ICS 35.240.40
A 11

JR

中华人民共和国金融行业标准

JR/T 0120.2—2016

银行卡受理终端安全规范
第2部分：受理商户信息系统

Security specification for bank card terminals—

Part 2:Merchant information system

2016-09-06 发布　　2016-09-06 实施

中国人民银行　发布

目　次

前　言

JR/T 0120—2016《银行卡受理终端安全规范》由以下五个部分组成：

——第1部分：销售点(POS)终端；

——第2部分：受理商户信息系统；

——第3部分：自助终端；

——第4部分：电话支付终端；

——第5部分：PIN输入设备。

本部分按照GB/T 1.1—2009 给出的规则起草。

本部分为《银行卡受理终端安全规范》的第2部分。

本部分由中国人民银行提出。

本部分由全国金融标准化技术委员会(SAC/TC 180)归口。

本标准负责起草单位：中国人民银行科技司、中国银联股份有限公司。

本部分起草单位：中国工商银行、中国农业银行、中国银行、中国建设银行、交通银行、中国光大银行、招商银行、中国邮政储蓄银行、中国金融电子化公司、中金金融认证中心有限公司、北京银联金卡科技有限公司、银联商务有限公司、福建联迪商用设备有限公司、飞天诚信科技有限公司、无线网络安全技术国家工程实验室、工业和信息化部计算机与微电子发展研究中心（中国软件评测中心）、信息产业信息安全测评中心。

本部分主要起草人：李伟、王永红、陆书春、李兴锋、杜宁、陈则栋、曲维民、汤沁莹、王禄禄、吴永强、赵哲、贾铮、周皓、王兰、李伟（中国银联）、吴潇、张志波、潘润红、邬向阳、杨倩、刘运、张晓欢、谭颖、严伟锋、曹宇、俞纹雯、周英斌、夏庆凡、王治纲、王伯铮、于华东、李同勋、冯健诚、代伟、钱菲、李穗申、李石超、顾才泉、侯智勇、张晓琪、高志民、高强裔、李超、高峰、周诗扬、孙茂增、马哲、尚可、胡盖、张俊江、蒋利兵、郭鑫、林眺、于海涛、白艳雷、李琴、宋铮、刘健、董晶晶。

银行卡受理终端安全规范

第2部分：受理商户信息系统

1 范围

本部分规定了受理商户信息系统在数据、应用、密钥体系、访问控制、传输及管理等方面的安全要求。

本部分适用于存储、处理、传输持卡人数据的受理商户信息系统。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

JR/T 0001 银行卡销售点（POS）终端技术规范

JR/T 0002 银行卡自动柜员机（ATM）终端技术规范

JR/T 0120.1 银行卡受理终端安全规范 第1部分：销售点（POS）终端

3 术语和定义

JR/T 0001和JR/T 0002中界定的以及下列术语和定义适用于本文件。

3.1

账户信息 account information

银行卡上记录的所有账户信息以及与银行卡交易相关的用户身份验证信息。记录在银行卡上的信息包括：卡号、磁条信息、卡片验证码2。与银行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。

3.2

交易信息 transaction information

银行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、卡片验证码2。

3.3

卡片验证码 2 card verified number（CVN2）

在邮购/电话订购等非面对面交易中对银行卡的卡片合法性进行验证的代码。

3.4

审核记录 audit trail

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操作设备的行为是否已经发生。

3.5

身份鉴别 authentication

用来验证身份或证实信息完整性的过程。

3.6

信息 information

机构转移资金、设定等级、发放贷款、处理交易等所用的数据。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。包含处理系统的软件部分。

3.7

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。

3.8

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。

3.9

静态密码 static password

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已知信息来实现的。

3.10

动态密码 dynamic password

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。

3.11

保密性 confidentiality

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。

3.12

完整性 integrity

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。

3.13

敏感数据（信息） sensitive data（information）

应防止被非法泄露、修改或破坏的数据，如个人标识码（PIN）、完整磁道信息、卡片验证码、卡片有效期等信息，及加密密钥以及包含设计特点、状态信息的数据。

3.14

敏感功能 sensitive functions

用于处理如PIN、密钥和口令等敏感数据的功能。

3.15

敏感服务 sensitive services

调用敏感功能的服务。

3.16

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。

4 缩略语

JR/T 0120.1中界定的以及下列缩略语适用于本文件。

DMZ 非军事区域(De-militarized Zone)

FTP 文件传送协议(File Transfer Protocol)

HTTP 超文本传输协议(Hypertext Transfer Protocol)

IPSEC 网际网路协定安全规格(Internet Protocol Security)

KEK 密钥加密密钥(Key Encryption Key)

LDAP 轻量级目录访问协议(Lightweight Directory Access Protocol)

MK 主密钥(Master Key)

MAK MAC加密工作密钥(Mac Key)

OWASP 开放式Web应用程序安全项目(Open Web Application Security Project)

RADIUS 远程验证拨入用户服务(Remote Authentication Dial-In User Service)

RBAC 基于规则集的访问控制(Rule-Base Access Control)

SQL 结构化查询语言(Structured Query Language)

SSH 安全外壳(Secure Shell)

TACACS 终端接入控制器接入控制系统(Terminal Access Controller Access Control System)

VPN 虚拟专用网(Virtual Private Network)

WEP 有线等效保密 (Wired Equivalent Privacy)

XSS 跨站脚本(Cross Site Scripting)

5 信息系统数据安全

5.1 磁道信息、卡片验证码、PIN、卡片有效期

禁止在身份认证结束后存储敏感数据：

——禁止存储磁条中磁道信息，为了降低风险，如果业务中需要在对账日内保留磁条中的一些数据字段（如持卡人姓名、主账号和服务代码等），应只存储业务必须的数据字段，不应存储卡片验证码、PIN、卡片有效期；

——认证后，不应存储用于校验无实卡交易的卡片验证码，不应存储PIN或者加密的PIN块；

——认证后，应及时清除系统在内存中存放的敏感数据，防止残留的敏感数据被挖掘；

——安全删除银行卡受理商户信息系统以前版本存储的任何磁道数据、卡片验证码、PIN和PIN块数据；

——安全删除任何来自日志文件、调试文件和从客户接收的其他数据源且用于调试或解决争执目的的敏感数据，确保系统中未存储磁道数据、卡片验证码，个人标识码、卡片有效期、PIN或PIN块数据。

敏感数据不应明文形式传输，且在传输过程中应防止泄露，防止被侦听。

5.2 银行卡主账号

严格控制银行卡主账号的使用和存储。银行卡主账号的存储仅限业务处理、清分清算、差错处理、业务对账、交易查询与分析、案件协查、风险管理和控制。

5.3 持卡人身份证件号码

采取严格措施保护持卡人身份证件号码，严格控制身份证件号码的使用。对开展基于用户定制类交易需要存储、传输身份证件号码时，应建立合适的销毁登记制度。

5.4 保护存储的持卡人数据

保护方法是持卡人数据保护的关键组件，如加密、截磁、掩模和哈希等。也可采用其他保护存储数据的有效方法。如：

——无必要不存储持卡人数据，不需要完整的PAN时应截断持卡人数据，以及不在未加密的邮件中发送PAN；

——在超过受理商户定义保留期后，软件提供商应指导受理商户清除持卡人数据；

——显示PAN时采用屏蔽措施，只显示前6位和后4位数字，其余应屏蔽显示；

——尽可能使PAN无法从存储空间直接复制，如便携式数字媒体、备份媒体、日志，可采用以下措施：

- 基于强效加密算法的单向哈希；
- 截取部分PAN信息；
- 索引记号与索引簿（索引簿应安全地存储）；
- 带有相关密钥管理流程和过程的强效加密算法。

——如采用了优于文件加密或数据库列级加密的磁盘加密，逻辑访问应独立于本地操作系统的访问控制机制，如避免使用本地系统账号或活动目录账号。解密密钥应不能和用户账号绑定或关联；

——受理商户信息系统应防止持卡人数据的加密密钥泄露，密钥明文应存放在硬件加密模块中；

——对于所有加密持卡人数据的密钥，应制定并实施全面的密钥管理流程和程序。

5.5 数据的使用

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

不应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，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。

5.6 数据的销毁

各受理商户信息系统可根据本商户的实际情况确定账户信息及交易数据的保存期限，通常不超过两年。对于超出保存期限的账户信息及交易数据，应及时销毁，以免造成信息的泄漏。

——对保存到期或已经使用完毕的数据建立销毁登记制度；

——通过以粉碎、焚毁、多次复写、消磁、破坏等方式对存储于设备或介质中的无用或过期的账户信息与交易数据进行销毁处理。

6 信息系统应用安全

6.1 日志

银行卡受理商户信息系统安装以后，默认设置应该记录所有用户的访问（特别是具有管理员权限的用户），并把所有的活动和用户本身关联起来。

——建立账户信息及交易数据访问与使用的日志记录机制。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。具体事件包括：

- 用户对账户信息的访问；
- 失败的尝试访问；
- 系统管理员的操作；
- 对系统日志的访问；
- 其他涉及账户信息安全的系统操作。

——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；

——采取有效措施，防止系统日志被非法篡改：

- 严格控制对系统日志的访问，只有工作需要的人员才能查看系统日志；
- 及时将系统日志备份到专用日志服务器或安全介质内；
- 及时将无线网络日志复制到内部专用日志服务器；
- 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，系统日志记录至少保存一年。

6.2 审计

银行卡受理商户信息系统应执行自动审计跟踪和监控访问。本项要求包括:

——应提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

——应保证无法单独中断审计进程，无法删除、修改或覆盖审计记录；

——审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

——应提供对审计记录数据进行统计、查询、分析及生成审计报表的功能；

——应制定安全策略。

6.3 配置文件

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，除系统管理员外，不应向其他系统用户开放对配置文件的访问权限。

6.4 开发、测试

开发、测试要求如下：

——所有的安全补丁以及对系统和软件的配置变更经过测试后才能部署，应满足：

- 所有输入的有效性；
- 所有错误处理的有效性；
- 所有安全加密存储的有效性；
- 所有安全通信的有效性；
- 所有基于角色访问控制的有效性（RBAC）。

——将开发、测试和生产环境分离；

——对开发、测试和生产环境进行职责分离；

——生产数据（实际有效的PAN）不允许被用于测试或开发。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，应遵循5.5节中的具体要求；

——生产系统正式上线之前，移除所有测试数据和测试账号；

——在正式上线或向消费者发布前，对定制代码进行复审，检查可能存在的编码弱点。

6.5 Web 应用

所有的Web的银行卡受理商户信息系统，包括内部、外部，以及产品的WEB管理应基于安全编码指南，如开放Web应用安全项目（OWASP）指南。软件开发流程中通常会出现的编码弱点包括：

——跨站脚本攻击（XSS 或 CSS）；

——注入缺陷，特别是 SQL 注入缺陷（验证用户数据的有效输入不能修改命令和队列的内容），另外也要考虑 LDAP 和 Xpath 以及其他的注入缺陷；

——恶意文件执行；

——不安全的目录对象索引；

——伪造的跨站请求；

——信息泄漏和错误处理不当；

——失效的身份认证和会话管理；

——不安全的加密存储；

——不安全的通信；

——限制 URL 失败。

6.6 变更和控制

软件厂商对软件配置的修改应按照变更控制过程进行。变更控制过程包括：记录所受到的影响、有关部门管理层审批、备份程序、测试操作功能、恢复程序、交易处理机制。

6.7 不必要的服务或协议

银行卡受理商户信息系统不应使用不必要和不安全的服务、协议。应具备以下材料：

——业务开展所必须的服务/端口记录表；

——除 HTTPS、SSH 和 SFTP 外，使用其他协议的原因和相关文件；

——被允许使用的风险协议（如 FTP 等）的原因和相关文件，相关文件包括使用这些协议所实施的

安全特征等。

6.8 弱点检查

软件厂商应制定新发现安全漏洞的处理流程并进行漏洞测试，任何提供的或系统环境要求的软件及系统都包含在该流程中。

软件厂商应制定流程来保障及时开发、部署补丁和升级程序，包括通过安全的途径分发补丁和升级程序、在分发和部署过程中维护补丁和升级代码的完整性。

6.9 网络环境安全

银行卡受理商户信息系统应在安全的网络环境中使用，并不影响其他本规范要求的设备、应用程序和配置。如银行卡受理商户信息系统环境不应影响防病毒软件、防火墙配置或其他的设备。

数据库不应与WEB服务部署在同一台服务器上，数据库服务器不应部署在DMZ区。

6.10 远程软件更新

应用程序的更新通过远程访问受理商户信息系统的方法分发时，软件厂商应告知受理商户只在需要使用的时候开启调制解调器，使用完毕立即关闭。

使用VPN或其他的高速连接时，软件厂商应建议受理商户合理配置防火墙以启用安全连接。

7 信息系统密钥体系安全

系统对传输数据加密涉及到的密钥包括：主密钥（MK）、密钥加密密钥(KEK)和工作密钥(WK)。

——加密机主密钥MK用于对密钥加密密钥(KEK)进行加密保护，每台加密机只设置一个MK。MK存储在硬件加密机中，受硬件保护，不能被读取。MK由若干分量合成，每个分量应由不同人员掌握；

——KEK用于对WK进行加密保护，存储在加密机和密码键盘中。KEK由若干分量合成，每个分量应由不同人员掌握。KEK应有安全保护措施，只能写入并参与运算，不能被读取；

——WK由硬件加密机生成，利用KEK加密后下载，并由KEK加密存储。WK在下载和传输时都应以密文形式出现，严禁明文传输。WK分为PIN加密密钥（PIK）、MAC计算密钥（MAK）、磁道信息加密密钥（TDK）三类。

8 信息系统访问控制安全

8.1 身份鉴别

银行卡受理商户信息系统安装完毕后，对于装有银行卡受理商户信息系统的PC、服务器和数据库的访问应进行身份认证。建议使用以下措施管理用户：

——应保证用户名唯一；

——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；

——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。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；

——如操作系统和安全管理软件中带有软件开发商设定的预用户名和密码，成员机构、成员机构的代理机构或商户应指定专人对预设用户名和密码进行管理，并在使用预设用户时更改其默认密

码。

8.2 权限管理

对于系统功能及数据的访问权限，应根据“最小授权，必需知道”的原则，保证只能访问相关业务所必需的数据。

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、职责分离的原则，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。

8.3 系统登录控制

应制定系统登录控制策略，设置系统登录失败次数上限，对达到控制限制的操作，应暂时冻结该用户账号，经系统管理员对用户身份验证并通过后，再恢复其用户状态。

用户登录系统后，工作暂停时间达到或超出10分钟，系统应要求用户重新进行身份验证。

8.4 密码口令安全控制

使用推荐的标准加密传输和存储系统中的密码。应用程序联机访问数据库时不允许将数据库密码明文赋予任何环境变量。

——为了增加密码的安全性，静态密码要求如下：

- 密码长度不少于6位，应由数字、字母组成，可包含特殊字符，不应设置简单密码；
- 密码应在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。密码不可共享，或被他人（包括管理人员）获取；
- 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）；
- 禁止记录密码；
- 密码在传输时应进行加密。

——为保证静态密码的完整性，应保证：

- 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，或在其他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。

——应确保在使用动态密码系统时进行合理的验证：

- 选择适当需要激活的身份验证标识，如个人识别码（PIN）、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，或终止赋予该安全标识的准入权限。

8.5 远程访问控制

远程访问控制要求如下：

——银行卡受理商户信息系统应不影响双重认证机制的使用，允许使用远程接入拨号用户服务（RADIUS）、终端访问控制器访问控制系统（TACACS）等技术以及在支持个人数字证书的VPN；

——如果银行卡受理商户信息系统可以远程访问，远程访问银行卡受理商户信息系统应使用双重认证机制。如果厂商、销售人员或客户可以远程访问，那么远程访问应该以安全的方式进行；

——应严格限制通过远程网络或无线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：

- 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；
- 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；
- 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；
- 在进行远程登录操作时，不应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；
- 远程登录操作应采用双因素验证方式，例如支持个人数字证书的VPN等；
- 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；
- 对于远程操作记录的访问、更改、删除应由获得合法授权的专人负责，同时通过系统的身份认证。

8.6 物理访问控制

物理访问控制要求如下：

——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；

——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；

——物理隔离区域进入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，监控录相资料至少保存三个月；

——外部来访人员应获得审批授权并进行身份登记后方可进入物理隔离区域；

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

9 信息系统传输安全

9.1 无线传输

银行卡受理商户信息系统使用无线传输时，应保证无线传输技术的安全。如使用WiFi方式传输，应采用WPA 、WPA2等技术进行保护，采用IPSEC VPN 或SSL/TLS进行传输加密。

9.2 公开网络敏感数据传输

如果银行卡受理商户信息系统向公开网络发送或协助发送持卡人数据，应支持使用强壮的加密算法和安全协议，如安全套接字层（SSL）/传输层安全（TLS）和IP 安全协议（IPSEC）来保护敏感持卡人数据在开放/公共网络上的传输。

银行卡受理商户信息系统不允许通过终端用户消息技术（如e-mail，即时消息，聊天）发送未加密的PAN。

10 信息系统的安全管理

10.1 网络及防火墙

网络及防火墙要求如下：

——所有接入互联网的系统都应安装防火墙，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；

——对于防火墙的管理建立规范制度，指定专人负责维护防火墙的配置与管理，具体包括：

- 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）；
- 明确业务必需的服务和端口清单；
- 所有允许从防火墙通过的传输协议都应经过审批（包括HTTPS、SSH和SFTP等）；
- 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。

——建立路由器的管理规范，按季定期检查路由器的规则配置；

——对网络访问进行控制，可采取以下措施：

- 限制通过互联网访问DMZ区IP的流量；
- 禁止通过互联网访问内部网络IP地址；
- 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；
- 将数据库放置于内部网络，通过防火墙与DMZ区隔离；
- 禁止内部网络地址通过互联网访问DMZ区；
- 保护并同步路由器配置文件，确保运行配置文件与初始化配置文件具有相同的安全配置；
- 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；
- 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。

10.2 设备安全管理

设备安全管理要求如下：

——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）；

——特别对于无线网络设备，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；

——当通过主控台以外的网络连接对设备进行管理时，应基于SSH、VPN或SSL/TLS协议等加密通道对设备进行管理；

——每台服务器只承担一项主要功能(如Web服务器、数据库服务器应该分别部署在不同的设备上)，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。

10.3 防病毒管理

系统应安装防病毒软件，以防范病毒、木马及恶意软件：

——在所有系统中部署防病毒软件（UNIX及大型主机系统除外）；

——严格限制下载和使用免费软件或共享软件；

——通过设置防病毒软件的服务器及时更新病毒库；

——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；

——所有外部存储介质（如软盘、移动硬盘、U盘、存储卡等）在使用前，应进行病毒扫描。

10.4 系统补丁管理

系统补丁管理要求如下：

——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，安全补丁应在通过综合风险评估后，确认需要再安装；

——建立并执行系统升级、版本更新等变更操作的审批和操作流程，详细登记升级软件的版权、来源、版本等信息；

——在安装安全补丁或变更系统及软件配置之前，应通过相应测试，方能投产运行。

10.5 系统安全检查

系统安全检测要求如下：

——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：

- 安装新的设备；
- 网络拓扑结构调整；
- 调整防火墙配置；
- 应用系统升级。

——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：

- 操作系统升级；
- 应用系统升级；
- 网络拓扑变更；
- WEB服务器变更。

——应采用入侵检测系统对网络数据传输进行实时监控；

——对系统核心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。核心文件包括：服务器配置文件、防火墙配置文件、交换机配置文件及路由器配置文件等。

11 其他方面安全

11.1 实施准则的更新（测试流程）

在实施准则中标明所有引用本规范的要求。至少每年复查一次，及时更新以保持文档与软件的更新、同步要求。

11.2 客户培训

开发并执行培训和通信流程，以确保销售人员知道如何执行银行卡受理商户信息系统以及相关的系统和网络。每年更新一次培训材料，在新的版本发布时更新培训材料。