经授权的变更，在任何时候、任何情况下应该严格遵守访问权限变更步骤。访问权限变更步骤应当：

- 建立规范的更改请求和授权程序；
- 每次更改后都应建立相应的测试和系统受理程序；
- 要求所有的变更都应按计划实施并保留相关纪录。

紧急变更

在紧急情况下保证系统的完整性，应当

- 只有在解决生产问题时才能采用紧急变更方式；
- 尽快恢复正常变更程序；
- 记录紧急支援人员变更情况；
- 审核所有的紧急变更记录。

3．4　物理访问控制

存储和处理账户信息和交易数据的设备应安装在物理安全的环境下。安全设施可用来控制对数据的物理访问，以保护信息和信息处理设备的安全。为了防止电脑和数据处理中心受到物理攻击，应考虑以下安全措施：

- 采取措施以防范逃避验证身份的行为，如：

— 若以前曾经发生过逃避验证的情形，就应当实施更为严格的验证程序；

— 当安全装置被破坏或失效时，如发生安全门被打开或者门窗遭到破坏等情形时，应发出报警信号；

- 拥有大型信息处理中心的机构应对所有访问信息处理设备的行为进行录像，作为控制物理访问的附加审核记录；
- 监控机构内部所有的计算机设备的进出情况；
- 防止未经授权进入存放信息处理设备的房间或区域。所有的墙壁、天花板、门窗和地板都必须坚固，并能防止逃避身份验证的行为发生；
- 建立并向员工宣传相应的安全控制流程，以便于员工对已出现或者可能出现的违反物理安全的行为迅速采取行动。

进入物理安全限制区域之前，应该验证来访者的身份。来访者必须有合理的理由才可进入安全限制区域，并在授权的条件下才能访问账户信息和交易数

据。

应当对设备和存储数据的载体进行库存登记。

重新使用任何设备或载体之前，要清除它们原来存储的所有数据。

3．4．1 不经意泄漏信息

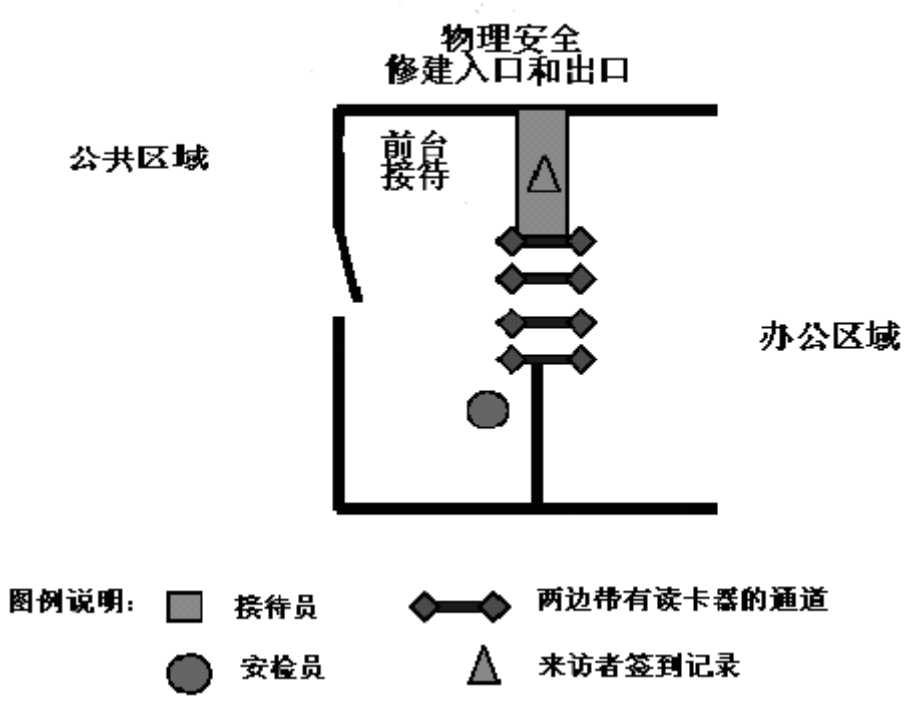
为尽可能减小账户信息和交易数据在电脑终端屏幕泄漏的可能性，显示器应安装在未授权人看不到的地方，否则需要安装隔离屏障。

3．4．2 员工工作环境

井井有条的工作环境可以减少盗取账户信息和交易数据的机会。应当将为持卡人和为商户服务的员工安置在不同的工作限制区域。在限制区域内，不允许出现雇员的私人物品，如公文包和钱包等。除非对工作有特别的要求，通常情况下不要让雇员有复制账户信息和交易数据的工具，如：钢笔，铅笔和复印机、打印机、照相器材等。

3．4．3 门禁的修建

修建门禁为授权人员访问存储在办公区域和数据中心的账户信息和交易数据提供了第一步安全保障。下图阐明了修建门禁的最佳方案：

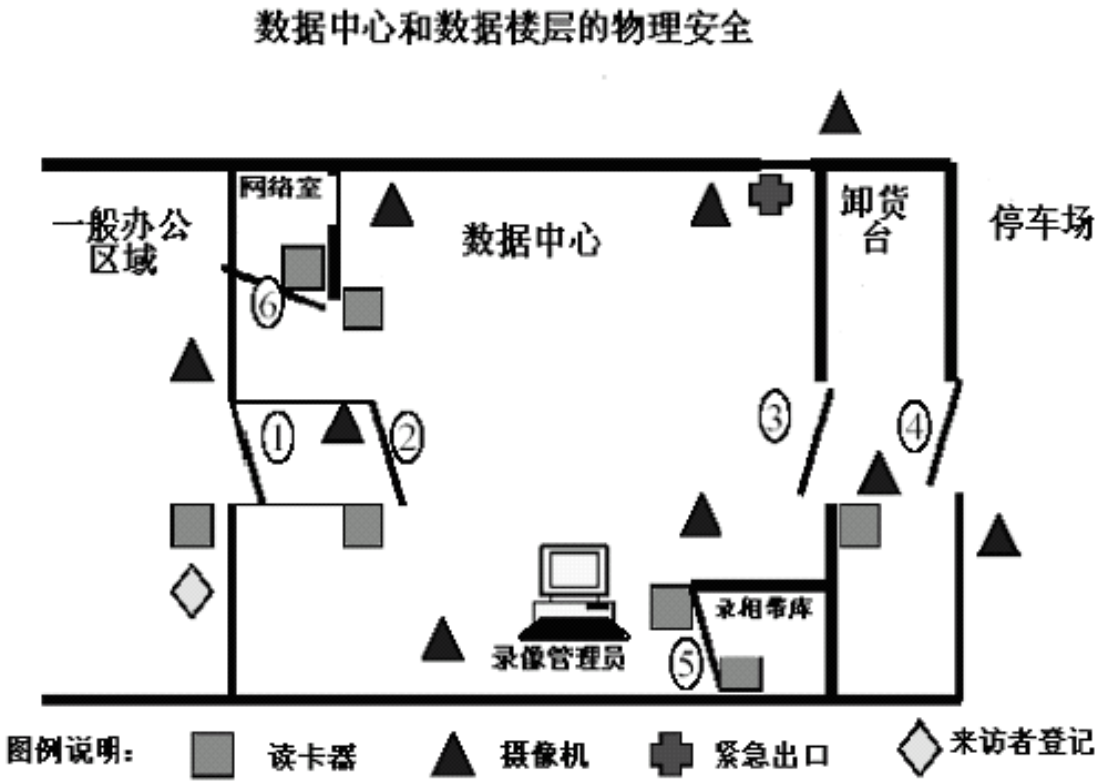


雇员和定期来访者应在进出通道时使用有效门禁卡。对于小型场所或者多门的大型场所，可用门作入口通道。在这种情况下，要采取措施防止多人使用一个门禁卡进出，这些措施包括对员工的教育和超时强制开门报警。

来访者必须登记。前台接待员应联系内部受访者并安排双方在接待区域见面。内部受访者在同意来访者进入后应在来访记录上签字。来访者应随时佩戴标有“来访者”的证件。离开时，来访者应签离。对于进入数据中心或其他重要安全限制区域的来访者，其证件（驾照，身份证，工作证）应先存放在入口处，离开时才可取走。

3．4．4 数据中心/数据楼层安全

数据中心存放着处理账户信息和交易数据的电脑设备。这些设备的物理安全对于保护账户信息和交易数据的安全至关重要。下图显示了数据中心安全的最佳布局。



所有数据中心的来访者必须登记出入并有人陪同。登记记录应包括进入者

姓名、来访时间、离开时间和陪同者等信息。

在出入时必须验证每个人的身份。最常见的验证方法是使用门禁读卡器来辨别身份。没有保安人员的通道的门禁系统持续开放超过 30 秒钟，必须安装开门报警装置以通知保安人员。

其他通道，如窗户、爬行通道等必须具有非法进入报警功能。

所有进出通道必须安装录像监控设备，以协助辨认进出人员。摄像装置应安装在能够记录出入人员面部和上身的地方。

办公区域出来的第一个入口（号码 1）处的读卡器要对已授权人员的通行证进行验证。进入第一道门后，安全保卫人员在打开第二道门之前，应通过影像设备核实通行证上的照片和持证人的相貌是否相符（号码 2）第二道门应由保安打开，从外（号码 1）到内（号码 2），每次只允许一个人进入。

必须记录从任何门进入数据中心的设备的序列号。任何机具在从数据中心搬走之前必须得到管理部门的同意。每次设备的进出都必须由同一个人负责。安全人员在机具搬走之前必须核对设备的序列号。

数据中心内应有封闭的储藏室用于保存敏感性更高的数据（号码 5 和 6 处）。可移动的数据存储载体，如磁带等，在不使用时应保存在只有授权人员才能进入的储藏室（号码 5）内。成员机构可指派专人来管理磁带的更换、收藏和再使用，因为即使磁带已过了有效期，磁带和其他可移动载体所存储的账户信息和交易数据仍有可能用于欺诈活动。由于磁带管理员经常接触存储敏感数据的可移动载体，其工作间最好设立在数据中心内，这样可以减少非法获取或不经意地泄漏数据信息。

数据中心的卸货门（号码 3 和 4）不能同时开启。无论使用那一道卸货门，在卸货时都应该指定保安人员来监管。

按照有关建筑部门的规定，数据中心必须有紧急出口用于紧急疏散。紧急出口在被开启的时候，警铃和报警信号应立即传到安全监控部门。在紧急出口的位置应安装摄像机以记录下所有出入的人员。

数据中心的以及与数据中心相邻的楼层的墙壁、地板和屋顶应使用结实坚固的材料修建，以抵挡对数据中心的非法暴力入侵。有些情况下，如安装通风设备等原因，不可能将墙、地板和屋顶做成一个整体，因此需要在相关的位置

安装结实的防盗网。

第四章　系统管理

4．1 对网络的管理

网络整合了信息处理和传输的设施以协助计算机之间或个人之间的相互访问和信息传递。网络可以是两个单机的连接，也可以是复杂的全球性的、多机构相连的支付授权网路。本章主要描述如何保护网络的完整性和安全性。

供货商入网

供货商入网是指供货商通过公共或者私人网络访问信息处理设施。

为确保供货商入网时不危及整个系统的安全，除了采取一般的安全控制措施以外，还应注意以下几个方面：

- 与供货商签署安全合约并确定各自的角色和职责。
- 建立入网“准入”制度，并由授权人员监控入网和使用的整个流程。在工作完成之后，应立即中断网络的连接。
- 对每个供货商的入网审核记录进行审核。

网络设备

为了防止非法使用网络资源和系统设备的运行中断， 应该做到：

- 通过权限设置来控制对系统设备的访问。
- 将系统设备安置在物理安全的环境下。
- 要对配线室进行安全控制，只有授权人员才可进入。
- 对系统设备的库存进行登记。

系统监控

为了防止监控设备泄露、篡改或销毁记录的数据信息，应对网络中传输的数据进行监控和记录，如使用网络协议分析仪或者其它的诊断设备，但是这些设备的使用必须经信息系统安全管理员或信息安全官员的批准。

犯罪分子可通过网络非法访问电脑资源和数据信息，要对网络系统进行监

控以防止罪犯对系统和电脑资源的攻击。为了尽可能地减小系统遭受攻击的可能性，最好对系统进行实时的，而非周期性的监控。

4．2 对软件的管理

保证软件的完整性是至关重要的。从某种程度上说，由于软件是一种无形资产，一般看不见、可被多次复制并且以多种形式存在，因而对软件安全的控制比对系统设备的安全控制更具有挑战性。应实施下列控管措施以保护软件和软件所处理的数据信息。

4．2．1 应用软件的使用

应用软件是指能够完成一项或多项功能的软件包，如转账、账单管理或者逻辑访问控制等。为了防止在使用应用软件时非法改动、泄露或销毁账户信息与交易数据，应该注意：

- 把应用软件安全和操作系统访问控制系统集成在一起，由操作系统访问控制设备来维护用户名和密码，这样可以使用户名和密码的管理标准化，也可以更有效审核审核记录和报告风险状况。
- 对重要的交易实施双重控制。

4．2．2 应用软件的测试

应用软件的测试用于检查新的或修改过的处理系统能否正常的工作。为了防止账户信息和交易数据在应用软件测试中被泄漏和被不恰当地处理，应采取以下措施：

- 签署相关协议，以控制账户信息与交易数据信息在测试中的使用范围。明确规定只有授权人员才能重新安装、更改、重新命名被测试文件或文件名；
- 在测试前，应先将账号、姓名等被测试数据的一个或多个敏感域值进行修改，以保护真实数据的完整性和安全性。应当保证最终的测试结果不应当与客户任何的真实账户信息与交易数据相关联，同时应采取相关控制措施以确保不会对生成的测试信息产生任何误解；
- 安全地处理测试后的数据信息。

4．2．3 软件的缺陷

为了减少软件中潜在的缺陷，要求采购软件时应选择有一定声誉和良好记

录的供应商。供应商必须确保提供足够的资源和保险以弥补使用他们的软件时可能带来的破坏。除了通常的安全控制措施以外，还应该注意：

- 建立软件质量保证机制；
- 对所有自行开发的软件必须保留完备的文档和严格的测试、验证。

4．2．4 软件病毒

为了防止数据由于病毒的入侵而被更改、泄露或销毁，应当采取以下措施：

- 严格限制下载和使用免费软件或共享软件；
- 严格限制访问公共网站和接收外部电子邮件；
- 在出现病毒感染后，要通过厂商、同事和反病毒交流栏目寻求帮助；
- 安装并及时更新防病毒软件和软件补丁。

4．2．5 软件检查

为了保证软件的完整性，需要对安装的软件进行定期检查，以判断是否有未授权使用的软件装入系统。

4．2．6 提供给顾客的软件

为了防止提供给顾客的软件被非法破坏或更改，应当采取措施保护存储顾客软件的软盘、磁盘和 CD 等载体的安全。这些措施包括对硬件、软件、软盘、磁盘和 CD 等在生产、复制的过程中以及对母带的保护等方面的物理及逻辑访问控制。

4．2．7 卡号屏蔽

在显示、打印交易凭证时，尽量做到只显示部分账号，这样既可以让持卡人知道并确认使用或将要使用哪一张卡进行交易，同时又不会完全或者大量暴露账号信息。注意在发给持卡人的月账单或者年账单上也只打印部分账号信息。

无论何时，成员银行的代理商和商户的员工只可以接触部分账号信息。在保证是账号不被猜出的前提下，部分账号可以是账号的任何一部分，但通常是卡号的倒数第二至第五位数。

4．3 Internet 数据库的保护

通常情况下用户可通过 Internet 访问账户信息和交易数据库中的数据。下面的示图描述了如何保护可被消费者访问的账户信息与交易数据的安全。为了有效地实施《规则》中的要求，只限有业务需要的人员访问账户信息和交易

数据。下面的示图从概念上说明了如何限制对网络系统的访问。在限制访问网络的同时，还应当采取措施限制对服务器的访问。

4．3．1　电子商户

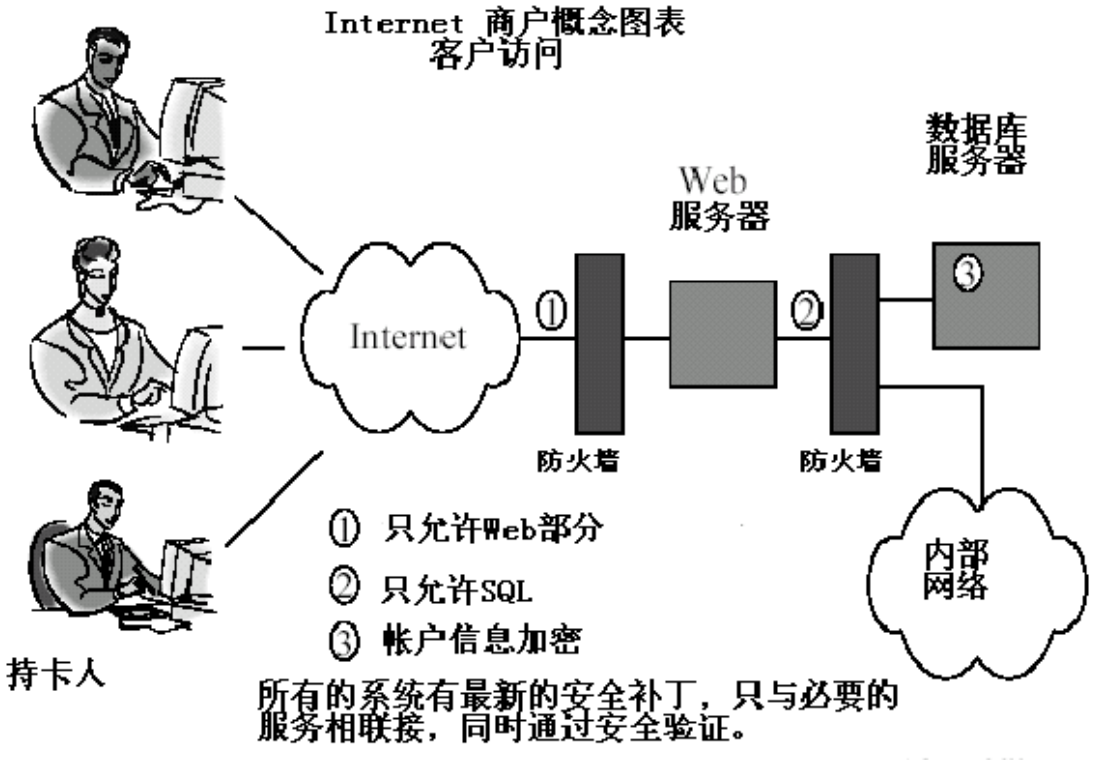


图 4－3

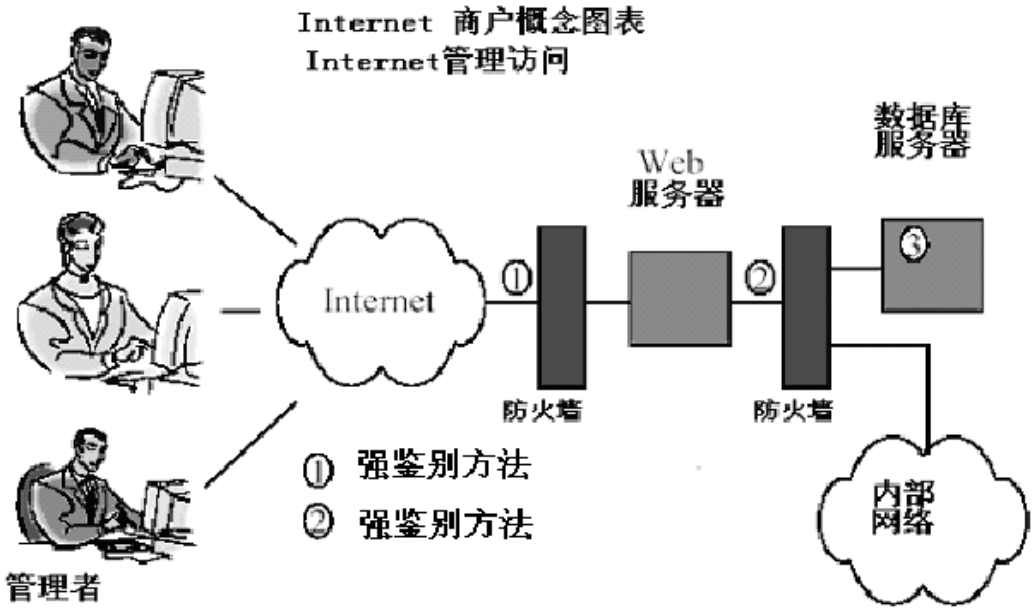


图 4－4

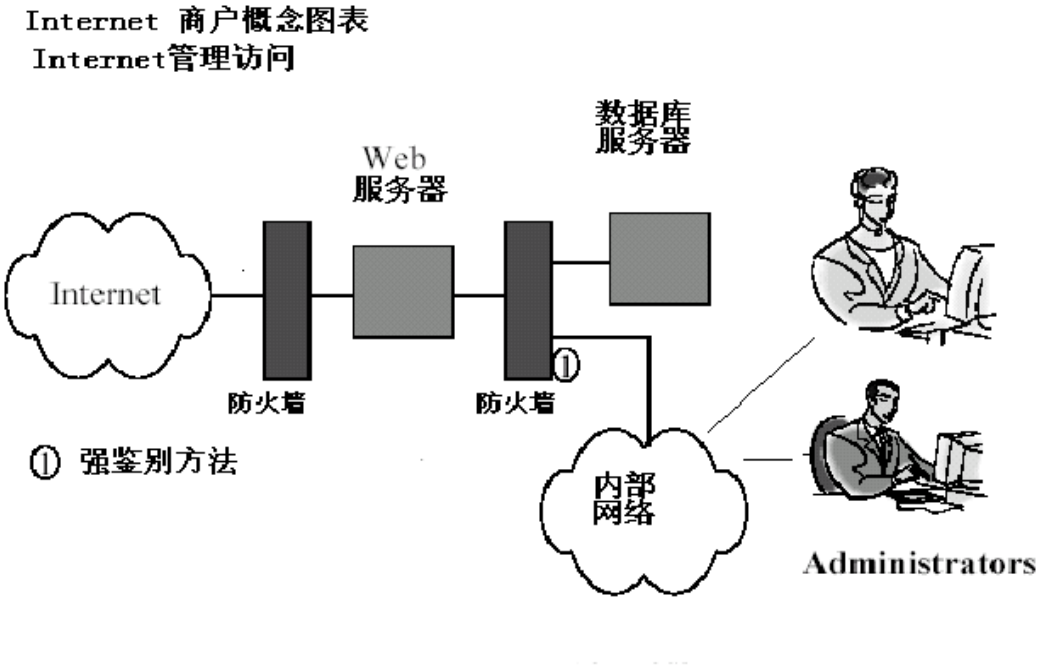


图 4－5

图示中的强鉴别法（Strong Authentication Mechanisms）包括动态密码

系统，生物鉴定和管理完善的数字证书。

第五章 合约管理

成员机构与商户或者服务代理机构签署的合约中应包括以下内容，但是成员机构可根据具体情况进行修改和补充。

- 商户和服务提供机构应保证只将持卡人姓名、账号或其他相关交易信息，包括凸印在卡片上的、写入磁条中的信息，用作与协助商户或服务代理机构完成与交易相关的业务，而不用作其他目的；
- 除了银行、金融机构或者指定的代理机构之外，商户或者服务代理机构保证不向任何其它第三方透露或提供持卡人姓名、账号或相关的交易数据，这些交易数据包括凸印在卡片上的、写入磁条中的信息，也包括以任何其他方式出现在卡片、文件、表格上的信息；
- 商户和服务提供机构同意保存持卡人姓名，账号和交易信息等记录，这些记录包括但不只限于买卖凭证、交易收据、买卖租赁合约和使用过的复写纸。只有经过授权的人员才能在安全范围内访问这些记录。在丢弃这些资料时，要采取妥善、安全的方式销毁废弃资料；
- 商户和服务代理机构应当按照《银联卡账户信息与交易数据安全管理规则》中有关“账户信息与交易数据”的定义，保护账户信息和交易数据的安全，并且承诺对不遵守《规则》要求的行为承担相应的责任。
- 商户和服务代理机构应积极配合成员机构或者中国银联对这些机构和对与他们签约的机构的交易处理设备及场地进行的检查；
- 商户和服务代理机构只允许符合《规则》要求的机构拥有、处理、存储和访问账户信息和交易数据。商户和服务代理机构必须和这些机构签订合约，要求他们保护账户信息与交易数据的安全信息。商户和服务代理机构需要实地检查该机构以确保他们符合《规则》中的要求；或要求其通过中国银联进行认证，确保其符合《规则》的要求。

第六章 交易受理

银联卡交易可通过多种方式受理，包括商户的 POS 机具、手工压印设备、

网上交易、邮购、传真和电话。上述每种受理方式都可能泄露持卡人的账户信息与交易数据信息。遵循本章所述的内容可以降低信息被盗的可能性。

本章对保护 POS 机具的安全提供了具体操作指南，其主要目标是：

- 减少 POS 设备被非法改造用于欺诈的机会；
- 减少通过 POS 机具盗取保密或敏感数据的机会
- 针对 POS 机具设计、发展、布放和操作的各生命周期环节，建立一套行之有效的“最佳指南”。

6．1　POS 设备和处理要求

本节对于 POS 机具和收单系统的设计和开发提供安全指南

6．1．1　敏感交易数据的保留

POS 机具和收单行系统应该只存储用于卡交易清分所必需的最基本的交易数据。特别是 POS 机具不能存储或显示磁条（道）的所有数据、CVC/CVV 数据和其他被收单机构限定的个人磁条数据。

6．1．2　对敏感交易数据的打印

账号和有效期只能部分显示或打印（卡号屏蔽），其它所有磁道信息不能显示和打印。本指南极力建议 POS 机具不打印出商户全称或终端认证号。

6．1．3　敏感数据，参数和功能的访问

只有授权人员能够访问存储在 POS 机具和收单系统里的参数和敏感交易数据。

POS 机具通常有两个密码：一个是“系统密码”，用来控制 POS 机具功能的改变和终端的设置，另一个是“管理员密码”，用作使用 POS 的功能权限设置。

由系统密码控制的功能应包括：

- 初始软件的下载；
- 通过键盘修改终端参数（如果允许）
- 与 POS 机具功能相关的其他系统（如诊断等）

由管理员密码控制的功能应包括：

- 作废/退货
- 清算
- 参数初始化下载

在安装前要对系统密码默认值进行修改。

应由商户来设定管理员密码。为了加强安全性，磁条卡或 IC 卡在使用时也应该使用密码。

6．1．4　POS 机具的序列号码

用于确认卡交易所使用的终端 POS 机具序列号应写入机具的硬件或固件中。这样可以减小测试时非法修改 POS 机具序列号的可能性。

6．1．5　对收单系统的访问控制

POS 机具的收单系统只将真实交易数据传入系统。收单系统至少需要验证机具和商户识别码的真实性。一般情况下，收单系统应验证 POS 机具初始登记的电话号码的有效性，一旦不匹配，应立即提交报告以便展开调查。

6．1．6　对 POS 机具和 POS 机具供应商的选择

（1）对供应商和分销商的选择

- 对 POS 机具提供商和分销商的选择应注意：
- 对公司的所有权的核查；
- 对财务状况的核查，以确保该服务商财务状况良好。
- 审核时应具体包括以下内容：
- 每年的财务报告和公司所有权情况；
- 供应商/分销商物理安全情况，特别是与机具存放相关的情况；
- 提供的运营服务（如商户培训）、 服务等级和流程；
- 数据安全；
- 书面报告和库存清单。

（2）与供应商和分销商的合约

收单机构和 POS 机具供应商/分销商应签署具有法律约束力的合约。合约应涵盖下列信息：

- 购买设备
- 开发应用软件
- 机具的安装和定制
- 机具的维护
- 交易的处理

合约的条款应在各方参与的有法律约束力的合约中体现，主要包括以下方面：

- 供应商/分销商提供的服务
- 每次服务的具体细节（软件的开发、设备的初始化、设备的安装、商户的培训、维护，包括约定的服务标准等）
- 物理安全标准和流程
- POS 设备的安全
- 数据安全
- 能确保雇佣可信赖的员工的招聘制度和过程
- 保密协议
- 终止政策
- 责任条款

成员机构应定期对 POS 设备的生产厂商/分销商进行实地考察，以确保 POS 相关功能的安全运行。

（3） 对 POS 机具设备的安全要求

POS 机具的安全机制的复杂性和类型由多方因素决定，如机具的使用年限、机具的成本、机具所采用的技术(磁条卡/IC 卡)、 收单系统对 POS 机具的支持等等。为了帮助参与各方设计、开发和挑选 POS 机具，以下列出机具的最低安全要求清单：

- 严禁显示，存储和打印敏感数据；
- 严禁通过键盘输入账户信息；
- 终端参数的变更；
- POS 机具功能的保护（使用密码）
- 源代码的保护

6．1．7 POS 机具的开发

收单机构在开发 POS 机具时，应考虑下列事项：

（1）需求书

POS 机具设备需求书应由相关各方共同签署同意。POS 机具的技术细节，尤其是与安全相关的信息应列为机密，必须严格控制。

（2）POS 机具的开发

POS 机具的开发（包括硬件、固件和应用软件）应该：

- 遵照行业开发标准；
- 核查任何与安全功能和特征有关的程序或软件代码。
- 正式使用前应防止对机具的未授权修改。

（3）源代码

严格控制对 POS 机具源代码的非法修改。源代码只可以提供给供货商/分销商的授权人员或成员机构授权的机构。

（4）机具的检验和测试

POS 机具在安装前应进行测试检验，以确保符合需求书要求并能正常操作。收单银行或指定机构应对 POS 机具的检验和测试负责。

6．1．8　POS 机具的设置与安装

以下描述在安装和设置 POS 机具时需要考虑的安全要求。

（1）责任

总体上由收单机构负责完成 POS 机具设置与安装工作。POS 机具的安装通常涉及装载相关的商户特别参数，如商户和终端认证号、商户名称、地址等，或者收单系统参数，如主机号码等。这可看成是对 POS 机具的格式化或初始化。

如果供货商，经销商或第三方提供这一服务，初始化的程序、责任和义务，特别是对敏感信息的处理应明确写入正式的合同中。

（2）POS 机具的初始化

POS 机具应在主机终端管理系统工作正常的状态下初始化。初始化和格式化的参数直接记入终端管理系统然后再下载到各 POS 机具中。这样可以确保更好地实施安全控制流程，同时确保只有授权人员才能访问敏感数据和使用相关功能。系统安全设计应考虑：

- 用户的访问控制（用户的姓名和密码）；
- 用户访问等级控制（用户和各级管理者）；
- 对敏感数据的访问控制（数据库的操作系统控制）；
- 记录用户访问和使用系统的情况，并记录 POS 机具的参数/编码的改动情况。

指南建议所有对 POS 机具的改动都应通过终端管理系统来控制。敏感参数，如商户/终端认证号或收单机构主机电话号码，不能由 POS 机具的键盘来改动。POS 机具的功能只限于通过连接主机来要求更改参数和软件。如果无法实现，参数的更改则只能由授权人员使用系统管理密码来控制。

（3） POS 机具的参数和数据安全

收单机构应在发放、下载、保存和销毁数据的整个过程中，加强对商户和系统设备的敏感数据，如收单机构主机电话号码、终端和商户识别码等各级数据的安全管理。

（4） 设备的物理安全控制

无论在安装前还是安装后，应加强对 POS 机具的布放、存放和安装的管理，以减小机具被盗窃和被非法修改的可能性。物理安全控制具体包括确保机具从工厂到经销商、到分销商、到收单机构都存放、在安全的环境中存放。在撤回或置换机具时也应当有同样的安全要求。应保留一个详细的机具存货目录，以便于对机具从出厂到最后销毁的全程跟踪。

6．1．9 POS 机具的使用和维护

（1） POS 机具的使用

只有被收单机构批准使用的 POS 机具才可以处理卡片支付交易。另外，任何与处理支付交易相关的机具改造都应征得成员机构的批准。

银联卡不能在未经批准的机具上使用，未经批准的机具也不能显示、印制、储存和处理卡片信息。

被批准使用的机具和安全操作要求应在收单机构的商户合约中明确，并应包括在商户的初次和后续培训中。

（2） POS 机具的维护

收单机构、商户和第三方处理机构应对机具维护达成一致意见，并形成正式合约。这些责任和流程的内容应包括在商户合约及供应商合约中。

维护人员在工作时应持有效工作证件（或穿工作服）以确保只有授权人员才能更换或改动已安装的机具。

为方便商户向收单机构报告机具的维护和升级时出现的任何可疑行为，应建立电话确认制度。这一内容应规定在商户合约中，并包括在商户初次和后续

培训中。

如果需要更换或改动任何预定的机具，收单机构或其代理机构应提前通知商户。

用于监控/确认机具维护或设备升级/改动的报告应定期产生。

（4）对硬件和软件的清查

收单机构负责对所有 POS 机具硬件的库存登记造册并保证其准确性。这项工作可以外包给第三方处理商、经销商或分销商，但必须定期确认和审核外包情况。库存清单的复印件应由收单银行保存。

库存清单主要用于对所有 POS 机具从运输、储存、初始化、安装、运行、维护和销毁的整个过程进行跟踪。

库存清单应包括 POS 终端、打印机、密码键盘。如果由商户拥有和操作机具，也应该保留库存清单。

机具库存内容应至少包括下列内容：

- 硬件打印设备（终端，打印机，密码键盘，ECR 等）；
- 物理或逻辑的机具序列号；
- 机具的布放点（商户名称和地址）；
- 机具的软件型号；
- 如果可能，还应包括下列内容：
- 安装日期
- 机具的基本功能（只可以授权，EDC，支持芯片卡等）
- 分享信息（如果与其他成员机构或组织共享）
- 其它功能（如支持延伸服务代码、在线功能等）

（5） POS 机具的更改和升级

机具更换、硬件升级、软件/参数升级或更改 POS 操作方式等等都应按照 6.1.8 节中规定的方式加以管理。

6.2 邮购

商户可通过各种方式（包括邮购服务）受理定购和银联卡支付。邮购服务提供商可采纳以下建议：

- 建议商户收集和整理所有含有持卡人信息的文件，如订单格式，复写

纸等；

- 含有持卡人资料的数据必须在规定区域内处理，只允许经授权的雇员接触文件。

6.3 传真

商户可通过传真方式受理定购和银联卡支付。通过传真受理定购和支付的商户可参考以下建议：

- 如果接收传真时涉及到持卡人账户信息及交易信息，就应将传真机放置在只有授权人员才能进入的指定区域。
- 收集和整理所有含有持卡人信息的文件，如订单格式，复写纸等
- 必须在指定区域内处理包含持卡人资料的文件，只允许经授权的雇员接触文件。

6．4 电话

商户可通过公共电话服务受理定购和银联卡支付。提供电话定购服务的商户可遵循以下建议：

- 确保电话客服人员询问来访者相关的持卡人信息。客服人员应按照经管理层核准的规则进行工作。
- 定期进行电话通话监控以减少风险，并确保客服人员没有获取超过交易需要的持卡人信息。
- 建立有效措施以控制持卡人信息被转录为硬拷贝形式，必须有人对这些拷贝负责。
- 所有文件保存在限定的区域内。

第七章 风险事件处理流程

7．1 处理流程要点

在科技快速发展的当今世界，单纯地加强内部网络安全管理已经不能有效地防止机构内部或外部受到攻击。因此，对于每一个机构而言，建立一套完善地、系统地数据安全风险事件应急处理流程是非常有必要的。这样可以有效地处理和恢复风险灾难，减小灾难可能造成的损失。

本节将主要介绍数据安全风险事件应急处理流程架构。应急架构可分为 7

个阶段：

第一阶段：准备阶段

建立数据安全风险事件应急处理团队。应急处理团队的任务在于迅速处理各类数据安全风险事件，以减小风险事件对本机构业务运营造成的影响。

第二阶段：风险识别

风险事件的发生是不可预知的。但是可以通过一些异常现象，如可通过分析日常系统操作行为发现风险事件的发生。

第三阶段：评估阶段

当识别了风险事件以后，需要对该事件进行评估，以确定该风险事件是否确实存在。评估包括确定事件的范围、影响程度和造成的损害等等。

第四阶段：控制阶段

为了减小风险事件给机构造成的损害和隔离被攻击的系统，需要对风险事件进行控制。

第五阶段：隐患根除

为了彻底根除风险事件隐患，风险事件处理团队需要决定造成数据泄漏的原因。

第六阶段：灾难恢复阶段

灾难恢复阶段是重新安装被损坏的系统，以使业务能正常开展。在系统恢复运行之前，必须对系统再次进行检查，以保证类似事件不会再次发生。同时，必须对系统进行全面监控，以及时发现攻击者的再次入侵。

第七阶段：事后跟踪阶段

对发生风险事件的系统进行事后分析，以了解造成风险事件的系统薄弱点和潜在的隐患。如果需要收集证据以采取法律的手段惩处罪犯，建议请求法律部门专家参与，以妥善保护保护电子证据。

7．2 数据安全风险事件的定义

根据美国联邦网络安全研究与发展机构 CERT/CC 的定义，数据安全风险事件是指：

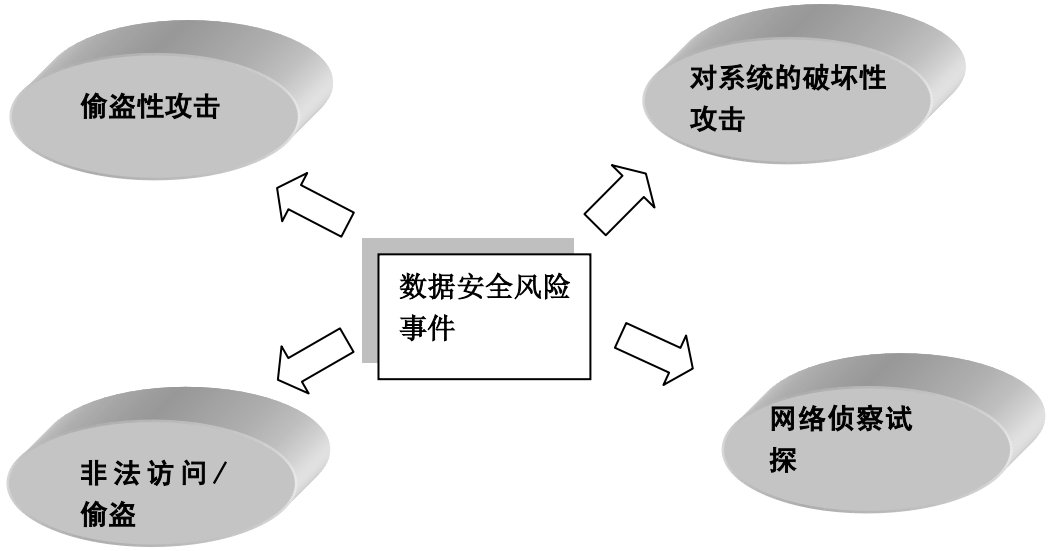
- 违反各类数据安全管理政策；
- 非授权访问的企图；

- 否认对数据资源的访问；
- 非法使用相关电子设施；
- 在未经系统持有者知道、同意的情况下，修改系统设置及数据。

对于各成员机构、成员机构的服务代理机构和商户而言，数据安全管理政策是指与《银联卡账户信息与交易数据安全管理规则》相关或者相配套的规则、实施指南。

7．2．1 风险事件的分类

数据安全风险事件可按下图分类：



1、偷盗性攻击

偷盗性攻击是通过病毒、蠕虫或文本文件等对系统的攻击。通过攻击系统，攻击者可以获取密码、账号等保密信息。由于病毒在侵入系统后会更改它们在系统的签名，因此偷盗性攻击通常很难被发现。为了隐藏未授权的攻击活动，一些病毒甚至会修改访问日志。

非法代码攻击的例子如下：

- ✓ 通过 Email 迅速传播的蠕虫或者病毒；
- ✓ 间谍代码（如 Caligula 病毒、Marker 病毒等等）；
- ✓ 远程控制代码（如 Back Orifice，NetBus 等）
- ✓ 协作攻击代码（如 Trinoo，Tribe Flood Network（TFN）等）

2、破坏性攻击

破坏性攻击是指攻击者使用某种工具造成网络、电脑系统停止运行，或者将系统中运行的重要程序删除的攻击。通常情况下，分布在不同区域的攻击者同时向某一主机系统发出攻击。由于攻击者可以从不同的网关进入被攻击的系统，因此一般很难跟踪到分布式破坏攻击的源头。在破坏性攻击中，DNS、Web 和 mail 服务器最容易受到攻击。

破坏性攻击的例子包括：

- ✓ 与 Email 相关的破坏性攻击（如 mail SPAM、邮件炸弹等）；
- ✓ 与服务相关的破坏性攻击（如 Slammer 蠕虫等）；
- ✓ 与网络阻塞相关的破坏性攻击（如同步洪水破坏性攻击、“Ping of Death”破坏性攻击等等）。

3、非法访问、偷盗

非法访问可以是非法使用系统登入保密信息，也可以是非法窜改存入系统中的文件和路径。非法访问还可以通过植入未授权的“偷窥”程序或设施，捕捉通过网络传输的其他电脑设备中的信息。许多电子商户通过使用 SSL（Secure Socket Layer）来保护通过网络传输的数据。SSL 提供服务器认证、数据加密和信息集成的功能。

内部信息泄漏一直是最常见、破坏性最大的盗取重要数据的方式。有组织的犯罪团伙通常通过发展各机构的雇员，以协助他们获取大量的账户信息与交易数据。

主要的非法访问方式有：

- ✓ 内部雇员盗窃机密信息；
- ✓ 使用前雇员的用户名访问系统；
- ✓ 使用特殊用途用户名或者密码访问系统；
- ✓ 为寻找机构网络系统、路由器或防火墙的安全漏洞而进行的访问。

4、网络侦察试探

为了掌握机构网络各部分的信息，攻击者往往通过侦测试探对系统进行攻击。侦测通常包括两个部分：主机服务器侦测和应用服务端口侦测。主机服务器侦测能发现网络中正在运行的系统；而端口侦测则能发现在系统上运行的服

务程序。

网络侦测攻击可能不会立即造成信息的泄漏，但它们是对系统进行破坏性攻击的信号。

网络试探攻击的例子如下：

- ✓ 服务器试探：SYN－FIN 扫描、PING Sweep、Directed Broadcast Pings。
- ✓ 接口服务试探：TCP 接口扫描、UDP 接口扫描

7．2．2 事件严重程度区分

对数据安全风险事件分类能决定事件的严重程度。事件的严重程度决定了应当采取什么措施来处理风险事件。风险事件严重程度可按以下五个级别分类：

- ✓ 非常严重级：事件的发生将严重影响人们的生活，并对机构造成不可挽回的损失，如大量磁条信息的泄漏；
- ✓ 严重级：这类事件的发生将会影响数据的完整性和机密性，使机构在业务上和信誉上蒙受损失，如大量的账号、有效期等数据的泄漏；
- ✓ 中级：这类事件主要影响数据的可用性，但不会影响数据的完整性，如收单网络出现故障；
- ✓ 低级：这类事可能会影响数据的安全性、完整性或可用性，但未造成数据的丢失。机构应当已经采取防范措施防止此类事件的发生，但仍需加强监管以及时发现任何非法的访问活动；
- ✓ 不明显级：风险事件给机构带来的风险可忽略不计。

当发生“非常严重级”和“严重级”的数据安全风险事件时，成员机构需向中国银联报告该事件。

7．3 风险事件响应与处理架构

建立数据安全风险事件响应与处理架构的目的在于向成员机构提供一套系统的风险事件应急处理机制，以协助各机构有效地处理风险事件，减小所发生的事件对业务正常运行造成的负面影响。在制定架构时，需要在风险事件发生之前预先考虑以下问题：

- ✓ 可能发生数据安全风险事件的区域；
- ✓ 可能受到影响的业务流程；
- ✓ 发生风险事件以后需要通知的相关部门和人员；

✓ 发生风险事件以后应采取的处理措施和行动；

✓ 处理措施和行动的具体实施步骤。

7．3．1 准备阶段

7．3．1．1 建立风险事件响应处理团队

数据安全风险事件响应处理团队应当由机构的管理高层和有经验的人员组成。建立风险事件响应处理团队的目的在于迅速控制、调查发生的事件，并实施灾难恢复。团队应当在高层的授权下，在危急时刻拥有决策权。在考虑团队成员构成时，处理事件所需要的资源和协助是主要的考虑因素。事件处理团队成员构成及职责见下表：

编号	风险事件响应处理团队成员	职责
1	管理高层	授权其他团队成员处理事件；同时，根据其他成员提供的信息进行决策。
2	信息安全	确定受害范围，实施基本的风险控制、证据收集和灾难恢复工作。
3	IT/信息系统管理	尽可能减小风险事件对系统终端用户的影响，为信息安全团队提供技术支持。
4	IT 审计	了解造成风险事件的原因，确保遵守信息安全管理流程，与信息安全和 IT 部门共同根除风险隐患。
5	保安	调查发生的物理破坏，收集物理破坏的证据。
6	法律	协助机构采取法律措施对付数据安全犯罪；对风险事件给顾客、公众等造成影响等责任问题，提供法律上的建议。
7	人力资源	在有内部员工参与作案时，需人事部门介入并提供相关的协助
8	公共关系	在与媒体或股东发布风险事件之前，与团队领导进行沟通，以准确了解风险事件发生状况及机构的立场。
9	财务审计	在索赔时，确定损失金额。

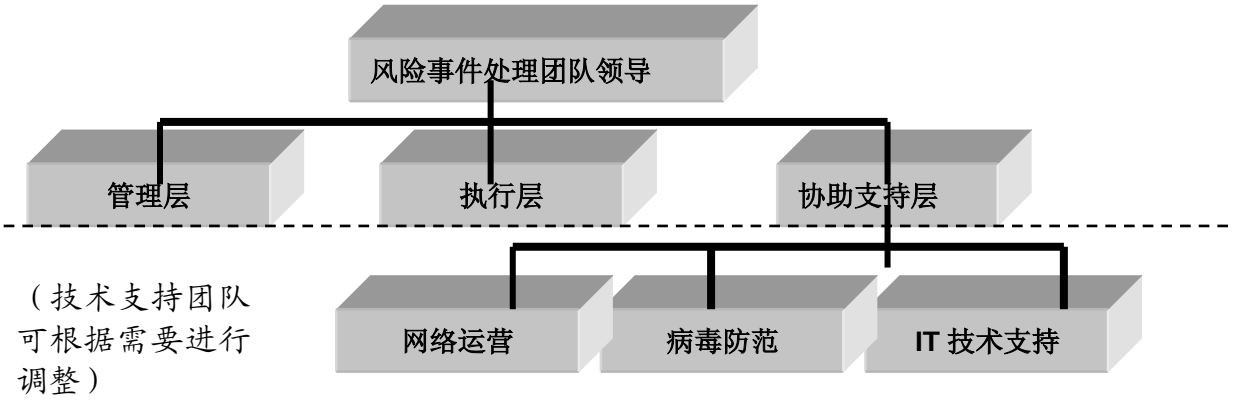
对于中小型机构，一人可以身兼多职，也可以外部咨询、服务机构人员。

7．3．1．2 风险事件处理团队的结构

风险事件处理团队可由三部分组成：管理层、执行层和协助支持层。

管理层	执行层	协助支持层
机构管理高层	IT/信息系统管理	人力资源
信息安全	保安	公共关系
IT 审计	IT 审计	法律
财务审计		IT/信息系统管理

管理模式如下图：



管理层的职责

- ✓ 决策、修订数据安全管理措施；
- ✓ 就数据安全风险事件的技术细节向管理高层或者董事会转达；
- ✓ 检查测试风险事件响应处理程序有效性和可行性的测试结果，并提出指导性建议；
- ✓ 协助相关部门开展工作；协助调配相关软硬件资源；
- ✓ 对相关事件和行动进行备案；
- ✓ 参与组织相关人员的培训；
- ✓ 掌握可能发生的突发事件，并制定相应的突发事件应对计划；
- ✓ 总结经验教训，及时更新风险事件应对流程。

执行层：

- ✓ 检查系统及其运行环境，确保系统安全；
- ✓ 控制风险事件的进一步恶化；
- ✓ 根除风险事件隐患，实施灾难恢复；
- ✓ 制作“灾难恢复工具包”，工具包应包括恢复流程、联系清单、启动软件、工具、硬盘等；
- ✓ 参与、组织相关人员的培训；
- ✓ 更新、维护风险事件处理流程。

技术支援层：

- ✓ 必要时，为其他风险事件应急处理团队提供后勤及技术支持；
- ✓ 通过媒体、网站、电话等方式通知公众和相关机构；
- ✓ 需要时，协调内部机构与外部机构之间的联络。

在发生风险事件时，风险事件处理团队领导负责召集相关部门处理风险事件。团队成员必须拥有所有成员及外部相关人员联系录。当系统受到攻击后，最好使用电话或者传真的方式报告风险事件，以防止报告的信息被再次泄漏。

7．3．2 风险识别

处理和恢复风险事件造成的灾难的成本很高。当某个雇员在交易数据、系统或者网络上发现可疑的行迹时，风险事件应急处理团队需要花费大量的时间和精力进行调查和验证。当虚假报告的数量超过真实报告的数量时，这种现象本生就蕴含着风险，因为它分散了资源，使得正真的风险事件得不到及时的处理。为了准确地辨别风险事件，可考虑以下部分或全部典型数据安全风险特征：

- ✓ 系统警铃或系统受到攻击时发出的信号；
- ✓ 访问系统或网络的可疑行迹，如 UNIX 系统用户不按照正常路径登入系统；
- ✓ 在短时间内多次出现用户登入系统失败；
- ✓ 出现非法注册的新用户；
- ✓ 出现异常文件或文件名；
- ✓ 出现文件长度、日期被更改的现象，特别是系统可执行文件；
- ✓ 非法篡改系统文件；

- ✓ 非法篡改或删除系统数据；
- ✓ 系统功能被破坏，或者出现一个或多个用户不能登入系统的现象；
- ✓ 系统瘫痪；
- ✓ 某个服务器出现运行缓慢等现象；
- ✓ 网络构造被截取；
- ✓ 非常规时间使用系统，如在非工作时间登入系统；
- ✓ 显示的登入系统的时间与实际登入时间有出入；
- ✓ 异常使用模式，如财务部门不懂编程的员工编译程序；

7．3．3 风险评估

风险评估是指对已发事件的范围、影响面和影响层度进行评估。**注意：在发生数据安全风险事件时，先不要关闭电源或者重新启动系统，这样会导致数据、信息丢失。应由相关专业人士收集与风险事件相关的证据。**评估时需要考虑的要素有以下几个：

- ✓ 受到风险事件影响的电脑的数量；
- ✓ 是否有重要数据的遗失？
- ✓ 发生事件的切入点，如网络、拨入的电话等等；
- ✓ 风险事件可能造成的潜在的危害；
- ✓ 进行灾难恢复所需要的时间；
- ✓ 控制风险事件需要的资源；
- ✓ 如何有效地进行风险评估。

风险事件应急处理团队应根据风险事件的严重程度，决定是否应当报告管理高层，对于级别为“非常严重级”和“严重级”的风险事件，成员机构必须报告中国银联。

7．3．4 控制局面

控制局面是指风险事件应急处理团队控制风险的破坏范围。应急处理团队可以考虑将被攻击、破坏的系统隔离开来，但这将可能影响业务的开展。因此，管理团队需要考虑风险控制与业务开展之间的平衡，同时尽可能地减小对开展业务的影响。

为了便于事后分析和调查，最好对系统进行备份。同时更改系统密码，以

防止对系统的再次攻击。

7．3．5 根除隐患

在控制灾难破坏以后，应当作进一步的调查研究，以通过分析各个设备的日志记录揭示造成风险事件的真正原因。在调查时，风险事件应急处理团队应当使用一套单独的管理工具，以防止攻击者修改系统设置，使系统受到破坏。

- ✓ 重新装载没有被病毒侵害的操作系统，同时还应当：
- ✓ 安装最新的补丁程序；
- ✓ 关闭所有不必使用的应用程序；
- ✓ 安装防病毒软件；
- ✓ 确保机构制订的安全策略的实施。

7．3．6 灾难恢复

从备份系统中将原数据导入被攻击的系统时，要确保系统风险隐患已被根除。备份数据导入完成后，在系统真实用于业务运营之前，要对系统进行测试，同时要加强对系统及网络的保护。

7．3．7 事后跟踪

7．3．7．1 事后分析

事后分析的目标在于发生风险事件后对事件进行更深入地调查，已确定事件的影响范围、可能造成的潜在的威胁。事后分析可根据各机构自身的实际情况，组织内部人员、司法机构人员等专业人士进行。

7．3．7．2 文档的建立

所有与处理风险事件相关的文件都必须归档，以便于以后查阅。这些文档一方面可用于事件的分析研究，另一方面在起诉犯罪分子时，也是重要的证据。建议保留以下文档：

- ✓ 所有与系统相关的访问记录；
- ✓ 所有采取过的措施，包括措施的实施时间
- ✓ 与外部人员的沟通，包括沟通过的人员、时间、沟通内容等等。

此外，在按照上述步骤调查完发生的风险事件后，事件应急处理团队应提交一份完整的事件报告，报告包括以下内容：

- ✓ 事件发生的经过；

- ✓ 发现风险事件方式；
- ✓ 已采取的防范措施；
- ✓ 防范措施是否全面、有效及相关建议。

提交事件报告的目的在于协助本机构改进数据安全风险事件的处理流程。

7．3．7．3 处理与公众媒体的关系

各机构应统一由公共关系部门处理与媒体相关的业务。当发生“非常严重级”和“严重级”数据安全风险事件时，在向媒体公布相关事件之前，最好先向相关的成员机构或中国银联咨询如何应对媒体。在向媒体公布相关信息时，要确保事件的调查不会受到阻碍。所有的对媒体发表的言论都必须与成员机构及中国银联的观点相一致。

附录：术语表

访问权限控制（Access Control）：是指通过授权接触信息的人来限制接触信息和信息处理资源的功能。

物理访问控制（Physical Access Control）：是指在未授权人员和被保护的信息来源之间设置物理保护的控制

逻辑访问控制（Logical Access Control）：指利用其他方法控制访问。

账户信息和交易信息.(Account and Transaction Information)：见本书 1.1 节中定义。

账号(Account Number)：主卡持卡人的账号是指凸印或平印在银联规则卡上的号码

审核记录(Audit Trail)：指从信息处理设备中频繁采集的一组记录，这些记录表明某些活动的发生。这些记录可用来判定未授权使用或试图使用上述设备的行为是否已经发生。

身份鉴别(Authentication)：用来验证身份或证实信息完整性的 过程。

生物鉴定(Bimetrics)：指通过身体的某些特征或行为，例如指纹、视网膜图案、声音或签名等验证人的身份的方法。

分级(Classification)：将信息分成许多类别，以便对不同类别施行适当控制的方法。可以基于信息的类别、重要程度、潜在的欺诈危险性或敏感度进行分类。

密码鉴定（Cryptographic Authentication）：基于用密钥生成的信息证实代码进行的鉴别；或基于不对称密钥进行的鉴别。

信息(Information)： 是指一个机构用作转移资金、设定等级、发放贷款、处理交易等所用的任何数据。这些数据可能是电子形式的，也可以是在会议中口头提出的，写在纸张或其他任何媒介上的。这个定义包含了处理系统的软件部分。

不可逆加密(Irreversible Encryption)：将原文转换成加密形式，但这种加密形式是不能还原的一种加密方式。

公共网络(Public Network)：普通大众都可以进入的网络，包括国际互联网和公共电话系统。

静态密码(Static Password)：是指用户记住的并能多次重复使用的密码。使用静态密码对身份的验证是通过检查用户知道的东西来实现的。

动态密码（Dynamic Password)：是使用特定设备，如身份验证令牌等在一定时间内生成密码，该密码只能使用一次，不能重复使用。使用动态密码对身份的验证是通过检查用户知道的东西和他是否拥有某件东西来实现的。

强加密(Strong Cryptography)：通过最新的科技产生的加密系统可以有效的防止已被保护的信息被窃取。由于解密成本的降低和计算能力的降低，需要定期对加密过程进行重新评估。强加密在本书出版是意味着密钥长度超过100Bits,公钥或不对称密钥的长度超过768bits。

保密性(Confidentiality)：是指账户信息与交易数据不被泄露给未授权的用户、实体或过程，或供其利用的特性，即数据只供授权用户使用的特性。

完整性(Integrity)：是指账户信息与交易数据未经授权不能改变的特性。即数据在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱续、重放、插入等行为的破坏和丢失的特性。

可用性（Availability)：是指处理、存储账户信息与交易数据的系统在规定条件下和规定时间内完成规定的功能的特性。可用性的测度包括：抗毁性、生存性和有效性。

银联卡密钥安全管理指南【磁条卡部分】V1.0

（银联风管委〔2004〕2 号）

第一章 概述

第一节 内容简介

“一切秘密寓于密钥之中”，密钥管理是设计安全的密码系统所必须考虑的重要问题，数据加密、验证和签名等需要管理大量的密钥，这些密钥经加密后以密文形式发送给合法用户。《密钥指南》是参考国际组织有关密钥管理的知识、经验和相关标准，结合国内跨行交易中密钥的实际应用情况编写的指导性制度。在结构上分为概述、密钥生命周期安全管理、设备安全管理、管理规定和辅导检查等章节。在内容上遵循《密钥规则》中提出的基本要求,提出密钥生命周期中各环节的详细操作流程和推荐的具体做法，供各银联卡网络参与方参考。

《密钥指南》适用于金融磁条卡对称加密算法的密钥管理，非对称密钥的相关内容将另行成册。

本指南的适用范围和生效时限与《密钥规则》相同。《密钥指南》基于现有技术规范，尽可能地兼顾应用与维护的方便性，在最大程度上确保安全，体现适当的规定、适当的投入保证相对安全，但不可能完全避免所有的风险。经验做法仅属于推荐性质，力求整体提升密钥安全管理水平。中国银联并不承担成员机构具体实施中发生的问题及其影响。

第二节 运用概述

1. 密钥体系与安全级别

按照使用范围和实际应用的不同，密钥划分为不同体系或类别，每个体系或类别都具有相应的功能与特点，须遵循不同的标准与要求。

《密钥指南》仅适用于跨行交易网络中的密钥安全管理，行内的密钥体系、类别或安全管理方法不在其叙述的内容之列。银联卡网络的密钥根据实际使用情况划分成三层，三层密钥体系根据密钥的使用对象而形成，上层对下层提供保护和一定的维护功能，不同层的密钥不许相同，不能相互共享。加密机主密钥（MK），即本地主密钥是最重要的密钥，应按照《密钥规则》的有关要求施行最高级别或

最严格的管理。成员主密钥（MMK）[或终端主密钥（TMK）]在硬件加密机以外的系统中存放和使用时，处于本地 MK 的保护之下。由于成员主密钥是参与交易双方机构共同生成且各自保存（或因地域原因交易机构完整持有成员主密钥组件），因此安全性存在互动、相互影响，同时更新频率较低，因此是最有可能被泄漏和攻击的密钥，需要相关方的共同维护与重视。工作密钥为最底层的密钥，因其数量庞大，需要用一定的管理设备（如终端密钥注入设备）加以辅助（详见第三章有关叙述）来确保安全。

2. 密钥生命周期的安全管理

包括密钥的生成、传输、注入、保管、泄漏与重置、删除与销毁等内容。其任务就是在整个生命周期内严格控制密钥的使用，直到它们被销毁为止，并确保密钥在各个阶段或环节都不能出现任何纰漏。

2.1 密钥生成

密钥必须随机或伪随机产生。其中随机指无法预知和重复；伪随机指由算法产生；密钥生成结果是一系列可以转换成二进制的数字。若需要人工产生密钥，允许产生密钥的方式有：丢硬币、摸彩球、掷骰子；不能用想象的方式生成各种密钥。

密钥生成后，在硬件加密设备外部的明文形式必须由两段或两段以上的组件构成。

2.2 密钥传输

密钥明文在传输时需采用双重控制和分裂学，分为两段或两段以上组件，传输的方式应采用多种传输渠道和不同传输时间的方法。

传输时存放密钥组件的介质可以是硬拷贝、磁盘、IC 卡等，每份介质只可存放一段密钥组件。不得以任何形式传输完整密钥的明文。

2.3 密钥注入

密钥组件的注入必须采用双重控制和分裂学，注入时应确定注入实施区域没有被非正常监控，有摄像监控系统的区域内，摄像头不得对准加密设备的操作面板，注入应有规定的操作流程。

采用人工键入方式注入密钥组件的明文时，每段密钥组件必须由指定的密钥注入员注入。

2.4 密钥保管

对于密钥组件的存储，必须坚持三个原则，即最小化、认可化和高安全性。

最小化：在密钥注入前的时间内，由指定专人负责保管密钥组件；

认可化：可以放在安全的容器内，只有指定的密钥管理员可以打开容器；

高安全性：存放在安全的容器内，采用双重控制，指定的密钥维护人员只拥有部分访问权限，并且密钥组件必须分开存储。

对于密钥注入设备，需要采用双重控制的原理来确保安全性。密钥保管人员不能开启和操作硬件加密机。

2.5 密钥泄漏与重置

除密钥泄漏或可能泄漏外，加密机主密钥（MK）一般不更新。成员主密钥（MMK）一般 2—3 年更新一次。若出现泄漏，则立即更换被怀疑或确认泄密的密钥，确定被涉及到的功能领域，并且向管理部门报告。若主密钥和成员主密钥出现泄漏，应采用与初次生成相同的控制方式产生新的主密钥和成员主密钥；若加密机主密钥（MK）泄漏，则替换主密钥并替换所有由该主密钥保护的密钥。若成员主密钥（MMK）泄漏，则替换成员主密钥并更换使用该成员主密钥加密的所有密钥。工作密钥（WK）必须经常更换，若怀疑泄漏，则可采用人工触发方式重置密钥，在连续重置一定的次数后，需要对该机构的密钥机制进行审核。

2.6 密钥删除与销毁

密钥生成后或在系统更新、密钥组件存储方式改变等情况时，不再使用的密钥组件（如以纸质或 IC 卡等方式存储的介质）或相关信息的资料应及时销毁。

作废或被损坏的密钥必须在双人控制下安全销毁，保证无法被恢复，销毁过程必须专人监控和记录。

第二章 密钥生命周期安全管理

第一节 密钥的生成

各类密钥及其组件必须遵循随机或伪随机生成的原则，密钥的生成必须确保随机性，生成工具应使用硬件加密机或其他安全的密钥生成工具。本节描述密钥及其组件生成的安全做法。

1. 加密机主密钥（MK）的生成

加密机主密钥必须由三段组件组成。加密机主密钥生成可使用硬件加密机、人工方法或符合本指南规定的其他方法和工具生成。

1.1 使用加密机生成加密机主密钥

1.1.1 生成时的工作人员及其职责

密钥监督员一名、设备操作员一名、密钥生成员三名；

密钥监督员负责监督整个密钥生成过程的合法性和规范性；

设备操作员负责设备生成密钥时的设备环境准备；

每个加密机主密钥生成人员各自负责从加密机操作界面上生成一段密钥组件，并负责今后该密钥组件的注入和保管。

1.1.2 使用加密机生成过程

由密钥监督员召集三名密钥生成员到场并讲解密钥生成规则和加密机生成密钥组件的操作方法。

由设备操作员将加密机的操作面板切换到生成第一段主密钥组件的界面，设备操作员即离开加密机到看不到加密机操作面板的地方。这一过程必须由密钥监督员在场监督。

第一位密钥生成员通过加密机操作面板生成第一段密钥，并记录下第一段密钥的内容后，将操作面板上的密钥内容全部清除。（如加密机有将密钥内容打印到密码信封封存的功能，则应将生成的密钥打印到密码信封内封存。如加密机有用 IC 卡保存密钥段的功能，则应将密钥段保存到 IC 卡上。）生成员将记录下的密钥内容当场装入信封[如密钥生成后同时产生该段密钥的检验值（Check Value），应同时记下该检验值]，并进行封口。由密钥监督员加盖密封章或签名章后，交由密钥生成员保管。

第一位密钥生成员生成完密钥段后，离开现场。

第一位密钥生成员完成密钥生成后，密钥监督员与设备操作员同时到加密机操作面板前检查前一段生成的密钥是否已清除。如密钥生成员未清除密钥内容，则应请该密钥生成员重新到场生成，前次生成的密钥应立即作废。如前一段密钥已清除，然后按第一段密钥生成的过程依次生成第二段和第三段密钥。

三段密钥生成完毕后，如加密机同时生成密钥的总校验值，则可由最后一位生成员单独记录下该校验值，由该生成员连同密钥组件一起保管。

1.1.3 操作要点

密钥监督员和设备操作员不得看见加密机面板上的密钥内容或密钥生成员记录下的任何密钥内容。

三位密钥生成员不得有两人或三人同时出现在现场。

密钥生成员记录下密钥内容后必须立即清除加密机操作面板上的内容。

1.2 人工生成的方法

1.2.1 生成时的人员组成及各自的职责

密钥监督员一名、主密钥生成员三名。

密钥监督员负责监督整个密钥生成过程的规范性。

主密钥生成人员负责按照指定的人工生成方法各自生成一段密钥组件，并负责该段密钥组件的注入和保管。

1.2.2 人工生成的过程

由密钥监督员（或设备管理员）召集三名密钥生成员并讲解人工密钥生成的方法和有关工具的使用方法和规则。

由密钥监督员逐个召集密钥生成员到指定的地点，按规定的方法，使用指定的工具分别生成三段密钥组件。

每个密钥生成员生成并记录由其生成的密钥组件后，将该密钥组件装入专用的信封内封装，由密钥监督员加盖密封章或签名章后，交由密钥生成员保管。

1.2.3 操作要点

密钥监督员要确信密钥生成员已掌握了人工密钥的生成方法后才能让密钥生成员正式进行生成操作，必要时可要求生成员模拟生成过程以便确认。

密钥生成员在生成密钥期间，密钥监督员及其他人员不得进入操作现场。

密钥生成员生成完密钥后，密钥监督员应提醒密钥生成员已生成的密钥的长度、密钥数字的取值范围、奇偶校验等要素是否符合规定。

2．成员主密钥（MMK）的生成

2.1 使用的工具

成员主密钥可使用加密机、人工或符合本指南规定的其他方法生成。

2.2 生成密钥组件的分工

成员主密钥一般由两段密钥组件组成，可由银联分支机构与其对应的成员

机构各自生成其中的一段密钥组件，也可由银联分支机构生成全部两段密钥组件。

2.3 成员主密钥生成的过程

2.3.1 银联和对应的成员机构各自生成一段密钥组件的操作过程

银联生成的密钥组件称第一段（A 段），对应的成员机构生成的称第二段（B 段）。

首先由银联分支机构按照本节 1.1 中加密机主密钥（MK）的生成方法和过程生成其中的一段密钥组件。

该段密钥组件应备份两个副本（包括 IC 或纸质的备份），一个副本由银联分支机构使用，另一个副本传送给对应的成员机构。

银联分支机构在传送给接收方（对应的成员机构）A 段密钥时，须附一张由接收方填写 B 段密钥的表格，同时应提供给对方密钥生成及回传的方法和要求。

由对方生成密钥的方法，应事先通知对方，了解对方的生成方法，如对方的方法不符合安全的要求，应向对方提出改进意见。

2.3.2 两段密钥组件都由银联有关机构负责生成的操作过程

这种方式与加密机主密钥的生成过程基本类似。主要区别为：

成员主密钥由两段密钥组件组成，因此只需要两个密钥生成员，生成的密钥为两段组件。

生成的每段密钥段需要保存两个副本（包括 IC 或纸质的备份），其中一份由银联机构使用，另一份提供给对方机构使用。

3. 工作密钥(PIK、MAK、TPK、TAK)的生成

工作密钥一律用联机的方式，由加密机生成。

生成的密钥在加密机中用相应机构的主密钥（MMK）加密后从加密机送到主机，再通过相应的联机报文发送到有关机构和终端设备。

加密后的工作密钥，可存放在主机上供系统使用，存放在主机上的工作密钥必须用加密机主密钥（MK）或成员主密钥（MMK）加密保护。

4. 工作表格

在生成密钥组件的过程中，应用单位应填制有关工作表格。加密机主密钥

（MK）或成员主密钥（MMK）生成完后，应由相关人员按规定填写密钥生成表格，签章封存，表格作为密钥档案资料妥善保管，留底备查。

密钥生命周期的其他工作环节也应填制相关的工作表格，操作步骤比照上述叙述进行。

第二节 密钥的分发与传输

1. 密钥分发过程要求

银联分支机构向同一地区的联网机构分发密钥时，应要求接收机构派专人接收：可以由接收机构负责保管和注入该密钥组件的人员，也可以由其委派的人员领取。

对每一段密钥组件接收机构必须分别派专人领取，不得由一人领取多段密钥。当对方领取多段密钥时，领取人员不得乘坐同一个交通工具。

对方机构领取密钥时，该密钥组件的保管人员和密钥监督员必须同时在场，由保管人员取出需分发的密钥信封，密钥监督员需检查信封的密封章或密封签名是否完整，并填写分发密钥的表格。密钥由对方机构领取后，密钥监督员与对方机构的领取人员需在分发密钥的表格上签名确认。

2. 密钥传输过程要求

2.1 加密机主密钥的传输

2.1.1 同城传输

加密机主密钥从保管处取出时，该密钥组件的保管人员和监督人员必须同时在场，并按规定填写分发密钥的表格。输送人员在表格上签名确认后，方可向对方传送。接收机构收到密钥后，应返回签收单，签收单由密钥保管人员负责保管。

加密机主密钥如在同城进行传输，应由三人分别持三件经密封的密钥信封，在不同的时间送达对方或由对方三名专人分别领取，传送或领取人员不得乘坐同一辆交通工具。

2.1.2 异地邮寄的要求

在需要采用邮寄方式传送密钥时，应尽量使用邮政部门的机要邮政系统邮寄。如无此条件则应使用特快专递方式邮寄。

密钥在邮寄前需按规定填写分发密钥的表格，并派可靠人员到邮局邮寄，邮寄时的手续凭证作为附件妥善保管。

邮寄时必须将每一段密钥单独作为一份邮件邮寄，不同的密钥组件需在不同的日期分别寄出。

2.2 成员主密钥的传送要求

成员主密钥的传送要求按照本节 2.1 对加密机主密钥的传送要求执行。

2.3 工作密钥的传输要求

工作密钥的传输必须通过联机方式进行，必须由成员主密钥加密后传输。

传输时利用《银行卡联网联合技术规范》中有关密钥切换的报文进行。

2.4 禁止方式

密钥明文及其组件不得采用电子邮件（E-mail）、传真、电传、电话等方式直接传递。

如采用其他电子方式传输，该方式应符合《密钥规则》的传输要求，或应符合国家密码主管部门的规定和相关标准，并经过国家认可的权威机构检测通过。

3. 密钥接收的要求

由其他机构分发给银联各机构的密钥，银联各机构在接收密钥时应遵守上述相关规定。

接收密钥时，保管、监督等相关人员应首先填写密钥接收表格。密钥接收人应在表格上签名确认。密钥启用前应由密钥监督员签字封缄，交由保管人员严密保管。保管人员应在接收表格上签字确认。为方便起见，接收人员与保管人员可以由同一人担任。

第三节 密钥的装载和启用

1. 基本要求

根据注入密钥的类型，确定注入过程中密钥监督员、注入人员、设备操作员等各自的工作内容和责任；

密钥应分段分人并在隔离状态下注入密钥使用设备；

密钥注入现场的摄像监控设备不得拍摄到密钥注入设备的操作面板部位；

密钥注入完成后，应按规定填写相关的密钥注入表格。

2. 注入过程

2.1 加密机主密钥的注入

2.1.1 注入人员组成及各自的职责

密钥监督员一名、设备操作员一名、主密钥注入人员三名；

密钥监督员负责监督整个密钥注入过程的合法性和规范性；

设备操作员负责在密钥注入过程中对加密机及密钥注入设备环境的准备；

主密钥注入人员负责将各自的密钥组件注入到加密机中，注入人员一般由该密钥组件的密钥生成员或保管人员担任。

2.1.2 密钥组件的取用

申请人填写登记表，经机构主管负责人审批同意。

保管员核对登记表的申请人是否为该密钥的生成员：如是，则在登记表上做好记录，由申请人签名后，将密钥组件密封信封交申请人；如申请人并非该密钥生成员，则应有生成人的授权书或口头声明（被授权人不得是该密钥另一组件的生成员或保管员），并由密钥监督员确认后，方可取用密钥组件。

2.1.3 注入前的审核

由密钥监督员负责通知三位密钥组件保管人员从保管处取出密钥组件保管信封，并检查信封的密封章和签名章等是否完好。如信封的密封章和签名章完好，则可进行下一步的注入操作。如发现破损或有被干预迹象等问题应报告主管领导，根据具体情况处理，必要时应重新生成新的主密钥组件。

2.1.4 注入过程

由设备操作员将加密机的操作面板切换到注入第一段主密钥的界面后，与此无关的人员均须离开，确保看不到设备显示面板（当用 IC 注入密钥时例外）。第一位密钥注入员根据注入密钥的方法（IC 卡或纸质）注入第一段密钥组件，并核对注入后该段密钥组件的检验值（Check Value）。如检验值不正确，需重新注入，直到正确为止。第一位密钥注入员注入完密钥组件后，离开现场，如无需重新注入密钥组件，不再回现场。这一过程必须由密钥监督员在场监督。

按第一段密钥组件注入的方法，再注入第二段和第三段密钥组件。

2.1.5 注入后的工作

主密钥所有组件注入完成后，由密钥监督员检验注入是否成功，用三段密钥组件注入后的总检验值与生成时的总检验值进行核对，如核对不成功则需重新注入；如生成时无总检验值，可不核对总检验值。

密钥注入完成后，原已开封的密钥保管信封需重新封装，并加盖密封章和密钥监督员签名章，交由原来的保管人员保管。

密钥注入完成后，需按要求填写注入表格，对注入过程签名确认。

2.2 成员主密钥的注入过程

成员主密钥的注入过程与加密机主密钥的注入过程基本一致。因成员主密钥由两个组件组成，注入过程只需两位注入员参加。

成员主密钥注入并正式启用后，凡记录在纸质上的密钥组件明文必须销毁，销毁的方法必须按本章第五节要求进行。

纸质的密钥组件明文销毁后，成员主密钥密文文件必须至少保留两个副本。副本的方式可以是 IC 卡，主机上的密文文件或机外密文文件的保存方法：

- 保存在主机上的密文文件，应设定最高级别的访问权限；
- 保存在机外的密文文件，应由专人密封保管，并应符合本章第四节要求。

2.3 工作密钥（PIK、MAK、TPK、TAK）的启用

工作密钥由主机通过联机方式从加密机生成，生成的密钥可放在加密机内使用，也可放在主机上使用。工作密钥必须用特定的成员主密钥进行加密后方可在加密机外存放和使用。

第四节 密钥的保管

1. 基本要求

各相关机构应在安全区域（如机要室或档案室）配备保险容器（如保险柜），用以存放密钥组件与密钥档案资料。

密钥存储介质要求用信封密封，由生成（或注入）人员与密钥监督员签名确认，加盖密封章；密钥组件或档案维护人员调离，办理交接手续时应由密钥监督员认可。

只有密钥组件的生成员或注入人员才有权使用该密钥组件。

密钥组件存取、使用情况应由保管人员作好记录，建议该记录也应存放在保险容器内，视同密钥组件处理。

2. 与密钥安全有关的机密设备及密码的保管要求

2.1 存放密钥的保险容器

根据密钥保管方式的不同相应配备保险容器。

如密钥分段分人保管，则每一密钥组件的保管人员都必须分别配备专用的保险容器，该保险容器的钥匙和密码由该保管人员负责掌管。

如采用所有密钥资料集中保管的方法，则密钥的每个组件应分开放于不同保险容器内，建议保险容器钥匙和密码必须分由不同的人员掌管，并且只有他们及密钥监督员同时在场才有权开启该保险容器。

2.2 硬件加密机钥匙的保管

为维护方便，硬件加密机钥匙可由设备管理员负责保管，但必须存放一份在保险容器中，以便于加密机应急维护时使用。

设备管理员调离时，应办理交接手续，保险容器中的钥匙备件也应同时移交。

2.3 与密钥有关的密码的保管

加密机的安全密码、操作密码（或授权操作密码）应分别由设备管理员、设备操作员掌管。上述密码应在保险容器保留备份，存入之前由密钥监督员用信封密封、签名确认，并加盖密封章。

上述人员调离时，应重新设置密码，并更新保险容器中的备份。

3. 密钥组件的保管要求

3.1 主密钥组件的保管要求

存储主密钥各段组件的 IC 卡或密封信封应在密钥监督员监督下，直接存入保险容器，且只有生成员（或授权人员）才有权取用各自生成的主密钥组件。

生成人员调离所在机构时，应办理主密钥组件的 IC 卡和密封信封的交接手续，交接手续应在密钥监督员监督下进行，且应当场存入保险容器。

3.2 成员主密钥组件的保管要求

各成员机构不保存成员主密钥的明文，除主机加密留存外，机外不允许有明文形式出现；

各成员机构不保管非本机构生成的成员主密钥的 IC 卡或密封信封。

3.3 工作密钥

不应出现在应用系统、终端、注入设备等相关设备以外的任何介质上。

4. 接收保管的过程

4.1 由本机构自己生成的密钥组件的保管

密钥生成员生成密钥组件后，用信封将密钥密封，由生成员在密封信封上注明密钥名称、用途、密封日期，密钥监督员签名确认，加盖密封章后，当场交付保管人员。

如未能当场交付，保管人员在接到密封信封后，应立即检查信封是否曾开封，如曾开封应不予接收，并通知监督员，必要时可发起重新生成密钥。如密钥信封完好，保管人员应在工作表格中做相应记录，签名确认，存放于保险容器中。

4.2 由对方机构分发的密钥组件的保管

由对方机构分发的密钥，接收机构需指定专门的接收人接收。接收时由密钥监督员和接收人员在场。

接到密钥组件的密封信封后，应由密钥监督员和接收员同时检查信封是否曾被开封。如曾被开封过则应通知发出者，要求其重新生成密钥后再发送。如密封信封完好，应由密钥监督员用信封再做密封，当场交给保管人员存入安全容器内，存入过程参考 4.1。接收过程应填写工作表格。

5. 密钥档案资料的保管

由保管人员负责保管，存放于安全区域的保险容器内，保存期限应不低于记录对象的生命周期。

保管人员调离岗位前，应妥善办理交接手续。

第五节　密钥的删除与销毁

为避免泄漏风险，失效密钥必须及时安全删除或销毁。

1. 失效密钥的认定

失效密钥包括过期密钥、废除密钥、泄漏（含被攻破）密钥。

1.1 过期密钥

对于不同密钥类型，有着一定的密钥生存期，超过这个期限，即可标志为

过期密钥，应该删除和销毁。

1.2 废除密钥

指在测试环境中不再使用的密钥、生产环境中因应用程序的修改不再使用的密钥、存放介质发生损坏的密钥、设备报废或废弃在设备中不再使用的密钥等。

1.3 泄漏密钥

指密钥在其生命周期内被泄漏或怀疑可能泄漏以及密钥被攻破等情况。

2. 密钥删除和销毁的方法

对失效密钥，应采用执行和检验相结合的方法删除和销毁，确保密钥被完全销毁。

2.1 主机系统中密钥的删除

找出在主机系统中存放待删除密钥的数据库表、密钥文件等，在删除操作时必须多人同时在场（设备管理员、密钥销毁员、密钥监督员等），专人执行（密钥销毁员），专人验证（密钥监督员），确保密钥的真正删除。

2.2 硬件加密机中密钥的删除

找出所有待删除密钥以及硬件加密机中相应的密钥索引值，对该密钥进行重写，冲销旧密钥。在删除操作时需多人同时在场（设备操作员、密钥销毁员、密钥监督员等），专人执行（密钥销毁员），专人验证（密钥监督员），确保该密钥被覆盖。

硬件加密机应具有密钥销毁功能，当加密机送检、维修或运输时应启动毁钥功能，保证硬件加密机中的所有密钥被彻底删除。在删除操作时需多人同时在场（设备管理员、密钥销毁员、密钥监督员等），专人执行（密钥销毁员），专人验证（密钥监督员），确保密钥被销毁。

2.3 终端设备中密钥的删除

终端设备中的密钥是指 POS、ATM、收银一体机等的 PIN PAD、金融多媒体终端等设备中使用的密钥。对报废不再使用设备的密钥可采用物理销毁的方法来删除密钥。对仍将继续使用的设备可采用覆盖的方法删除密钥。在执行删除操作时需多人同时在场（设备管理员、密钥销毁员、密钥监督员），专人执行（密钥销毁员），专人验证（密钥监督员），确保密钥被销毁。

2.4 存放密钥的组件介质的销毁

找出待销毁密钥的组件，由密钥监督员和保管人员同时在场执行销毁操作。销毁的要求如下：

纸介质：采用焚毁、溶化的方式，保证不可恢复；

IC 卡：对于重复利用的介质，交密钥销毁员重新写卡，确保有写卡操作，覆盖旧密钥而不可恢复，销毁过程由密钥监督员验证。对于不再利用的介质，交密钥销毁员物理毁卡，必须采用芯片毁损的方式，保证不可恢复，销毁过程由密钥监督员验证。

密钥枪类：设备管理员启动密钥枪毁钥功能，由密钥销毁员执行，密钥监督员验证。

母 POS：设备管理员启动母 POS 毁钥功能，由密钥销毁员执行，密钥监督员验证。

2.5 相关机构成员主密钥的删除和销毁

当一方销毁密钥涉及另一方的成员主密钥时，应书面通知对方机构相应删除和销毁，对方机构执行密钥删除和销毁后需要书面回执并由相关人员签字确认。

2.6 建立密钥删除和销毁登记制度

密钥删除和销毁登记由密钥监督员负责。密钥资料销毁的情况应记录在案，包括销毁时间、操作员、密钥监督员等要素。销毁记录由销毁人和密钥监督员签字后与相关资料一同保存。

第六节　密钥的泄漏与重置

1. 可能被泄漏的密钥

1.1 可能被泄漏的密钥类型

在银行卡交易中经常涉及的密钥类型有三类：MK（加密机主密钥）、MMK（成员主密钥）、PIK / MAK / TPK / TAK（工作密钥）。

由于工作密钥用于交易报文中的相关数据加密且更新频繁，因此非法攻击者企图截获工作密钥的机率较低。

由于成员主密钥是参与交易双方机构共同生成且各自保存（或因地域原因交易机构完整持有成员主密钥组件），因此银联卡网络参与方之间密钥的安全性

存在互动因素影响，同时成员主密钥更新频率也较低，如果一方密钥泄漏将影响交易对方的密钥安全，从而影响对方系统的整体安全，因此成员主密钥是最有可能被泄漏和攻击的密钥。

主密钥的更新频率是最低的。主密钥的重要性和更新频率低是造成密钥可能被泄漏和攻击的主要因素。

1.2 密钥泄漏或被攻击的方式

密钥泄漏的方式大致分：非法获取、推测规律、直接穷举三种。内部人员通常侧重攻击主密钥来破解数据库中保存的其他密钥，外部人员则通过攻击成员主密钥破解工作密钥。

1.2.1 非法获取

由于硬件和软件资源的限制，一般非法攻击者采用直接穷举的方式并不多见，密钥的泄漏大部分是通过非法途径或利用管理疏忽获取的，如下列情形：

- 存放密钥的保险柜被盗；
- 设置木马程序窃取密钥；
- 买通密钥管理员或密钥涉及者监守自盗；
- 测试系统中出现生产系统密钥；
- 密钥明文抄写后被当作废纸随手丢弃，废旧密钥未及时销毁；
- 密钥明文出现在文档资料、程序源码、通信联络中；
- 硬件加密设备无专人管理，无权限设置，未授权情况下开启加密设备时密钥未自毁等。
- 废弃的设备中密钥未销毁等。

1.2.2 推测规律

从根本上说，推测规律也是穷举法中的一种，通过推测规律减少穷举的次数。对于一种规律性强的密钥，推测是有效的。

推测规律主要是找出密钥的相关性，因此提高密钥的非相关性是在密钥设置时需要考虑到的方面。推测规律的方式有：

- 找出密钥的相似处，进行比对，总结规律以试图解析密钥；
- 通过对废旧密钥的联想，猜测规律以试图解析密钥；
- 通过对密钥输入者的习惯进行分析，猜测密钥规律；

- 通过对测试系统密钥进行分析，猜测生产机密钥规律；

1.2.3 直接穷举

直接穷举需要硬件和软件资源支持，非法攻击者利用合法交易，通过穷举密钥明文，比对密钥密文来破译密钥明文，这种方法耗用一定时间，但隐蔽性较高。

1.3 密钥泄漏的补救措施

加密机主密钥泄漏后，应立即停止所有交易，重新生成新密钥并马上启用，需生成的密钥包括加密机主密钥，成员主密钥和终端主密钥，以及各类工作密钥。

成员主密钥泄漏后，重新生成相应成员主密钥并立即启用，并更新对应的工作密钥。

终端主密钥泄漏后，重新生成相应终端主密钥并立即启用，并对终端的工作密钥进行更新。

1.4 记录相关操作

密钥泄漏的补救措施完成后，应记录相关操作填写相应表格，表格要素包括：密钥使用单位、设备名称和编号、泄漏密钥的类型、发生密钥泄漏的时间和方式、密钥泄漏造成的损失和补救的措施等。

2. 密钥泄漏的核查

2.1 加强系统跟踪，在日常工作中定期核查系统状态。检查内容包括：

- 在某时间域内，大额交易的频度是否异常；
- 在某时间域内，交易频率是否异常（如突发同类交易是否增多）；
- 在某时间域内，密钥类错误交易是否增多；
- 是否非法访问增多；
- 是否合法访问异常操作增多；
- 是否有大量的伪卡出现；
- 异常情况是否具有一定相似性和规律性。

2.2 禁止发生的情形

对执行密钥生成、保管、启用、更新、销毁操作等过程进行检查，杜绝违规或超权限操作，禁止发生以下情形：

- 未使用加密设备，密钥的明文出现在系统或程序中；

- 加密机主密钥、成员主密钥以单个完整的密钥形式出现在硬件加密机外部，或密钥组件在权限范围外可以被合成；
- 工作密钥未按规定动态更新，长时段呈静态状况，导致被穷举攻破；
- 废旧设备中仍在使用的密钥未及时销毁，随意丢弃或放置；
- 在测试系统和生产系统使用同一密钥，或在测试系统出现生产系统密钥的明文；
- 同一密钥在多个地方使用（此种情形在 POS 终端上较为多见）。

2.3 专人负责加密设备

对硬件加密设备的使用、维护应专人负责，每次操作应登记记录，多人在场，对违规超权限的操作应及时查处。

2.4 加强系统用户权限和密码管理

对系统管理员密码、各用户密码及用户权限应严格管理，一旦上述密码发生泄漏、权限失控或人员离职，应及时对系统各密钥进行核查跟踪，根据需要及时更新密钥。

3. 密钥泄漏和被攻破情况的界定

在生产中使用的各类密钥都有可能发生泄漏或被攻破，在发现下列情况时，可以考虑认定密钥已泄漏或被攻破，必须及时采取措施更新密钥。

3.1 加密机主密钥泄漏和被攻破的情况

- 密钥未按本指南生成、分发、保管、注入所规定的条款执行；
- 有两段或两段以上密钥明文被盗或同时丢失；
- 有两段或两段以上密钥明文同时存放在同一台可被人读取的设备上；
- 系统内大部分成员主密钥、工作密钥泄漏或被攻破；
- 其他经密钥安全管理工作组认定的情况。

3.2 成员主密钥泄漏和被攻破的情况

- 密钥未按本指南生成、分发、保管、注入所规定的条款执行；
- 两段密钥明文被盗或同时丢失；
- 两段或两段以上密钥明文同时存放在同一台可被人读取的设备上；
- 系统内工作密钥泄漏或被攻破；
- 其他经密钥安全管理工作组认定的情况。

3.3 工作密钥泄漏和被攻破的情况

- 密钥未按本指南生成、分发、传输规定的条款执行；
- 报文中加密的数据被攻破；
- 其他经密钥安全管理工作组认定的情况。

3.4 密钥被认定泄漏和被攻破的审核程序

经密钥安全管理工作组共同认定，报本单位主管领导批准后，认定密钥已泄漏和被攻破。对于工作组无法认定的情况，可聘请有关专家和管理人员进行审核。必要时可报公安部门协助追查。

对于密钥被认定已泄漏和被攻破的情况，需填写相应的表格，表格要素包括：泄漏或被攻破密钥的类型，发生泄漏或被攻破的时间、地点和方式，密钥使用单位，设备名称和编号等。对于情况比较复杂的事件需专题报告。

对任何加密机主密钥和成员主密钥泄漏或被攻破的情况，银联各分支机构需报总公司主管部门备案，情节严重的需要向当地公安部门报案。其他成员机构发生与银联卡有关的密钥泄漏情况也应及时报送中国银联。

第三章 银联卡受理终端及 MIS 系统密钥安全管理

银联卡受理终端形式多样、型号不一，随着业务的不断拓展，其形式将愈发多样化，为确保持卡人个人识别码（PIN）及关键信息的安全传输，严格管理终端密钥与商业 MIS 系统，本章提出一些基本做法，着重对对称密钥体系下受理终端的密钥安全做出规定。

第一节 银联卡受理终端的密钥体系

终端密钥分为终端主密钥（TMK）和终端工作密钥（TWK）。

终端主密钥用于 ATM 自动柜员机、POS 终端、商店收银一体机、自主多媒体终端等使用银行卡的终端设备，为终端与交换主机之间的工作密钥（TWK）在传输和保存时提供保护。在实际使用中有时需设置终端主密钥的终端管理密钥（TGK），用于传输和保存终端主密钥。

终端工作密钥分为两种密钥，即终端个人识别码 PIN 的加密密钥(TPK)和终端报文合法性认证密钥(TAK)。

1. 终端主密钥（TMK）

终端主密钥用于对工作密钥在传输和保存时进行加密保护，一般每台终端设定一个密钥，必要时若干台终端可共用一个终端主密钥，但只允许在同一商户内共用一个终端主密钥。

终端主密钥在主机中受加密机主密钥（MK）或终端管理密钥（TGK）的保护。在终端设备中受终端的硬件加密设备保护。

终端主密钥组件的分段数、生成、分发、保管及注入的方法与成员主密钥（MMK）相同，终端主密钥的长度为 128 位或以上。

2. 终端工作密钥（TWK）

终端工作密钥分 TPK 和 TAK 两种密钥。

TPK 和 TAK 由主机经加密机联机生成，并由该终端的终端主密钥加密后进行传输和保存。终端在每次签到时由主机重新生成新的工作密钥，加密后将密钥的密文下载到该终端上。

终端工作密钥的长度及其他各种要素与成员机构的工作密钥相同。

3. 终端管理密钥（TGK）

通常情况下，终端主密钥在主机中受加密机主密钥的保护，其生成、传输、注入时同样采用分隔、分段、分人控制的方法进行安全控制。

由于终端数量巨大，用上述方法管理，必然花费大量的人力和物力。因此在实际应用中可采用密钥枪、母 POS、IC 卡等专用的密钥传输及注入设备进行终端主密钥的传输和注入。终端管理密钥在这些设备中起到保护终端主密钥的作用。

在一个系统中可设置若干个终端管理密钥，分别用于不同的终端或不同的机构之间进行终端主密钥的传输和保存。

密钥枪、母 POS、IC 卡等专用的密钥传输及注入设备的安全要求见本章第三节中的有关内容。

4. 终端密钥的管理权限

凡直接接入银联交换系统的终端设备，其密钥的生成、注入、分发与保管等过程操作和管理由相关的银联分支机构负责，并按本指南的要求进行监督检查。

凡交易不直接接入银联交换系统的终端设备，转接机构属于金融机构的，其终端密钥的生成、分发、保管、注入等操作和管理由该金融机构负责，密钥的安全由该机构参照本指南要求进行。转接机构属于非金融机构的，密钥的安全由银联相关的管理机构按本指南的要求负责执行。

第二节　MIS 商户的密钥安全要求

1. MIS 商户的密钥机制

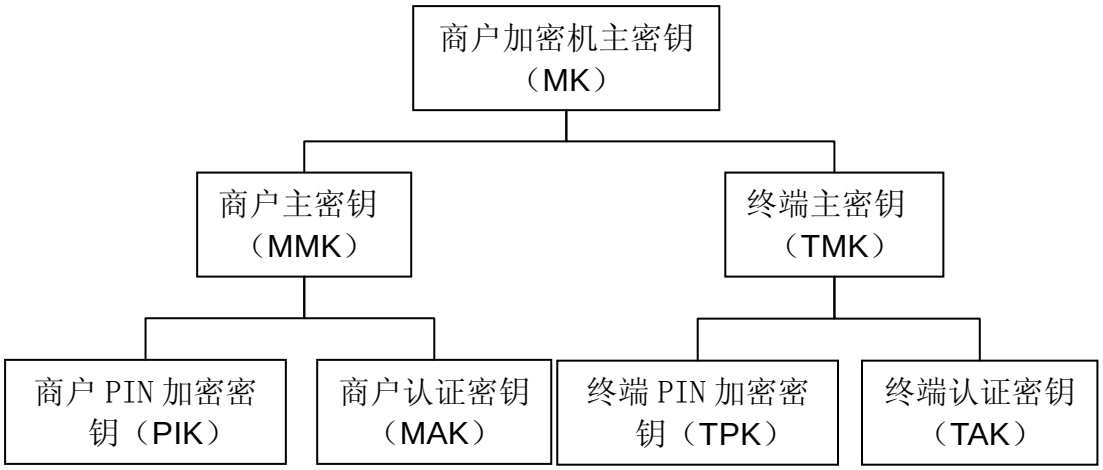
MIS 商户可按密钥机制的不同实行密钥管理。目前 MIS 商户的密钥机制主要分为两种：一种为两级密钥机制，另一种为单级密钥机制。

1.1 两级密钥机制

两级密钥机制系由 MIS 商户的商户密钥和终端密钥两级构成。在两级密钥机制中商户服务器端必须配有硬件加密机，数据的加、解密等操作必须在硬件加密机中进行。

1.1.1 密钥结构图

两级密钥机制的结构如下图所示：



MIS 商户两级密钥体系结构图

1.1.2 商户级密钥

商户密钥由商户主密钥（MMK）和商户工作密钥组成，商户工作密钥与成员工作密钥类似分为 PIK 和 MAK。

商户主密钥按成员主密钥的方法和要求管理。商户工作密钥在商户服务器向银联交换主机签到时，由银联交换主机经加密机生成并下载到 MIS 商户的服务

器上，该工作密钥在传输和存放时受商户主密钥(MMK)的保护。

1.1.3 终端级密钥

终端级密钥由终端主密钥（TMK）和终端工作密钥组成，终端工作密钥分为终端的 PIN 加密密钥（TPK）和终端报文合法性认证密钥（TAK）。

终端工作密钥的生成、传输和使用方法与成员工作密钥 PIK 和 MAK 相同。在终端每次向商户服务器签到时，由商户加密机生成后用该终端主密钥加密后下载到终端上。

终端主密钥在商户服务器端由商户加密机主密钥加密后存放在商户服务器内或者直接存放到加密机内。在终端侧必须存放在终端的加密设备中。

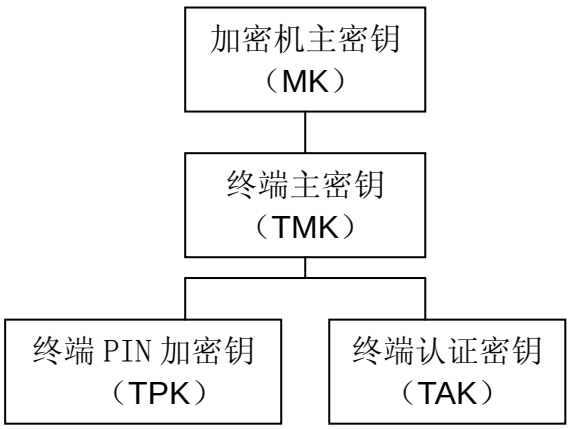
1.1.4 商户主密钥与终端主密钥使用相同的密钥

根据实际系统的不同，采用两级密钥机制的 MIS 商户的终端主密钥和工作密钥可直接使用 MIS 商户的商户主密钥（MMK）和商户工作密钥（PIK/MAK），以减少密钥管理的工作量和降低 MIS 系统密钥管理系统的复杂度。

这种模式的商户需采用“一商户一密”的方式，商户主密钥与终端主密钥使用相同的密钥。终端向商户服务器签到时，服务器将商户服务器向主机签到后获得的工作密钥下载到终端的加密设备上，供终端使用。

1.2 单级密钥机制

MIS 商户单级密钥机制的结构如下图所示：



MIS 商户单级密钥机制结构图

在单级密钥机制中，MIS 商户的服务器端不进行数据的加、解密操作。

在终端处设置的密钥为终端主密钥（TMK）和终端工作密钥，MIS 商户的终

端工作密钥与通常的终端工作密钥类似，分为终端的 PIN 加密密钥（TPK）和终端报文合法性认证密钥（TAK），其中 TPK 用于终端 PIN 数据的加密，TAK 用于终端对数据的正确性认证。

单级终端主密钥的生成及使用和管理方法与常规的终端主密钥相同。

2. MIS 商户密钥管理的权限

2.1 两级密钥机制的 MIS 商户

对直接连接到银联交换系统的两级密钥机制的 MIS 商户（直连商户），商户服务器的主密钥由银联接入机构按本指南的要求生成，并进行分发、保管、注入等操作的管理。密钥的安全由银联各分支机构负责。

商户的工作密钥在 MIS 商户签到时，由银联交换主机经加密机生成，用商户主密钥加密后，下载到该商户的服务器上。

对直接连接到银联交换系统的两级密钥机制的 MIS 商户（直连商户）的终端主密钥的生成、分发、保管、注入等操作和管理一般也由银联各分支机构负责执行。如该商户的收单银行有较严格的密钥管理制度和能力，也可由该商户的收单银行参照本指南的要求负责执行。

凡交易经各银联成员机构转接的 MIS 商户（间连商户），转接机构属于金融机构的，商户密钥和终端密钥的生成、分发、保管、注入等操作可由该金融机构负责，密钥的安全由该金融机构参照本指南的要求进行。转接机构为非金融机构的，密钥的安全由银联相关机构按本指南的要求负责执行。

2.2 单级密钥管理的 MIS 商户

使用单级密钥管理的 MIS 商户的密钥管理要求可参照本节中“终端密钥的管理权限”的方法执行。

第三节　各类终端设备的安全要求

1. 商户服务器的安全要求

对采用两级密钥机制的 MIS 商户的服务器必须配备有硬件加密机，交易传输过程中敏感数据的加、解密必须在加密机内完成。

MIS 商户服务器所配备的硬件加密机的安全要求与交换主机使用的加密机的要求相同,在具体功能方面可有所不同。

在加密机使用过程中的密钥安全管理方面，与本指南中对加密机的安全管理要求相同。其密钥的生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置等过程参照本指南第二章进行管理。

MIS 商户的服务器不允许存储持卡人银行卡的磁道信息、账户信息及个人识别码信息。

MIS 商户的服务器和加密机应放置于专用的房间内，服务器应有专门的管理员管理，对服务器的操作必须有密码控制，并设置不同级别的操作权限，服务器管理员有最高级别的权限，其密码只能由服务器管理员掌握，管理员的密码应定期更换。其他级别的权限只能对一般的交易信息进行读取操作。除服务器管理人员外，其他人员进入该房间应有服务器的管理人员在场。有条件的商户应在房间内安装摄像监控、防盗、IC 卡门警控制系统等安全装置。

2. 收银 POS 一体机的安全要求

受理银行卡的收银一体机必须配备密码键盘，密码键盘的要求与金融终端密码键盘的要求一致。

收银一体机应具有签到、签退功能，签到时进行工作密钥的更新，签退后收银机不能进行受理银行卡的交易。

收银一体机中不得存储持卡人银行卡磁道信息、账户信息及个人识别码。

3. 终端的密码键盘（PIN PAD）

与银联网络联网受理银行卡的 POS、ATM、自助多媒体、商店收银机等终端设备都需配有密码键盘，自动存取款机、自助多媒体终端等设备需配备专门的硬件加密模块，以保护密钥不被泄漏和非法窃取。目前，对不符合要求的设备应设定具体的时限予以淘汰，淘汰的时限中国银联风险管理委员会根据具体情况讨论商定。

凡在银联网络中使用的密码键盘必须通过国家认可的测试部门进行的安全测试和认证。密码键盘内部包含具有加、解密运算处理功能的专用器件，能够进行 PIN 数据的加、解密及报文合法性的认证计算。密码键盘必须能够安全地存储密钥，防止被非法读取。

持卡人键入密码时，密码键盘的显示屏上不能显示明文，只能显示星号(*)。密码键盘键入不同键时，不能发出不同的声音。密码键盘必须安装防窥装置。

持卡人的 PIN 在密码键盘上输入后，必须用终端工作密钥（TPK）加密后以密文形式传输给终端主机。

4. 终端密钥的注入设备

4.1 终端密钥注入设备的合法性认证

终端密钥的注入设备是指密钥枪、母 POS、IC 卡等向终端的加密模块中注入密钥的专用设备。使用这类设备进行终端密钥的传输和注入，其设备的安全必须满足相应要求，并应通过国家认可的测试部门进行的安全测试和认证。

终端密钥注入设备是终端生产或提供商为各自终端产品提供的专用设备。在与终端设备连接注入密钥时应有专门的安全控制机制，使密钥明文只能注入到特定的终端安全模块中而不能被其他任何方式读取。

4.2 终端密钥注入设备中的密钥管理体系

终端密钥注入设备中应设两层密钥，第一层为终端主密钥的管理密钥（TGK），第二层为终端主密钥。终端密钥注入设备中终端主密钥的管理密钥（TGK）与该终端的上级接入的主机相关，并与该主机中的终端主密钥的管理密钥一致。

终端主密钥的管理密钥在终端密钥的注入设备中必须存放在安全加密模块中，不能被读取或非法截取。

终端密钥注入设备可存放多个终端主密钥，并用索引的方式加以区分。存放在终端注入设备中的终端主密钥受该设备中的终端管理密钥的保护。

4.3 向终端密钥注入设备装载密钥

4.3.1 通过密钥生成设备自动装载

用这种方式装载终端主密钥，终端密钥注入设备应与密钥生成设备建有通信接口，并按事先约定的格式将生成的密钥装载到终端密钥注入设备中。通过这种方式装载到终端密钥注入设备中的密钥必须是密钥的密文，其加密密钥为该终端密钥注入设备中的终端主密钥的管理密钥（TGK）。

4.3.2 通过人工方式装载

通过人工方式向终端密钥注入设备装载终端主密钥，密钥生成设备应生成密钥的密文，然后用人工方式将密文注入终端密钥注入设备中，装载的密钥由该终端密钥注入设备中的终端主密钥的管理密钥进行加密。装载的媒介可以用 IC 卡、软盘等设备。

如果只能用明文方式向终端密钥注入设备下载终端主密钥时，则密钥生成、方法、保管及注入的方式必须按本指南中关于分段、分人、分隔控制的方法进行。

4.4 向终端设备注入终端主密钥

终端密钥注入设备向终端设备注入密钥时，必须直接连接到终端的加密设备上进行，执行注入操作时应由密码控制。此外，终端密钥注入设备与终端加密设备之间的连接应有特定的互相认证的方式，具体认证方式可由各终端生产或提供商制定，但认证方式必须能确保除终端专用的加密设备外密钥的内容不能被其他的设备读取。注入到终端专用的加密设备的密钥受终端专用的加密设备保护。

第四章　设备安全管理

1. 硬件加密机（HSM）安全要求及管理

1.1 基本要求

- 硬件加密机用于保护密钥、产生密钥、PIN 的加、解密以及报文鉴别等。这些操作应在硬件加密机中完成，单个完整的密钥和 PIN 明文不能出现在硬件加密机之外。
- 银联各分支机构和联网成员使用的硬件加密机必须通过国家密码管理委员会办公室审核通过。未通过审核的硬件加密机不得在银行卡网络中使用，已经使用的应予以更换；
- 硬件加密机应满足中国人民银行颁布的《银行卡联网联合技术规范》、《银行卡联网联合安全规范》以及中国银联颁布的有关规范中规定的基本功能和性能要求。

1.2 硬件加密机（HSM）设备的功能要求

- 加密机需支持 64 位、128 位、192 位三种长度的密钥。除工作密钥外，其他密钥可由两段或三段组件合成。密钥在生成和注入时应产生每个分量的检验值（Check Value）和密钥合成后的总检验值。
- 加密机需支持单 DES 和三重 DES 的算法。作为选择项，加密机还应具有支持 RSA 算法的功能，作为可选项具有支持 CVN、PVN 校验功能。
- 在加密机上输入密钥组件时，应提供如下三种屏幕显示方式，并可由设备操作员通过参数设置进行选择。

A. 全部显示本段密钥组件的明文（显示时间可控）

B. 全部显示*号

C. 只显示刚刚输入的单个字符

- 加密机应提供密钥组件生成指令，可通过外部命令控制加密机生成密钥组件，同时打印输出或写入 IC 卡中。
- 加密机应设计成具有生产、管理两种可同时运行的状态。在进行管理操作时不应影响正常的生产运行。
- 加密机需提供按索引删除密钥的功能，在注入新的密钥时能够自动提示是否覆盖原密钥。
- 硬件加密设备被强行打开外壳后，应自动销毁机内的所有密钥。

1.3 设备存放及监控

- 应尽量对硬件加密机进行双机热备，避免单机故障造成交易失败和密钥丢失；
- 应将加密机放置在有严格管理的机房内；
- 硬件加密机应存放在带锁机柜中，机柜背板应固定安装；
- 对于硬件加密机的操作，应配备 CCTV（摄像监控）进行全过程监控。

1.4 设备操作

- 每次对硬件加密机的操作，需经批准后严格按照操作手册、操作规程进行，并记录操作日志；
- 在应用系统中禁止和加密机非法连接或用做其他用途；
- 严禁打开加密机机壳。

1.5 设备启用及报废

- 在硬件加密机启用之前，应确定机壳未被拆卸；
- 新购买的加密机应修改加密机相关缺省口令；
- 若使用 IC 卡保存加密机的密钥，应在得到 IC 卡的第一时间更改卡片的缺省密码；卡片应分级分人保存，绝不能交由一个人管理；
- 在硬件加密机报废时，存贮在该设备中的密钥必须删除。

1.6 设备维修与升级

- 根据需求提出书面申请；

- 加密机生产厂商、维护商专人持有效身份证明或介绍信，经证实获准；
- 详细记录工作日志，包括设备类型、故障现象、维修时间等要素。

2. 终端设备安全管理

2.1 终端设备安全要求

- 终端设备内的密码模块应符合国家密码主管部门的规定和相关标准并经过国家认可的权威机构检测通过；
- 终端设备应满足《银行卡联网联合技术规范》、《银行卡联网联合安全规范》中规定的基本功能和性能要求；
- 在操作环境中明文 PIN 和明文密钥应仅出现和存放在于专门设计的密码模块中。

2.2 终端设备操作与监控

- 终端设备技术维护人员与日常业务管理人员应分离，职责明确；
- 应指定专人管理终端设备，或通过闭路电视监控系统对其使用情况进行 24 小时有效监控；
- 每次对终端设备的操作，需严格按照操作手册、操作规程进行。

2.3 设备启用、使用及报废

2.3.1 在终端设备初始化或更新配置之前，应确定：

- 机壳未被拆卸、PIN PAD 粘贴封条、密码模块未被非授权修改或替换；
- 主密钥生成、装载过程应符合本指南要求；
- 主管密码、操作员密码是否为缺省值。

2.3.2 各机构应定期对生产中的终端进行安全检查，检查的要点为：

- 终端硬件（包括 PIN PAD）是否完好
- PIN PAD 封条是否损坏
- 终端软件是否更新过
- 终端操作是否正常

2.3.3 在终端设备报废时，必须：

立即将存储在该设备中的终端主密钥、工作密钥删除和销毁（包括终端及主机数据库），清除操作员、主管密码，销毁终端软件，并由专人监督检查。

2.3.4 终端设备的维修与升级

参见 1.6 有关内容。

3. 设备的物理安全

硬件加密机、终端设备的管理或维护人员应经常对设备进行安全检查，主要包括：

- 设备的物理环境如电源电流及电压、温湿度是否变化；
- 照明、消防及监控设施是否完好，摄像头是否清晰有效，摄像头不能对准键盘或屏幕；
- 设备的外壳是否完好，是否有被拆卸、破坏的迹象；
- 设备有无多余的连接线或外接电缆；
- 终端设备（如 ATM）周围是否张贴有关操作提示；
- 其他各项安全检查指标是否符合要求。

第五章　管理规定与监督检查

银联卡网络参与方应对本单位密钥维护人员岗位设置、工作职责和审批手续做出严格的制度规定，并定期进行专项检查。

1. 组建密钥安全管理工作组

1.1 组织形式

密钥工作组由本单位领导或分管领导任组长，由涉及密钥生命周期全过程的相关部门，如银行卡部门、个人零售部门和科技部门及密钥维护人员共同参加。

1.2 工作职责

- 按照指南规定，结合本单位的实际状况，制定严格而有效的实施细则，落实岗位责任制；
- 制订其他有关的安全专项管理制度，对涉及到密钥的生成、传输、保管各个环节的设备提出相应的安全管理要求，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。
- 负责密钥生命周期，包括生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置等各环节全方位、全过程的规范操作与安全管理。
- 根据密钥特性，妥善保管密钥组件、密码函、IC 密码卡、软件、源代

码、涉及密钥安全管理的各种文档。

- 定期检查密钥安全管理状况，按规定填报有关表格、报告。

2. 密钥安全管理工作人员要求

2.1 基本要求

根据密钥安全管理的要求，各单位需配备专职或兼职人员，专门负责密钥生命周期各环节的具体操作。

2.1.1 专人负责

所有的审批和操作必须指定专人负责，各专管人员均有自己的业务主管权限，未经有权人批准，不得擅自互换或代替。

密钥工作可以兼职，但人员必须相对固定，兼职必须按照本指南第二章与第三章的规定遵循知识分隔、双重控制的原则。

密钥管理员每两年须轮换一次，如密钥管理员自行辞职，应按重要岗位离职进行审核，同时须经六个月的脱密期后，才能让其离开。

2.1.2 基本素质要求

- 具有一定的计算机系统知识基础、接受能力和基本操作技能；
- 了解数据传输加密体系与加密设备的基本操作；
- 具有较强的工作责任心，工作坚持原则。

2.1.3 系统管理与设备维护人员要求

- 熟悉密钥分层管理的原理与基本流程；
- 熟练掌握交换系统主机、前置机、密钥操作 PC 机（如有）、终端设备密钥的操作实务；
- 熟悉加密设备的使用和维护。

2.2 岗位设置

按照密钥安全管理工作的要求，各单位应设置如下一些基本岗位：密钥监督员、设备管理员、设备操作员、密钥生成员（注入、接收工作）、档案管理员、密钥销毁员等。

2.2.1 密钥监督员

- 负责监督本单位密钥安全管理的各项工作，即在整个密钥生命期内监督生成、保管、注入、分发及销毁等操作的正确性；

- 制止不正确操作，杜绝违规操作或超越权限操作的行为；
- 严格考察本单位重要岗位的工作状况，对不适合密钥维护工作或发现有不良行为的人员，提出调整要求；
- 协助完成定期或不定期的专项辅导检查工作。

2.2.2 设备管理员

- 按照本指南第四章中有关设备管理的各项规定，维护加密机等机密设备保持良好的运行状态。
- 负责对其他密钥维护人员讲解有关生成、装载等操作原理、操作步骤、操作要点和注意事项，指导密钥维护人员将密钥建置在各个相关设备的安全模组内，并在审批表格上记录相关操作情况。
- 凡手续不完备的需求，加密机管理员有权拒绝。
- 设备管理员一般可以由机房系统管理员兼任，履行机房安全管理工作的一般性要求。
- 协助完成定期或不定期的专项辅导检查工作。

2.2.3 设备操作员

- 负责加密设备的界面操作，协助完成生成、装载等操作过程。
- 审查有关审批表格的要求是否合理，操作结束在审批表签名认可。凡手续不完备的申请，操作员有权拒绝。
- 协助完成定期或不定期的专项辅导检查工作。

2.2.4 密钥生成员

一般情况下，密钥生成员同时履行注入、保管等工作职责。

- 按照信息择分、随机性、不可测等原则生成密钥组件；
- 分别保管主密钥组件；
- 接收密钥资料（组件），验证接收到的新密钥资料是否受损；
- 键入和改变密钥资料；
- 在监督下销毁密钥组件备份介质；
- 协助完成定期或不定期的专项辅导检查工作。

2.2.5 档案管理员

- 负责收集、归档所有的审批和登记表格等密钥档案，按不同的操作特

征和类型分类，保存在档案室、磁带备份室等安全区域；

- 对档案建立较高的保密级别，未经书面授权，不允许借阅、复制及传播。
- 维护经管理人员授权后使用密钥的记录；
- 协助完成定期或不定期的专项辅导检查工作。

2.2.6 密钥销毁员

在监督下，完成密钥组件备份介质、文档等密钥资料的销毁。

3. 审批制度

对密钥的任何操作必须履行相关审批手续，执行表格登记制度，未经履行审批手续的操作过程一律视同为违章操作，应严格禁止。

中国银联分支机构的审批制度详见《中国银联密钥安全管理暂行办法》。各银联卡网络参与方可参照制定相关细则。

4. 应急措施

银联卡网络参与方应根据本单位的具体情况制定应急措施以防范以外因素导致的业务无法正常运营，应急措施应包括申请审批手续、启动与恢复流程、记录操作日志等内容。

5. 监督

银联卡网络参与方应按照《密钥规则》要求做好自查，并配合做好相关监督与调查工作。

开办外卡收单业务的银联卡网络参与方按照国际组织要求填报相关表格。

银联卡 MIS 商户账户信息安全管理调查问卷 V1.0

填表单位：_____　　（单位公章）

填表人：_____

电话：_____传真：_____

E-mail 地址：_____

一、　MIS 系统基本情况

商户名称			
商户地址及联系方式			
商户代码		商户所属收单机构名称及代码	
MIS 系统名称		上线时间	
系统版本号		当前版本更新时间	
系统开发商		系统维护商	

二、　制度及人员管理

1、系统开发单位是否与开发人员签订了劳动合同，并签订保密协议；

□　是

□　否

2、系统维护单位是否与运维人员签订了劳动合同，并签订保密协议；

□　是

□　否

3、MIS 商户是否与商户系统管理及日常运维人员签订了劳动合同，并签订保密协议；

□　是

□　否

三、　账户信息生命周期安全管理

（一）数据存储

1、MIS 系统客户端存储情况

A．存储的账户信息为：（可复选）

	是否加密存储
☐　银行卡磁道信息	☐ 是　☐ 否
☐　个人标识码（PIN）	☐ 是　☐ 否
☐　卡有效期	☐ 是　☐ 否
☐　卡号	☐ 是　☐ 否
☐　其他信息，请说明_____	

B．所存储账户信息的保存周期为：_____

C．账户信息的存储方式：

☐　数据库　　☐　文件

☐　其他，请说明_____

2、MIS 系统服务器端存储情况

A．存储的账户信息为：（可复选）

	是否加密存储
☐　银行卡磁道信息	☐ 是　☐ 否
☐　个人标识码（PIN）	☐ 是　☐ 否
☐　卡有效期	☐ 是　☐ 否
☐　卡号	☐ 是　☐ 否
☐　其他信息，请说明_____	

B．上述信息的保存周期为：_____

C．账户信息的存储方式：

☐　数据库　　☐　文件

☐　其他，请说明_____

3、在 MIS 客户端刷卡完成交易后，是否要求收银员在客户端或商户收银终端上进行再次刷卡

□　是

□　否

如选择“是”，请回答如下问题：

A．请说明进行“二次刷卡”的原因

_____

_____

B．通过第二次刷卡获取的信息内容（可复选）

□　银行卡磁道信息　　□　个人标识码（PIN）

□　卡有效期　　□　卡号

□　持卡人身份证号码

□　其他信息，请说明_____

（二）数据传输

1、MIS 系统客户端至服务器端的数据传输方式

□　数据专线　　□　专用网络

□　互联网　　□　无线网络

□　其他传输途径，请说明：_____

2、个人标识码（PIN）输入设备

□　密码键盘，请说明密码键盘厂商：_____型号：_____

□　收银机普通键盘

□　其他输入设备，请说明_____

3、个人标识码（PIN）的加密算法及强度

□　DES

□　3－DES

□　其他加密算法，请说明_____

4、MIS 系统客户端至服务器端的其他交易或账户信息（如磁道信息，等）传输过程的安全程度

□　明文传输

□　加密传输，　则请回答如下问题：

A．请说明加密方式：

☐　调用密码键盘的安全芯片进行加密（硬加密）

☐　调用加密程序进行加密（软件密）

B．请说明加密算法及强度：

☐　DES

☐　3－DES

☐　其他加密算法，请说明_____

5、MIS 系统客户端至服务器端的数据传输方式

☐　数据专线　　☐　专用网络

☐　互联网　　☐　无线网络

☐　其他传输途径，请说明：_____

6、MIS 系统服务器端是否对客户端上送的交易请求进行报文转换

☐　是

☐　否

如选择“是”，则请回答如下问题：

A．MIS 系统客户端至服务器端是否进行 MAC 运算

☐　是

☐　否

7、MIS 系统服务器端是否对 PIN 的加密信息进行加解密操作

☐　否

☐　是，　则请回答如下问题：

A．请说明加密方式：

☐　调用硬件加密机进行加密

请说明厂商名称：_____；加密机型号：_____

☐　调用加密程序进行加密

B．请说明加密算法及强度：

☐　DES

☐　3－DES

☐　其他加密算法，请说明_____

（三）数据备份及销毁

1、MIS 系统是否进行数据备份

□　是

□　否

如上题选择“是”，则请回答如下问题：

A．备份数据涉及的账户信息内容为

□　银行卡磁道信息　　□　个人标识码（PIN）

□　卡有效期　　□　卡号

□　持卡人身份证号码

□　其他信息，请说明_____

B．备份数据载体

□　磁带

□　光盘

□　其他介质，请说明_____

C．数据备份周期

□　每日　　□　每周　　□　每月

□　其他，请说明_____

D．数据备份时限

□　三个月　　□　半年　　□　一年

□　其他，请说明_____

2、MIS 系统是否进行数据销毁

□　是

□　否

如选择“是”，请回答如下问题：

A．数据销毁周期

□　三个月　　□　半年　　□　一年

□　其他，请说明_____

B．销毁方式

□　可恢复　　□　不可恢复

（四）数据接口

1、MIS 系统客户端与商户收银终端之间是否有数据接口

□　是，请说明通过接口进行传输的数据内容：_____

□　否

2、MIS 系统服务器端与商户收银系统之间是否有数据接口

□　是，请说明接口传输的数据内容：_____

□　否

3、MIS 系统是否通过其他途径向商户提供账户及交易信息的查询及下载功能

□　是

□　否

如选择“是”，请回答如下问题：

A. 是否可以通过该途径，对服务器端存储或传输的账户及交易信息进行修改

□　是　　□　否

B. 通过该途径可获得的信息中，是否包含如下内容：（可复选）

□　银行卡磁道信息　　□　个人标识码（PIN）

□　卡有效期　　□　卡号

4、MIS 系统客户端安装的读卡器如何驱动

□　由 MIS 系统客户端驱动

□　由商户收银系统驱动

5、显示器是否支持卡片磁道信息的显示功能

□　是　　□　否

6、显示器是否支持个人标识码明文的显示功能

□　是　　□　否

四、　数据访问控制

1、操作系统、应用系统及数据库的管理员是否为同一员工

□　是　　□　否

2、是否为每个用户设置单独的账户及密码

□　是　　□　否

3、是否设置密码容错次数

□　是　　□　否

如选择“是”，请回答如下问题：

A．对何种账户设置密码容错：_____；

B．密码容错次数设置为：_____次；

C．超过容错次数的用户如何解锁，请说明：

_____

_____

4、MIS 系统是否支持商户内部网络的远程登录操作

□　是　　□　否

如选择“是”，请说明系统开放的访问端口（可复选）

□　Telnet　　□　FTP

□　数据库访问端口　　□　其他端口，请说明_____

5、MIS 系统是否支持通过互联网直接远程登录操作

□　是　　□　否

如选择“是”，请说明系统开放的访问端口（可复选）

□　Telnet　　□　FTP

□　数据库访问端口　　□　其他端口，请说明_____

6、MIS 系统正式投产运行后，是否保存通信日志

□　是　　□　否

五、　物理安全管理

1、 商户是否对 MIS 系统单独部署服务器

□　是　　□　否

2、MIS 系统服务器是否可以直接访问互联网

□　是　　□　否

3、在部署 MIS 系统服务器的同一网段内，是否部署有其他网络设备

□　是　　□　否

如选择“是”，请回答如下问题

A．该网段内部署的网络设备数量：_____台；

B．这些网络设备是否可以访问互联网

☐　全部均支持　　☐　部分支持　　☐　全部均不支持

C．支持访问互联网的网络设备，是否可以访问 MIS 系统服务器

☐　全部均支持　　☐　部分支持　　☐　全部均不支持

4、MIS 系统客户端与服务器端之间是否设置防火墙

☐　是，请说明防火墙配置的管理方：_____

☐　否

5、MIS 系统服务器端与银联转接前置系统之间是否设置防火墙

☐　是，请说明防火墙配置的管理方：_____

☐　否

6、商户内部网络与互联网之间是否设置防火墙

☐　是，请说明防火墙配置的管理方：_____

☐　否

7、商户对部署有 MIS 服务器的机房是否设置了访问控制措施

☐　是，请说明

☐　否

如选择“是”，请具体说明商户所采取的机房访问控制措施

_____

_____

8、该商户采用的密钥管理方式

☐　一机（客户端）一密　　☐　商户内多机一密

☐　一商户一密　　☐　全城一密

☐　其他密钥管理方式，请说明_____

9、MIS 服务器是否安装防病毒软件

☐　是　　☐　否

如选择“是”，请回答如下问题：

A．防病毒软件的型号和版本：_____

B．病毒库更新日期：_____，

C．病毒库是否为当前最新版本：　□　是　　□　否

六、　系统开发及版本控制管理

1、MIS 系统开发人员与维护人员是否相分离

□　是　　□　否

2、商户是否掌握 MIS 系统的源代码

□　是　　□　否

3、系统维护商是否掌握 MIS 系统的源代码

□　是　　□　否

4、是否将真实的交易数据信息用于系统开发测试

□　是　　□　否

七、　MIS 商户与第三方管理

1、MIS 商户与其收单机构是否签订书面银行卡受理协议

□　是　　□　否

2、受理协议中是否具备了《银联卡收单机构商户风险管理规则》所要求的必备风险条款

□　是　　□　否

银联卡第三方处理商账户信息安全管理调查问卷 V1.0

单位名称：_____　　（单位公章）

填表人：_____

电话：_____传真：_____

E-mail 地址：_____

第一部分 业务系统安全状况调查表

基本情况			
第三方处理商名称			
第三方处理商地址及联系方式			
第三方处理商入网机构代码		第三方处理商所属收单机构名称及代码	
系统名称		上线时间	
系统版本号		当前版本更新时间	
系统开发商		系统维护商	
是否接入互联网	□是　□否		
账户信息			
系统处理所涉及的账户信息	□二磁道信息 □三磁道信息 □卡片校验码[6] □卡有效期 □卡号 □个人密码 □互联网支付密码 □持卡人身份证件号码 □其他 _____ □无	系统从其他业务系统中获取的账户信息包括	□二磁道信息 □三磁道信息 □卡片校验码 □卡有效期 □卡号 □个人密码 □互联网支付密码 □持卡人身份证件号码 □其他 _____ □无 请说明从什么系统获取信

[6]本问卷中提到的卡片校验码包括 CVN 及 CVN2。

			息：
数据存储			
系统保存的账户信息内容	□二磁道信息 □三磁道信息 □卡片校验码 □卡有效期 □卡号 □个人密码 □互联网支付密码 □持卡人身份证件号码 □其他 _____ □无	系统加密存储的账户信息包括	□二磁道信息 □三磁道信息 □卡片校验码 □卡有效期 □卡号 □个人密码 □互联网支付密码 □持卡人身份证件号码 □其他 _____ □无
账户信息存储方式	□数据库 □文件 □其他 _____	账户信息的使用是否获得发卡机构的许可	□是 □否 □其他 _____
存储系统采用的架构是	□DAS □NAS □SAN □其他_____	是否使用硬盘冗余阵列（RAID）进行数据存储	□是 RAID 级别为_____ □否 □其他_____
数据传输			
传输载体	□专线 □专用网络 □互联网 □无线网络 □其他	加密传输的账户信息包括	□二磁道信息 □三磁道信息 □卡片校验码 □卡有效期 □卡号 □个人密码 □互联网支付密码 □持卡人身份证件号码 □其他 _____ □无
数据加密			
存储或传输时所采用的加密算法	□DES □3DES □RSA □其他 _____	加密密钥的管理方式	□一级密钥 □二级密钥 □三级密钥 □其他 _____
加密方式	□硬加密 □软加密	互联网传输时是否所有信息都加密	□是 □否 □无互联网传输
数据备份			

备份涉及的 账户信息内容	☐二磁道信息 ☐三磁道信息 ☐卡片校验码 ☐卡有效期 ☐卡号 ☐持卡人身份证件号码 ☐个人密码 ☐互联网支付密码 ☐其他 _____ ☐无	备份载体	☐磁带 ☐光盘 ☐其他 _____
备份周期	☐每日 ☐每周 ☐每月 ☐其他 _____	备份保留 时限	☐三个月 ☐半年 ☐一年 ☐其他 _____
数据销毁			
系统账户信息 的销毁周期	☐不销毁 ☐三个月 ☐半年 ☐一年 ☐其他 _____	销毁日志	☐记录日志 ☐不记录日志 ☐其他 _____
销毁方式	☐不可恢复 ☐可能恢复 请描述：		
系统日志			
日志内容	☐用户登录记录 ☐用户操作记录 ☐其他 _____	日志保存时间	☐三个月 ☐半年 ☐一年 ☐其他 _____
硬件备份			
业务系统	☐有备份， 备份方式：_____ ☐无备份	加密机	☐有备份 备份方式：_____ ☐无备份 ☐无加密机
身份验证			
是否为每个用户单 独设定账户与密码	☐是 ☐否	有权访问账户信 息的用户包括	☐操作系统管理员 ☐数据库管理员 ☐应用程序用户

			☐其他 _____ _____
操作系统管理员、数据库管理员、应用系统的管理员是否为同一员工	☐是 ☐否	是否为账户信息访问权限单独设立权限代码	☐是 ☐否
用户密码长度	☐大于等于 6 位 位数 _____ ☐小于 6 位 ☐不限	密码更新	☐定期强制修改 ☐一个月 ☐三个月 ☐六个月 ☐其他 _____ ☐不强制修改
是否自动锁定多次密码输入错误的用户	☐是 ☐否		
报文管理			
系统是否存储外部报文和通信报文	☐存储 ☐不存储	报文中是否包含磁道信息	☐是 ☐否
是否有访问权限的控制	☐有 ☐无	存储方式	☐日志文件 ☐数据库 ☐其他 _____
系统测试			
上线前是否对操作系统及应用系统进行了漏洞扫描？	☐是 ☐否 ☐无法确认	系统升级或安装补丁前是否进行安全检查或测试？	☐是 ☐否 ☐无法确认

第二部分 问答

一、 制度与检查

问题1. 是否按照《银联卡账户信息与交易数据安全管理规则》、《银联卡收单机构账户信息安全管理标准》的要求，制定本单位有关账户信息安全管理规定？

□是　　□否

如是，请给出规定名称：_____

请以电子或书面形式提供相关文档

□是　　□否

问题2. 每年或每次安全事件后是否对安全制度进行完善或修订，以确保制度符合业务实际？

□是　　□否

问题3. 2004 年 1 月以来，本单位是否开展过账户信息安全管理的内部检查？

□是　　□否

如是，请说明检查次数：____

二、 人员与组织管理

问题4. 本单位是否建立了负责信息安全的组织机构？

□是　　□否

问题5. 从事信息安全管理相关工作的人员是否是专职人员？

□是　　□否

问题6. 对从事信息安全管理相关工作的人员是否有资质要求？

□是　　□否

如是，请具体说明：

□国际注册信息安全专家（CISSP）

□注册信息安全专业人员认证(CISP)

□国家信息安全技术水平考试(NCSE)

□注册信息安全审计师（CISA）

□思科认证网络专家（CCIE）

□其它，请说明：_____

问题7.　2004 年 1 月以来，是否组织相关人员参加过账户信息安全方面的学习或培训？

□是　　□否

问题8.　是否与有权访问敏感账户信息的员工签订保密协议或在劳动合同中包含保密条款？

□全部　　□部分　　□否

三、 访问控制管理

问题9.　访问账户信息相关的业务系统是否都必须经过身份验证？

□是　　□否

问题10.　是否根据“业务需要”[7]的原则来控制对敏感账户信息的访问？

□是　　□否

问题11.　建立具有账户信息访问权限的用户是否需要经过审核？

□是　　□否

问题12. 在业务系统中，操作系统、数据库及应用系统的管理员用户是否为同一员工？

□是　　□部分是　　□否

问题13. 具有使用 SQL 语句进行数据库查询权限的用户包括：

□数据库管理员　　□特定应用程序用户

□无用户限制　　□其它

问题14. 在应用系统中，是否存在开发人员、维护人员以及业务人员使用相同账号的情况？

□是　　□部分　　□否

问题15.　在同一类用户中，是否存在多名用户共用同一个用户账号的情况？

□是　　□否

问题16.　密码管理

a)　分配给不同用户的初始密码是否相同？

□是　　□否

[7]“业务需要”原则是指仅向因业务需要而必须访问数据的用户提供访问权限。

b)　　是否存在分配给用户的初始用户名和密码相同的情况？

□是　　□部分　　□否

c)　　是否所有的系统强制要求用户更改初始密码？

□是　　□部分　　□否

d)　　是否所有的系统对密码的长度及组成都有要求？

□是　　□部分　　□均无

e)　　是否所有系统均要求用户定期修改密码？

□都要求　　□部分系统要求　　□均未要求

问题17. 如果配置文件保存了数据库访问用户（用户名、密码等）信息，对其的访问是否有限制？

□是　　□部分　　□否

问题18. 对于应用于程序内部（如配置文件）的数据库访问用户，其密码是否定期更换？

□是　　□部分　　□否

问题19. 登陆系统的用户一定时间（如 10 分钟）不进行操作时，应用系统是否要求重新验证身份信息？

□是　　□否

问题20. 相关人员离职或调离岗位后，是否及时注销其在系统中的用户与密码？

□是　　□否

问题21. 是否将真实的账户信息数据用于开发测试？

□是　　□部分　　□否

四、 敏感信息保存场所的管理

问题22.工作人员进入敏感信息保存区域时，是否验证其身份并登记？

□是　　□否

问题23.对于涉及敏感账户信息的存放介质（纸面、光盘、磁盘、磁带等），是否按照文档管理规定分级妥善保管？

□是　　□否

问题24.是否有专人定期审查外来人员访问记录？

□是　　□否

五、 备份与档案管理

问题25. 交易日志、清算信息等关键数据的备份

备份介质_____ 备份方式(同城同处/同城异处)_____

备份频度_____ 保管方式_____ 保存时间_____

问题26. 应用软件的备份

备份介质_____备份方式(同城同处/同城异处)_____

备份频度_____保管方式_____ 保存时间_____

问题27. 在存储敏感帐户信息时，是否采取“存储业务系统必须使用的最少数据”的策略？

□是　　□否

问题28. 对于已经不再需要的备份数据，是否对其进行销毁？

□是　　□否　　□其他_____

问题29. 对于所存储和备份的敏感数据，是否采用加密方式保存？

□是（加密算法_____）　　□否　　□其他_____

六、 访问日志

问题30. 是否建立了账户信息数据的访问日志？

□是　　□否

问题31. 对于通讯设备的访问是否有控制和记录？

□是　　□否

问题32. 是否通过有效手段对各类访问日志进行保存和保护（如将日志集中备份至中央日志服务器、对日志文件进行访问控制等）？

□是　　□否

问题33. 是否定期对访问日志进行审核？

□是　　□否

如是，审核周期为_____

七、 网络安全

问题34. 在生产网络上部署任何安全产品是否取得了相关机构和法规的认证？

□是　　□否

问题35. 是否通过对交换机、路由器进行配置（如划分 VLAN、建立访问地址控制列表等）对不同网络进行隔离？

□是　　□否

问题36. 生产系统网络和每个外部网络（包括 Internet、无线网络、外部专线等）之间是否采用防火墙进行隔离？

□是　　□否

问题37. 生产系统网络是否采用了异构防火墙？

□是　　□否

问题38. 生产系统网络是否构建 DMZ 区和内部网络？

□是　　□否

问题39. 防火墙是否按照来自外部网络的主机只能访问 DMZ 区而不能访问内部网络的原则配置？

□是　　□否

问题40. 防火墙是否完全或部分开放内部网络对外部网络或 DMZ 区的访问？

□是　　□否

问题41. 是否将数据库服务器等存放重要信息的主机放置在内部网络而不是 DMZ 区？

□是　　□否

问题42. DMZ 中的主机是否可以访问内部网络中的数据库服务器？

□是　　□否

问题43. 对于所配置的防火墙，是否修改默认管理员口令和相关默认的安全参数（如 WEP 密钥、默认 SSID 和密码、SNMP 通讯字符等）？

□是　　□否

问题44. 防火墙除开放业务系统必需的端口外，是否关闭其他所有端口？

□是　　□否

问题45. 是否制定了防火墙配置策略，并与实际的配置一一对应？

□是　　□否

问题46. 防火墙是否采用了端口/网络地址转换（PAT/NAT）技术以防止内部网络地址暴露在外部网络？

□是　　□否

问题47. 连接到生产网络的任何个人电脑是否安装了单机防火墙系统？

□是　　□否

问题48. 是否采用入侵检测系统（IDS）监控网络入侵？

□是　　□否

问题49. 是否周期性对网络系统进行安全漏洞扫描？

□是　　□否

八、 防病毒管理

问题50. 是否禁止在生产系统上使用个人移动存储介质，包括软盘、U 盘、移动硬盘等？

□是　　□否

问题51. 各类生产应用系统是否都部署了防病毒软件？

□是　　□部分　　□否

问题52. 连接到生产网络的任何个人电脑是否安装了单机防病毒系统？

□是　　□否

问题53. 防病毒系统是否正常运行？

□是　　□否

问题54. 防病毒软件病毒码是否保持最新？

□是　　□否

如是，病毒码更新周期是_____

问题55. 连接到生产网络的任何个人电脑是否安装了单机防病毒系统？

□是　　□否

问题56. 是否配备相应的人员负责防病毒工作的日常管理及维护？

□是　　□否

问题57. 是否周期性查看病毒威胁日志，并对日志中的威胁记录进行处理？

☐是　　☐否

如是，查看周期是_____

九、 事件及应急处理

问题58. 本机构以往是否发生过账户信息安全事件？事件的类型包括但不仅限于：账户信息泄漏、由于误操作引起的账户信息丢失等。

☐是　　☐否

如是，请提供相关材料，材料应包括以下内容：事件的经过，造成的损失，采取的整改措施及效果等。

问题59. 是否已书面制定对账户信息泄漏事件的应急处理机制，包括对数据本身、对所影响的单位和人员、对媒体的处理？如有，请一并提供。

☐是　　☐否

第三部分　典型案例分析

[案例一] TJX 公司账户信息泄漏案

（一）案情简介

2007 年 1 月，美国零售商 TJX 公司发现其客户交易系统被黑客入侵，失窃数据中包括 4,570 万个支付卡的账户信息，45.5 万名客户的驾驶证号码、军人证号码、身份证号码，以及他们的姓名和地址等敏感信息。

此案中，黑客首先利用 TJX 公司下属某零售门店无线局域网安全防护强度不足的漏洞，通过大功率无线接收设备搜寻到该门店的无线信号，并成功破解无线局域网密码，入侵该门店局域网；随后，黑客借助 TJX 公司后台服务器与零售门店局域网之间的连接通道，利用 TJX 公司后台服务器在远程访问控制和管理等方面存在的漏洞，以零售门店局域网内的终端为“跳板”，成功侵入 TJX 公司的后台数据库系统。入侵公司后台数据库系统后，黑客不仅窃取了 TJX 公司留存在数据库系统中的持卡人账户信息和身份信息（包括卡片磁道信息、持卡人身份证号、军人证号等个人信息），还在 TJX 公司的后台服务器上安装了流量捕获软件，记录经过 TJX 公司传输的交易数据，从中提取银行卡磁道信息，并通过电子邮件直接发往黑客制定的服务器。

据估计，此次数据泄露事件给 TJX 公司造成的各项损失大约在 2.56 亿美元，此外，美国联邦商务委员会还要求 TJX 公司必须每隔一年委托独立的第三方机构进行账户信息安全合规检查，并持续 20 年。

（二）风险点分析

该案显示出 TJX 公司的账户信息安全管理存在以下薄弱环节：

1、违规留存持卡人账户信息

违规留存持卡人敏感账户信息，特别是银行卡磁道信息是导致案件发生的根本原因；同时，TJX 公司对过期或使用完毕的账户信息也未及时予以销毁和删除。

2、TJX 公司对后台数据服务器的远程访问控制和管理存在漏洞

首先是远程访问端口长期处于开启状态；其次是远程登陆访问的身份验证机制过于简单，未采用令牌、生物特征等安全级别较高的验证措施；同时，TJX 公司对于远程访问操作的接入设备、允许操作的业务范围等也未进行严格限制和

管理，使得黑客得以利用上述漏洞，远程登陆后台数据库通过 FTP 等高风险协议大肆下载系统中存储的敏感账户信息。

3、内部管理和监督制度不完善

TJX 公司没有对公司后台数据系统及网络平台进行定期巡检，未能及时发现黑客的入侵行为；同时，也没有建立完善的访问日志管理制度，导致事后难以对案件进行追踪调查。

4、TJX 公司对后台数据库的网络防火墙管理存在漏洞。

TJX 公司的后台数据库不仅与互联网直接联接，同时也通过零售店终端与互联网间接相联，但 TJX 公司在“互联网－零售店终端－公司后台数据系统”的信息通道中未安装防火墙，使得黑客轻易通过上述通道入侵公司后台数据系统；其次，TJX 公司虽然在“互联网－公司后台数据库”的直接通道上设置了防火墙，但管理策略存在漏洞，允许以电子邮件的方式向外部互联网服务器发送磁道信息等账户信息，使得黑客得以利用上述漏洞，长期窃取交易传输过程中的持卡人账户信息。

5、TJX 公司零售门店无线局域网的安全保护措施不够。

TJX 公司零售门店的无线局域网使用了安全级别较低的 WEP 技术，且开启了 SSID 广播功能，导致黑客能通过大功率接收设备成功搜索到门店的无线信号，并成功破解。

（三）风险防范措施及建议

针对此次账户信息泄漏案中暴露出的风险问题，应在以下环节加强风险防范和建议：

1、加强账户信息存储、使用和销毁各环节的安全管理

首先各类业务参与方业务系统、数据库等设备均不得留存银行卡磁道信息等敏感账户信息，且对于数据系统中已留存存量账户信息的，应立即全面清理和删除；其次，对于银行卡主账号和持卡人身份证件号码等信息，应建立并严格落实存储、使用与销毁登记制度。

2、加强后台数据服务器的远程登陆访问控制与管理

应严格审批和管理对后台数据系统的远程登陆和访问。一是仅在业务开展需要时激活远程登录端口，访问结束后立即关闭；二是加强远程登陆访问的身份验

证，采取口令、令牌或生物特征等验证措施；三是严格限制对通过远程网络或无线网络接入后台数据库的设备、用户、业务范围和操作权限。

3、加强内部监督管理，建立并严格执行完善的日志记录和检查机制

应建立严格的日志记录和审核制度，详细记录每次登陆核心数据库的用户名称、登陆时间、访问内容等，并定期对日志记录进行审核；同时，定期开展账户信息安全自查，对公司的业务系统、网络平台、通讯日志（报文）等进行定期检查和监控，

4、为后台数据库安装防火墙，并优化防火墙安全策略

应后台数据库和外部网络之间安装边界防火墙，同时优化防火墙的安全策略，严格禁止通过电子邮件方式传输卡片磁道信息等账户信息。

5、加强无线局域网的安全防范

无线局域网应采取 WAP 或 WAP2 等安全级别较高的加密技术，并关闭 SSID 广播功能。

[案例二] Heartland 公司账户信息泄漏案

（一）案情简介

2009 年 1 月 22 日，美国第六大银行卡处理商 Heartland Payment Systems Inc.（以下简称 Heartland 公司）的计算机系统发生大规模银行卡账户信息泄漏事件，涉及 1.3 亿持卡人数据，成为迄今历史上最大一笔账户信息泄漏案。

据 Heartland 公司对外报道，黑客于 2008 年下半年利用 Heartland 公司网页漏洞，使用 SQL 注入技术入侵了 Heartland 公司的内部网络，并控制了 Heartland 公司位于加州、新泽西及荷兰等地的远程电脑，继而利用这些远程电脑作为跳板发起攻击，侵入公司的内部生产网络（支付处理系统）。黑客利用 SQL 注入获取 Heartland 公司支付处理系统的访问权限后，在服务器上安装后门软件及嗅探程序。嗅探程序实时监控并拦截服务器发送和接收的持卡人账户信息，再通过后门软件定期将持卡人数据发送到入侵者指定的服务器。为了隐藏痕迹，入侵者关闭了记录出入流量的日志程序，并使用了代理服务器，黑客安装的后门程序能够逃过二十多种防病毒软件的查杀，还能够很好的隐藏自己。

2010 年，各国际卡组织向 Heartland 公司主张近 1.9 亿美元的赔偿金，用于向因本次泄露事件遭受损失的发卡机构支付换卡费用补偿和伪卡损失赔偿。

（二）风险点分析

该起案件暴露出 Heartland 公司在网络系统本身、以及内部管理、检查监督等方面存在以下薄弱环节：

1、Heartland 的网络系统本身存在安全漏洞。

Heartland 公司网络系统中一段用于公司网页的程序代码存在两个方面的漏洞。该段程序存在 SQL 注入漏洞，使得黑客可以利用 SQL 注入技术成功入侵公司的外部网络；同时，该段程序还为黑客通过外部网络入侵公司生产网络提供了通道，使得黑客最终利用该漏洞，以公司外网的终端为“跳板”，入侵公司支付处理系统，获取系统的访问权限，并注入后门和嗅探程序窃取持卡人信息。

2、Heartland 公司账户信息安全内部管理和检查机制有待完善

（1）经过后续调查，存在 SQL 注入漏洞的程序代码是在数年以前制作公司网站时编写的，但公司一直未能发现和识别，直到黑客在 2007 年利用 SQL 注入

技术发起针对性的攻击，并成功入侵公司网络。

（2）Heartland 公司在入侵发生后到案件爆发近 1 年多的时间里，未能及时通过系统监控、定期检查等手段发现黑客入侵行为和植入公司支付处理系统的恶意程序，使得黑客得以长期潜伏，窃取海量持卡人账户信息。

3、通讯日志（报文）管理存在薄弱环节。

Heartland 没有严格管理系统流量监控日志记录，并进行定期检查，未能及时发现黑客非法关闭监控数据流量日志的行为。同时，Heartland 公司在核心系统的访问登陆日志管理方面存在薄弱环节，如可能未设置核心系统访问日志机制，或未对访问日志进行严格管理和定期检查，导致系统未及时预警黑客在支付处理系统的非法登陆行为。

（三） 风险防范措施及建议

针对此案暴露出的风险问题，建议在以下方面加强风险防范：

1、定期对系统进行升级，消除安全漏洞。

应定期打补丁、版本升级等手段对公司的网络系统进行升级优化，及时发现和消除系统中存在的安全漏洞。

2、进一步完善系统日志记录的安全管理机制，包括：

（1）建立完善的系统访问控制日志记录和检查审批制度，详细记录每次访问的用户、登录方式、访问操作等内容，以及时发现黑客的非法登录行为。

（2）针对各项系统日志记录（包括系统登录访问日志、系统流量监控日志等），建立完善的日志记录及审核机制，采取有效措施，防止系统日志（被非法篡改，采取监控软件保证日志的一致性与完整性，每天应对系统日志进行审核，以及时发现系统中的异常行为。

3、加强账户信息安全内部管理和检查机制

应定期（如每年）或在网络发生重大变更后，对系统账户信息安全管理状况进行检查和评估，，并聘请有资质的机构开展账户信息安全外部合规评估，以及时发现系统中存在的安全隐患，并采取整改措施。

[案例三] 境内某 MIS 商户账户信息泄漏案

（一）案情简介

2010 年第一季度，黑龙江地区一家 MIS 商户发生系统端泄露案件，涉及泄漏银行卡 5 千余张。

据调查，犯罪嫌疑人刘某为该 MIS 商户收银系统维护人员。2008 年 11 月至 2010 年 2 月期间，刘某利用在某 MIS 商户维护收银系统工作便利，窃取了该商户 2008 年 11 月系统升级改造前留存的 5000 余条银行卡磁道信息。随后，又利用该 MIS 商户在会员卡信息系统管理方面存在的薄弱环节，从该商户会员登记系统中窃取了大量的姓名、身份证号、联系方式等个人身份信息，并利用收银机记载会员卡和银行卡刷卡间隔几秒钟的特点，按时间将会员身份信息和银行卡磁道信息进行匹配，再通过电话银行等渠道，根据会员身份信息测试银行卡密码。最后，刘某利用在维修收银系统过程中接触收银台的机会，窃取大量用过后回收的空白购物卡，将银行卡磁道信息写入购物卡中，制成伪卡后在 ATM 上取现。

截止案发时，刘某已成功破解近 60 张卡片的密码，并制成 20 余张伪卡进行盗刷，造成 3 家发卡机构 20 余万元经济损失。

（二）风险点分析

该案是一起典型的内部人员作案，而 MIS 商户在账户信息安全管理方面存在的诸多漏洞也给欺诈分子实施作案提供了便利：

1、违规留存敏感账户信息是导致案件发生的根本原因。

该 MIS 商户在收银系统中违规留存了交易中传输的银行卡磁道信息。虽然该商户在 2008 年 11 月对系统进行了升级，停止了违规留磁的行为，但该商户并未及时对此前违规存储的存量账户信息进行有效清理，并最终导致案件的发生。

2、核心数据系统的访问控制管理不善。

商户对收银系统、会员登记系统等核心系统的访问控制存在薄弱环节，违背了“业务需要”、“双人控制”等基本原则：

（1）商户对收银系统的访问控制管理不到位，没有实行严格的权限管理和监督机制，使得欺诈分子在对核心收银系统进行操作时，可以随意访问并下载系统中存储的敏感数据信息，同时在业务操作时也没有人员在场进行监督，为欺诈

分子作案提供了便利。

（2）商户会员系统的访问权限管理存在漏洞。商户会员系统中存储了大量的会员姓名、身份证号、联系方式等个人敏感信息，应对其进行严格的管理。该案中，商户没有对会员系统的访问权限进行有效控制，使得欺诈分子作为收银系统的维护员工，仍有权限访问会员卡数据系统，并拷贝和下载其中的敏感信息；

3、商户对回收的空白购物卡等重要物品保管不严。

商户回收的购物卡属于重要物品和凭证，应进行妥善的保管，并建立相关记录登记制度。该案中，MIS 商户未落实上述基本管理要求，回收的购物卡随意摆放在收银柜台，使得欺诈分子有机可乘。

4、核心岗位人员的职业道德教育不到位。

商户收银系统维护人员等核心岗位工作人员的职业道德素养不高，导致内部核心人员利用商户管理漏洞实施作案。

（三）风险防范措施及建议

针对在此次账户信息泄漏案中暴露出的问题，应在以下方面重点加强管理和风险防控：

1、停止违规留磁，并及时清理前期留存的账户信息

应立即停止违规留存银行卡磁道信息的行为，同时对前期系统留存的磁道信息进行及时清理和销毁，并严格落实双人在场的要求，一人操作、一人监督，并详细记录销毁操作人员、监督人员、销毁时间、地点、销毁方式等，并由操作人员和监督人员签字确认。

2、加强收银系统的访问权限管理和控制

应加强收银系统的访问控制和管理，严格落实“业务需要”和“双人控制”等基本原则，根据业务开展需要分配相应的访问和操作权限，严格限制和管理不同权限可以访问的数据范围；同时，加强日常监督。在权限分配和对核心数据库的访问上应严格落实一人操作、一人监督。

3、加强持卡人个人身份信息的保护和访问控制

如对于会员系统中存储的持卡人身份证号等账户信息，应进行妥善保护，建立严格的使用与销毁管理制度，控制身份证号的使用范围；同时，根据“业务需要”原则分配访问权限，严格禁止没有业务需要的人员访问持卡人个人信息。

4、加强对重要物品和拼争的管理

应加强对空白购物卡等重要物品的管理，建立严格的回收、保管、领取、发放和登记管理制度，并予以落实。

5、加强核心岗位人员的职业道德教育

应组织开展内部宣传培训工作，重点加强核心岗位人员的职业道德培训和法律意识教育，切实提高内部员工的职业道德水平。

[案例四] 收单机构账户信息泄漏案

（一）案情简介

2005 年下半年，某市多名持卡人向当地公安局报案，称银行卡并未离身，但卡内资金已被他人盗用。

公安机关通过分析涉案卡片的交易记录，发现某收单机构的 ATM 机具为信息泄漏点，但在实地检查终端机具时并未发现机具存在被安装侧录设备的痕迹，因此初步判断存是收单机构内部人员或终端机具维护商存在作案嫌疑。经深入调查侦破，发现此案系该收单银行的 ATM 机具维护商内部工作人员舒某所为。舒某为该 ATM 机具维护商的应用软件工程师，并同时兼任 ATM 机具维护工作。舒某工作期间，编写了一个后门程序，并在 ATM 日常维护时将程序安装在位于某地区的两台 ATM 机具上，非法获取交易中银行卡账户信息（包括磁道信息和密码）。随后，舒某利用 ATM 机故障维修的机会将程序所记录的一个月内所有在这两台 ATM 机上发生交易的银行卡磁道信息及密码拷入笔记本电脑，并利用该 ATM 机具仅对银行卡密码进行软加密的漏洞破解银行卡密码，之后在网上购买了白卡、读卡器，先后制作伪卡 100 多张，疯狂盗取卡内资金。

经查证，犯罪嫌疑人累计窃取了 7 千余张卡片的账户信息，涉及 19 家发卡银行，造成经济损失 20 余万元。

（二）风险点分析

该案属于内部人员作案，欺诈分子利用兼职 ATM 维护工作的便利，编写后门程序截取交易中的银行卡磁道信息和密码，破解后制成伪卡实施盗刷，暴露出收单机构在账户信息安全管理方面存在以下问题：

1、收单机构对第三方专业化服务机构的监督管理力度不足

该案中收单机构将 ATM 机具的日常维护工作外包给第三方机构，但并未采取必要的监督管理手段，使得 ATM 的账户信息安全完全依赖于第三方机构自身的管理水平，缺乏有效保障；

2、程序开发人员和维护人员兼职兼岗

该案件中犯罪嫌疑人既是 ATM 机具软件的开发人员，同时还兼任 ATM 机具的维护工作，使得犯罪嫌疑人得以轻易利用工作便利将自己编写的后门程序植入

ATM 机具，窃取银行卡账户信息。

3、ATM 机未落实对 PIN 的硬加密要求

该起案件中，ATM 机具未配备具备硬加密功能的密码键盘，对密码加密使用软加密算法，因此欺诈分子得以编制后门程序，在加密之前截取密码明文，实施伪卡欺诈。

（三）风险防范措施及建议

针对在此次账户信息泄漏案中暴露出的问题，应在以下方面重点加强管理和风险防控：

1、收单机构应加强对第三方外包服务机构的监督管理

首先应加强对第三方专业化服务机构的风险培训，提高风险意识，并督促第三方机构提高账户信息安全管理水平；其次应加强对第三方机构的监督和管理，如在合作协议中包括账户信息安全保密和责任条款、加强对第三方机构的日常监督巡检等措施；

2、加强人员岗位设置管理

收单机构应督促第三方专业化机构进一步完善人员岗位设置，严格禁止开发人员和维护人员相互兼职兼岗；

3、收单机构应加强 ATM 终端机具安全管理

对 ATM 终端机具进行升级改造，配备硬加密模块，实现对 PIN 进行双倍长密钥算法的硬加密，确保交易传输中任何环节不出现密码明文，防止密码明文被窃取的风险。

5、加强核心岗位人员的职业道德教育

应通过培训、学习等形式，提高核心岗位人员的职业道德素质。

[案例五] 东莞某酒店侧录案[8]

（一）案情简介

2008 年 5 月，某行卡中心接到部分信用卡持卡人投诉，均称卡片未丢失，却在北京发生盗刷交易。公安机关经过侦查，确定东莞的 2 家五星级酒店为 CPP 信息侧录点，并一举抓获以白某为首的欺诈犯罪团伙。

经调查，2007 年下半年，犯罪嫌疑人白某先后在广东、北京等地购买了磁卡数据采集器、读写卡器、空白磁卡等制造伪卡的工具，并在广东东莞分别勾结 3 名五星级酒店的前台服务人员，利用工作便利，在客人刷卡结账时，用侧录设备窃取持卡人信用卡磁道信息，并以每条 5 元－10 元的代价提供给白某。白某随后将非法窃取的磁道信息制成伪卡，再通过网上广告与另一犯罪嫌疑人张某、任某结成团伙，由上述 2 人介绍白某到北京某欺诈犯罪商户刘某处进行集中盗刷套现。

该犯罪团伙再北京先后利用多家银行的 POS 机具进行伪卡集中套现，并伪造消费记录，共计造成损失 90 余万元。

（二）风险点分析

上述侧录案件暴露处收单机构在商户风险管理方面还存在风险漏洞：

1、收单机构商户风险管理存在薄弱环节

（1）商户入网审核不严格，使得欺诈团伙得以在多家银行申请 POS 机具，为伪卡集中盗刷套现提供的渠道。如东莞酒店侧录案中，白某制作伪卡后在北京某套现商户处大量集中盗刷伪卡；

（2）商户日常巡检落实不到位，使得商户内部人员与欺诈分子勾结，长期窃取持卡人账户信息；

（3）商户人员职业道德和法律意识不足，内部工作人员与欺诈分子勾结作案。

2、持卡人风险意识不足

该案同时暴露出持卡人风险意识不足，在酒店刷卡时被欺诈分子伺机侧录

[8] 侧录是指不法分子通过在终端机具上安装侧录仪器，盗录持卡人磁条信息，出卖给伪卡制作集团或自行制作伪卡的犯罪行为。

卡片。

（三）风险防范措施及建议

针对在此次账户信息泄漏案中暴露出的问题，收单机构应采取以下风险防范措施：

1、加强商户风险管理

一是应加强商户入网审核。审核“三证一表”，并拍摄实地照片，防止欺诈分子骗领 POS 机具后，实施集中伪卡盗刷；二是应加强商户日常巡检回访，重点检查商户终端机具有无被改造，商户关键岗位操作人员是否严格合规开展业务等；三是应加强商户交易风险监控，如短时间内的交易频率，非营业时间交易频率、短时间内不成功交易次数等等，发现可疑情况及时进行调查回访。

2、加强持卡人风险教育

应通过在网络、媒体、社区、宣传手册等多种渠道，加强持卡人宣传教育，提高持卡人安全防范意识。