附件 2

《银联卡收单机构账户信息安全管理标准》主要修订点列表

修订规则	修订项目	修订前	修订类型	修订后
标准名称	调整标准名称	《银联卡收单机构账户信息安全管理标准》	调整	《银联卡支付信息安全管理标准》
第一章 总则	拓展标准适用范围	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。	调整	1.2 适用范围 本标准适用于基于银联卡开展支付业务的主体及为支付业务主体提供相关服务的机构，包括但不限于: 1.2.1 直接参与方 是指直接参与支付业务的主体，包括但不限于银联卡发卡机构、基于银联卡的支付账户发行方 、涉及银联卡交易的银行卡清算机构、从事银联卡收单业务的收单机构、银联卡收单特约商户、基于银联卡的二维码应用服务方等。 1.2.2 间接参与方 是指向支付业务直接参与方提供专业化服务的机构，包括但不限于银联卡卡片生产厂商、聚合技术服务商、托管服务提供商 、受理终端厂商、软件供应商及其他专业化服务机构。 对于上述机构，只要业务涉及银联卡卡号的采集、传输、处理、存储，均适用本标准。

第二章 基本要求	延伸账户信息定义	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。	调整	2.1 支付信息定义 支付信息是指银联卡上记录的账户信息、基于银联卡开展支付业务的网络支付账户信息、身份鉴别信息、支付业务涉及的必要个人信息和其他支付相关信息。包括但不限于: 2.1.1 银联卡上记录的账户信息 包括银联卡卡号、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，以及基于上述信息产生的支付标记。 2.1.2 基于银联卡开展支付业务的网络支付账户信息 包括网络支付账户、用户注册名、用户登录名、用户ID等，以及基于上述信息的支付标记。 2.1.3 身份鉴别信息 包括个人标识代码(PIN)，网络支付业务中的登录密码、手势密码、查询密码、支付密码、动态口令、短信验证码、密码提示问题答案，指纹、虹膜、人脸等个人生物特征信息，预付卡支付密码等。 2.1.4 支付业务涉及的必要个人信息 包括但不限于姓名、身份证和护照等证件类识别标识、手机号码、固定电话号码、电子邮箱、工作及家庭地址以及支付业务中采集或产生的其他个人信息。 2.1.5 其他支付相关信息 机构或商户名称、机构或商户编码、批量制卡文件、加密密钥、终端编码、终端序列号、设备标识、支付应用软件标识、IP地址、交易位置信息等。

	细化账户信息分级	2.1 定义 根据是否允许存储将账户信息分为敏感账户信息和其他账户信息	调整	2.2 支付信息分级 按照支付信息对完成支付交易的影响程度，分为敏感支付信息、重要支付信息和一般支付信息。
	扩大敏感账户信息范围	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。	调整	2.2.1 敏感支付信息 指作为支付要素能够直接完成交易，且一旦泄漏将对信息主体的资金安全造成严重影响的支付信息，包括但不限于卡片有效期、磁道信息（含芯片等效磁道信息）、卡片验证码（CVN 及 CVN2）、个人标识代码（PIN）、网络支付密码、预付卡支付密码以及用于身份鉴别的个人生物特征信息。
第四章 组织管理	优化组织保障策略	无	新增	3.1.1 设置支付信息安全管理委员会 3.1.1.1 应设置支付信息安全管理委员会，委员会成员应至少涵盖本机构研发、测试、运维、风控、清算等与支付信息安全管理相关部门和具体负责人。 3.1.1.2 支付信息安全管理委员会职责应包括但不限于：规划和建设支付信息安全管理机制、审批支付信息安全管理制度和流程、管理支付信息安全管理岗位职责和权限、推动支付信息安全管理制度落实、统筹支付信息安全事件应急处理。 3.1.2 明确支付信息安全责任人 3.1.2.1 应通过正式书面授权指定支付信息安全责任人。 3.1.2.2 支付信息安全责任人职责应包括但不限于：统筹支付信息安全合规评估工作，开展支付信息安全事件先期处理、后续跟踪和损失处理等，配合相关调查和评估鉴定。

	补充外部合作方及人员管理要求	无	新增	3.2.5 外部人员管理 3.2.5.1 外部人员物理访问受控区域前，应先提出书面申请，批准后由专人全程陪同，并登记备案。 3.2.5.2 应采取有效措施（如临时工牌等），识别和区分外部人员和内部员工。 3.2.5.3 外部人员离场时，应及时回收临时工牌或其他类似凭证。 3.2.5.4 外部人员接入网络访问系统前，应先提出书面申请，批准后由专人开设账号、分配权限，并登记备案。 3.2.5.5 外部人员完成系统访问后，应及时终止其所有的访问权限并删除相应账号。 3.2.5.6 获得系统访问授权的外部人员应签署保密协议，不得进行非授权操作，不得非授权获取和变更支付信息。 4.3 外部风险防范策略 对于涉及支付信息处理的外部合作方及服务提供商，应建立支付信息安全管理机制，明确其支付信息保护要求及责任，防范因外部因素引发的支付信息泄漏风险。
第五章 访问控制	新增日志审计要求	无	新增	5.7 日志审计 5.7.1 应建立日志审计机制。 5.7.2 日志审计内容应包括但不限于: 所有执行安全功能的设备日志（如防火墙、IDS/IPS）以及安全事件; 所有用户访问支付信息的行为记录; 所有涉及支付信息处理系统的日志记录。 5.7.3 应每年至少对日志记录进行一次审计，将审计结果及时向本机构支付信息安全管理委员会或支付信息安全责任人进行报告，并妥善保管审计结果等记录文件。

第六章 支付信息生命周期安全管理	补充账户信息生成保护要求	无	新增	6.1.1 支付信息生成 6.1.1.1 制卡文件要求 应保证制卡文件生成、存储、传输的安全，制卡文件使用完毕后应进行安全清除。 应设定制卡文件保存期限，定期检查并及时清除超过保存期限的制卡数据。 6.1.1.2 网络支付业务开通要求 通过绑定银联卡开通网络支付业务时，应对银联卡卡号、卡片验证码、卡片有效期等支付信息进行脱敏，支持基于支付标记化技术的交易处理，从源头控制信息泄漏风险。 二维码等条码生成时应不包含任何敏感支付信息并对生成的动态条码信息设置有效时限。
	明确账户信息采集原则	无	新增	6.1.2 支付信息采集基本要求 6.1.2.1 采集支付信息应遵循“业务必须”和“最小化”原则，不得收集与所提供服务无关的支付信息。 6.1.2.2 采集支付信息必须经信息主体明示同意，并确保所采集信息来源的可追溯性。
	明确加密采集磁道信息要求	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。	调整	6.1.3.4 从受理终端（包括但不限于个人支付终端、公共自助终端、商户终端）采集磁道信息（含芯片等效磁道信息）时应进行加密保护，包括但不限于使用加密芯片实现硬加密。

	优化网络支付业务采集敏感账户信息要求	6.1.1 个人标识代码的加密 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 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。	调整	6.1.4 网络支付业务采集敏感支付信息 6.1.4.1 开展网络支付业务时，不得委托或授权无支付业务资质的外部合作方及服务提供商采集敏感支付信息。 6.1.4.2 通过互联网、移动设备、固定电话等支付渠道输入卡片有效期、CVN2、个人标识代码（PIN）、网络支付密码等敏感支付信息时，应通过强效加密等技术措施进行保护，包括但不限于使用安全控件、密码软键盘等。 6.1.4.3 应采取有效措施防止外部合作方及服务提供商获取、留存敏感支付信息。
	新增支付交易报文安全要求	无	新增	6.2.1ATM 及 POS 交易报文安全要求 6.2.1.1 为保障交易报文信息的唯一性和可追溯性，对于 ATM 终端，各商业银行要在交易报文中包含终端编码。 6.2.1.2 为保障交易报文信息的唯一性和可追溯性，对于 POS 终端（含连接扫码设备的 POS 终端），各收单机构应在交易报文中包含受理机构编码、商户编码、终端编码、终端序列号、终端应用版本编号等信息。 6.2.2 网络支付交易报文安全要求 6.2.2.1 网络支付交易报文应包含设备标识 、IP 地址 、手机号码 、账户 ID（或哈希值） ，以保证交易报文的必要完整性。 6.2.2.2 网络支付交易报文应同时满足以下安全要求: 应防止对交易的重放攻击; 应保证交易的抗抵赖性，包括但不限于数字证书、电子签名等技术手段; 应用系统应保证在一段时期内同一商户交易、订单的唯一性; 应用系统应检查交易请求报文中记载的交易要素是否完整，拒绝不

				完整的交易请求。
	补充传输协议和版本要求	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）。	调整	6.2.3 传输加密 6.2.3.1 在公共、开放网络上传输支付信息时，应对支付信息进行加密或通过加密通道传输。 6.2.3.2 采用加密通道传输时应符合以下要求: 使用强壮的安全协议，例如使用安全套接字层（SSL）或传输层安全（TLS）、互联网协议安全（IPSec）等。使用 SSL/TLS 协议时，应使用安全的版本，取消对存在安全隐患版本以及弱加密套件的支持。安全协议所使用密码算法应符合国家密码管理部门相关密码管理要求。
	新增跨境传输要求	无	新增	6.2.4 跨境传输要求 因业务需要，确需向境外提供支付信息的，应符合国家法律法规和相关标准要求并进行安全评估，同时通过业务规则及协议等有效措施，要求境外的信息接收机构为所获得的支付信息保密。
	新增存储地域要求	无	新增	6.3.1.1 境内开展支付业务、提供支付业务相关服务过程中，采集或产生的支付信息应在境内存储。

	细化敏感支付信息存储要求	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。	调整	6.3.2 敏感支付信息存储要求 6.3.2.1 不得记录或存储非本机构的敏感支付信息，包括但不限于以下位置: 涉及支付信息处理的应用系统; 受理终端、支付应用软件、Web 应用等到服务器之间以及服务器与服务器之间的通信日志; 交易记录表、银行卡绑定关系表等数据库表。 6.3.2.2 对于本机构的敏感支付信息，应进行强效加密后存储，防范明文泄漏的风险。 6.3.2.3 个人生物特征信息应存储在本地安全环境范围内，存储时应采用技术措施处理后再进行存储，如仅存储个人生物特征信息的摘要。
	优化个人生物特征信息存储要求	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。	调整	6.3.3 重要支付信息存储要求 6.3.3.1 当两种或两种以上重要支付信息组合、重要支付信息与一般支付信息组合构成交易授权的完整要素时，如银联卡卡号与证件类识别标识、手机号码，应对系统中存储的全部或部分信息采取加密或屏蔽等措施。 6.3.3.2 登录密码、查询密码等密码类信息，应进行强效加密后存储，防范明文泄漏的风险。
	明确授权使用原则	无	新增	6.4 支付信息使用 6.4.1 基本要求 6.4.1.1 使用支付信息时，不得超出已征得信息主体明示同意的使用范围。 6.4.1.2 因业务需要，确需超出上述使用范围使用支付信息的，应再次征得信息主体的明示同意。

	补充卡片有效期显示要求	无	新增	6.4.4 支付信息显示要求 银联卡受理终端打印的各类交易凭条上，除预授权交易外，不得打印卡片有效期。
	新增硬件加密机等管理要求	无	新增	6.6.3 加密设备 6.6.3.1 硬件加密设备应采用双机热备，避免单机故障造成密钥丢失，影响正常交易。 6.6.3.2 硬件加密设备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。 6.6.3.3 应配备摄像系统监控对硬件加密设备的操作，但不得监控到注入内容。 6.6.3.4 硬件加密设备的上线、下线应有严格的审批手续和记录。 6.6.3.5 至少双人控制钥匙或密码来执行对硬件加密设备的操作，并根据不同的操作权限，设置不同的操作密码。
第七章 系统及网络安全管理	提高恶意代码防范要求	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	调整	7.2.2 恶意代码防护 应对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: 7.2.2.1 所有运行 Windows 操作系统的主机应部署防病毒软件。 7.2.2.2 对于运行其他操作系统且未安装防病毒软件的主机，应定期评估其是否能够充分防范恶意代码攻击，并根据评估结果确认是否需要安装防病毒软件。 7.2.2.3 允许公共访问的服务器应部署防病毒软件或者采用其他恶意代码检测手段。 7.2.2.4 维护允许使用的软件列表并指定软件获取方式，严格限制下载和安装列表以外的软件。 7.2.2.5 应及时更新防病毒软件及病毒库，并定期对系统进行扫描，

		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。		对扫描结果进行分析处理。 7.2.2.6 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。 7.2.2.7 所有外部存储介质（软盘、光盘、移动硬盘和 U 盘等）在使用前，必须进行病毒扫描。 7.2.2.8 防病毒软件应一直处于保护状态，用户无法禁用防病毒软件或修改其策略。
	完善安全开发流程	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。	调整	7.3.1.2 系统上线之前进行代码安全审计和渗透测试，识别可能的恶意代码和安全漏洞。
	新增开源软件使用要求	无	新增	7.3.1.3 如应用系统使用开源软件，应对开源软件预先进行安全测试评估，使用其稳定版本，并安装最新的安全补丁。
	新增变更下线的管理要求	无	新增	7.3.2.2 变更下线的程序、相关配置文件、数据和日志文件应至少备份保存一年。

	提高外部漏扫和渗透测试要求	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; 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。 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。	调整	7.4.4 漏洞扫描 应定期及在网络发生重大变更时，对系统进行漏洞扫描，具体包括: 7.4.4.1 至少每季度执行外部网络漏洞扫描，外部网络漏洞扫描应由中国银联授权的第三方专业化检测机构执行; 7.4.4.2 至少每季度执行内部网络漏洞扫描，内部网络漏洞扫描可由机构或中国银联授权的第三方专业化检测机构执行; 7.4.4.3 在网络发生重大变更时应进行内部和外部网络漏洞扫描。网络重大变更应包括但不限于安装新的设备、网络拓扑结构调整、防火墙配置调整、应用系统升级等; 7.4.4.4 应根据需要重复执行漏洞扫描，以确保扫描发现的漏洞得到有效修复。 7.4.5 渗透测试 应定期及在系统发生重大变更时，对系统进行渗透测试，具体包括: 7.4.5.1 至少每年执行一次外部渗透测试，外部渗透测试应由中国银联授权的第三方专业化检测机构执行; 7.4.5.2 至少每年执行一次内部渗透测试，内部渗透测试可由机构或中国银联授权的第三方专业化检测机构执行; 7.4.5.3 在系统发生重大变更时应进行内部或外部渗透测试，系统重大变更包括但不限于操作系统升级、应用系统升级、网络拓扑变更、Web 服务器变更等。 7.4.5.4 应根据需要重复执行渗透测试，以确保测试发现的漏洞得到有效修复。

第八章 银联卡受理终端及支付应用软件安全管理	完善终端技术标准符合性要求	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。	调整	8.1.1 技术标准符合性 受理终端应符合《银联卡受理终端安全规范》及其他相关规定的要求，且需通过中国银联授权的第三方专业化检测机构检测并获得安全认证，以确保受理终端采集支付信息时的安全性。
	新增终端业务权限管理要求	无	新增	8.1.3 终端业务权限 应根据《银联卡受理终端业务准入管理办法》相关规定，加强对预授权、预授权完成撤销、消费撤销、联机退货等功能开通的审批和交易监控，记录并管理终端与交易权限的匹配关系，以确保支付信息处理的合理性和风险事件的可控性。
	新增终端程序管理要求	无	新增	8.1.4 终端程序管理 8.1.4.1 应保障终端程序安全、稳定、完整、有效地执行交易流程。 8.1.4.2 应确保终端程序功能与开通业务类型要求一致。 8.1.4.3 应采取措施防止未经授权私自篡改终端程序、窃取支付信息等违规行为，确保终端程序具备抵御恶意破坏等黑客攻击的能力。
	新增终端注册管理要求	无	新增	8.1.5 终端注册管理 应采用终端入网签名、唯一性标识等技术措施，确保终端注册信息真实可靠，交易可追溯到每一台终端。

	新增终端采购及出入库管理要求	无	新增	8.1.6 终端设备管理 8.1.6.1 应加强受理终端选型、采购、验收等环节的安全管理，确保受理终端的技术标准符合性。 8.1.6.2 应加强受理终端出入库记录，并建立完整的库存台账。 8.1.6.3 应建立并维护受理终端清单（包含终端型号、序列号、布放位置等信息），持续开展终端抽巡检工作，确保布放的终端与合格样品的一致性，防范终端被非法改装风险。
	明确支付应用软件安全检测要求	无	新增	8.2.1 技术标准符合性 支付应用软件应符合《银联卡支付应用软件安全规范》的要求，且需通过中国银联授权的第三方专业化检测机构检测并获得安全认证，以确保支付应用软件采集支付信息时的安全性。
	新增支付应用软件完整性要求	无	新增	8.2.2 支付应用软件完整性 8.3.2.1 支付应用软件应采用防逆向工程保护措施，如支付应用软件采取代码化指令、反调试、代码混淆等技术手段，防范攻击者对支付应用软件的反编译分析。 8.3.2.2 应对支付应用软件进行签名，标识支付应用软件的来源和发布者，保证客户所下载的支付应用软件来源于所信任的机构。

	新增客户端软件运行安全	无	新增	8.2.3 支付信息处理安全 8.2.3.1 支付应用软件应提供自定义软键盘，支持键位随机布局；输入支付密码时，应提供即时加密功能；完成身份鉴别后应及时清除缓存，防止信息泄漏。 8.2.3.2 应提供防截屏功能，防止在显示支付信息、付款条码等内容时，被恶意程序窃取。 8.2.3.3 支付应用软件业务逻辑应能够防范跨账户越权操作、业务欺骗等风险，确保响应报文仅包含必要的支付信息。
	新增合规评估要求	无	新增	9.1 支付信息安全合规评估要求 9.1.1 评估范围 所有涉及支付信息采集、传输、存储、使用等环节及可能影响支付信息安全的业务处理系统及技术支撑环境。 9.1.2 自评估要求 涉及支付信息采集、传输、存储、使用等环节的支付业务直接参与方应每年根据本标准开展支付信息安全自评估，并保留自评估相关记录；同时，通过合作协议等方式要求提供专业化服务的间接参与方每年开展支付信息安全自评估，并保留相关记录。 9.1.3 外部评估要求 9.1.3.1 直接参与方 涉及支付信息采集、传输、存储、使用等环节的支付业务直接参与方需每年聘请中国银联风险管理委员会授权的第三方专业化检测机构开展外部合规评估，包括但不限于: 信息安全等级保护级别为三级及以下的发卡机构; 基于银联卡的支付账户发行方; 从事银联卡收单业务的收单机构；基于银联卡的二维码应用服务方; 在自有 Web 应用或支付应用软件采集支付信息的银联卡收单特约商

				户、达到《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）规定的外部合规评估条件的银联卡收单特约商户。 对于上述机构，如已通过外部合规评估可不再开展自评估。 9.1.3.2 间接参与方 直接参与方开展外部合规评估时，评估范围应包含间接参与方提供的涉及支付信息处理的服务。如直接参与方提供了间接参与方的外部合规评估材料，可不再评估相关服务。
	优化账户信息安全相关审计要求	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。	调整	9.2 支付信息安全相关审计要求 9.2.1 在日常专项审计和检查等基础上，每年至少开展两次支付信息安全管理相关的内部或外部全面审计，并保留相关记录。 9.2.2 审计内容应至少包括支付信息安全策略的科学性、组织架构及岗位设置的合理性、员工对支付信息安全管理要求和职责的熟悉程度、内控制度和外部风险防范策略的有效性、交易及支付信息保护要求的准确性、支付业务设施的安全性等。
	补充安全策略持续改进要求	无	新增	9.3 安全策略持续改进 9.3.1 每年根据支付信息安全合规评估结果和审计情况，并在业务、系统或外部环境发生重大变更时，调整支付信息安全管理策略，并确保得到有效执行。 9.3.2 每年在支付信息安全管理策略调整后，应加强员工支付信息安全培训，确保所有涉及支付信息的员工熟悉最新的支付信息安全管理要求和保护责任。 9.3.3 每年定期维护外部合作方及服务提供商列表、合作协议，并监控其对本标准的遵从状态，持续改进外部风险防范策略。