**PCI标准变更内容---2017**

*2017年1月PCI标准更新，将于2018年全面实施PCI新标准*

*2017年1-6月实施旧标准，2017年7月以后实施新标准*

**物理安全变更内容**

|  |  |
| --- | --- |
| 2人员 | |
| **2.1.3.2工作和敏感任务分配** | **明确要求**-卡商负责确定分配给临时工（包括顾问和承包商）的工作职责等级，除非员工的工作职能受限制。 |
| **2.1.3.4 访问卡运用** | **详细说明**-**安全经理必须每周检查**ID卡访问控制系统的审计日志。注：2.1.3.3-2.1.3.5章节移到3.4.2 |
| **2.1.4.1 员工职能变化** | **声明**-安全经理是在一个工作日内修改限制区域的访问控制，而不是及时地。 |
| **2.2.3 保安：文件记录** | **澄清**-内部程序手册关于保安的报警响应包括执法通知，如有对厂区未授权的访问。这些程序必须经过审查，验证，如有必要，进行年度更新。 |
| **2.3.3 来访者识别** | * 卡商必须设定来访者卡片（贵宾卡）可以追踪所有来访者的行动。该程序只在允许来访者授权的区域激活。 * 来访者必须将来访卡放在卡阅读器上来进入相应的区域。   也就是事先对预约的贵宾卡进行门禁设定，只允许进入预约的区域（刷卡）。   * 任何可行的区域都必须有卡访问追踪。任何无卡访问都必须记录在日志。日志可以是电子档或者手写。 |
| 3厂区 | |
| 3.3.2.1内部结构-安全控制室：规定 | **澄清**–CCTV和访问控制服务器必须在安全控制室或者在与之相当的安全空间，并且不可在高安全区内。 |
| 3.3.3.1 高安全区：规定 | **详细说明**–云基础系统必须在高安全区机房或者在HSA有符合标准条件的房间。  **澄清**-**HSA和所有在HSA的隔离室必须受内部移动探测的保护，即便室内无生产发生。** |
| 3.3.4.4 安全控制 | **澄清**–**在高安全区使用防弹玻璃（如UL752）保护不可打开的窗户，而不是用不可打破的玻璃或铁栏。** |
| 3.3.5.3 卡生产和组件销毁室 | **允许**在装卸区进行第三方销毁，可使用轻便/移动的设备。所有销毁室的要求必须与此临时使用相符。（MOBILE PROVISIONING） |
| 3.3.5.4 PIN信封生产室 | 说明：   * 个体应表现除了PIN打印外的非个人化活动，除了提供访问给持卡人数据，例如数据管理，包装或者邮寄活动。 * 涉及个人化的人员必须从不参与关联卡的PIN打印。程序文件里阐明这些人员不涉及相关联的卡的生产。 |
| 3.3.5.5机房&密钥管理房 | 云基础网络物理隔离  建立云基础配置网络的系统和应用，必须与其他卡商的网络和互联网连接网络物理隔绝。包括服务器，防火墙和加密机。例如，传统卡商环境里，可以是机房里的隔离架，或者在一个只做配置的实体里，一个隔离间或者数据中心一个房间。不同目的不可与其他服务器相同框架。 |
| 3.3.5.6 金库 | **明确要求**-   * **金库必须有足够数量的入侵探测器设备，可指示早期攻击。例如，地震，震动，电话线，话筒等，没有进入企图，并提供墙，天花板和楼梯的全覆盖。** * **金库必须用钢化加固的门，双锁机制（机械的或者逻辑的，例如机械组合和生物识别技术）要求物理和同时双重访问控制。** * **未封盒子仅可在库存里每天多次开启，且须在金库的中央区域。数卡流程必须在开启环节中。每班次最后盘库未封盒子须双人操作。其他盒子必须封住。** |
| 3.3.6.2运送和交付区域 | **修订此要求以提供更多灵活性**   * 运送区域的其中一个房间必须有个措施解决受控文件的转移不通过与外部人员的联系，也不能与之交流和看见他们。例如，一个安全窗户，可视对讲，监控等。 * **里面的运送/交付区域的门必须安装门禁控制来限制授权的用户访问，并记录使用记录。记录至少包括每次门的开和关。** |
| 3.4.2厂牌管理 | 新章节–移至2.1.3相关要求  3.4.2.1 识别卡  3.4.2.2 ID卡或访问卡使用  3.4.2.3 ID卡或访问卡清单和管理  **详细说明**：**安全经理必须每周检查门禁系统日志** |
| 3.4.3.2内部安全：系统管理 | **增加条款**–   * 访问控制系统管理必须在安全控制室内进行。 * **对于不能取消的一般管理员账户，密码只可以在紧急情况使用。必须更换初始密码，由双人控制。** |
| **3.6 退役计划** | **新要求：说明处理生产活动的终止的资产设备**   1. **卡商必须记录与卡片生产和provisioning活动相关的资产的方针和程序，证明如果生产活动终止，这些资产是安全的。** 2. **程序必须识别所有数据存储、卡片设计材料、卡片、卡片部件、物理钥匙、密钥，和用于生产活动的硬件，它们必须是安全的。** 3. **必须定义每个被识别物体的预期处置，例如，物体可能返回原主，传给授权用户，或销毁。** |
| 4生产程序和审计追踪 | |
| 4.7.3 个人化审计控制 | **每个个人化批次，包括**  **澄清**– 额外的指引  **由谁登出：负责验证总数的个人（而不是操作员）的名字和签名** |
| 5包装和交付要求 | |
| 5包装和交付要求 | **修订快递员的发货条款** |
| 5.4.3 安全运输 | **修订标准-装甲的和非装甲的车辆** |
| 6 PIN打印和未个人化预付款卡的包装 | |
| 6 | 修订-PIN打印的员工不可参与卡片个人化流程或者与PIN流程有关的卡包装 |
| 附件A | |
| 要求的适用性 | 新附件定义要求适用于：；   * 物理卡片 * SE基础供应 * HCE供应 |
| 附件B | |
| 逻辑安全要求 | 新附件定义CCTV逻辑管理和访问控制系统的要求（**用户管理-名单**） |

逻辑安全变更内容

|  |  |
| --- | --- |
| 2 角色和职责 | |
| 2.2 安全责任的任务 | **增加条款-CISO必须识别，IT安全经理负责监督卡商的安全环境** |
| 3安全手册和程序 | |
| 3.1 信息安全手册 | **澄清**-必须维护员工查阅和接受ISP的证据 |
| 3.3 事件响应计划和法务 | **澄清**-卡商对于任何分类数据的已知或存在疑问的方案的事故响应计划，必须与相关方沟通。 |
| 4数据安全 | |
| 4.1.2 机密数据 | 增加机密信息的例子：移动站点国际用户目录号码（用于识别手机号码） |
| 4.1.4 说明：保护 | **增加条款-**   * **必须存在安全要求里定义分类范围相当的保护控制。** * **所有支付数据必须要求有一个可视为相同的持有者负责分类和确保实施和动作保护控制。** |
| 4.3 **持卡人数据访问** | **澄清**-关于PAN的屏蔽，在被展示和打印时，发卡行的商业要求必须存在，且PAN必须全程加密，只允许在过程中需要的最小时间里解密  **详细说明**-   * **只有授权的数据库管理员有权限直接访问持卡人或云基础供应数据库。其他用户访问和用户咨询必须经过程序化的路径。** * **限制授权的数据库管理员进行数据库的直接访问。必须有数据库管理员访问的系统日志且每周审查。** * 用于云基础流程的应用（程序）ID只在预期目的时使用，不用于个人用户访问。 |
| 4.4 持卡人数据的交换 | **详细说明**-**数据传输给外源，或从外源接收，或在云基规则网络里转移必须加密，并依照此文件里的加密要求进行解密。** |
| 4.6 媒介处理 | **澄清**-**个人持有可移动媒介，不可对任何包含在媒介里的敏感或机密数据进行解密。** |
| 4.9 移动供应活动日志 | 新规定要求一个电子日志，含卡片成功或不成功供应信息。 |
| **4.10 退役计划** | **新规定：说明处理生产活动的终止的资产设备。**   1. **卡商必须记录与卡片生产和provisioning活动相关的资产的方针和程序，证明如果生产活动终止，这些资产是安全的。** 2. **程序必须识别所有数据存储、卡片设计材料、卡片、卡片部件、物理钥匙、密钥，和用于生产活动的硬件，它们必须是安全的。** 3. **必须定义每个被识别物体的预期处置，例如，物体可能返回原主，传给授权用户，或销毁。** |
| 5 网络安全 | |
| 5.1.3 传统卡商网络：卡生产DMZ | **详细说明**–**所有出入个人化网络的连接必须通过一个在DMZ区的系统，因此DMZ必须专用于卡生产/供应活动。** |
| 5.1.6 移动供应网络 | 主机卡仿真供应必须在它独立的网络上，安全元件层供应可以与其他个人化活动共存。 |
| 5.2 通用要求 | **澄清**-云基础供应网络必须与其他卡商和互联网连接网络物理和逻辑分离，并且不可与其他用于不同目的的服务器在一个框架里。 |
| 5.4.1 防火墙：通用 | **详细说明**-防火墙必须在外网和DMZ区之间，在DMZ和云基础供应网络之间部署。  修订-在每次防火墙配置修改以后，允许每月或每季度审查防火墙规则设置。 |
| 5.4.2 配置 | **澄清-授权的服务必须有一个文件化的业务理由，并且经过安全经理的批准。**  **详细说明**-卡**商必须维护基线安全配置标准的文件，对系统组件处理最小基线配置：**   * **用户和群组访问安全** * **文件和目录安全** * **限制的服务** * **系统更新和装载标准** * **安装安全软件**   **详细说明**-**卡商必须每月在云基础供应环境里检查基线安全配置。**  **罗列行业公认的系统加固标准。不限于：**   * **互联网安全中心** * **ISO** * **SANS协会** * **NIST**   **修订-在每次配置修改以后，允许每月或每季度审查配置。** |
| 5.5 防病毒软件或程序 | **详细说明**-卡商必须定义，文件化和依照程序说明：   * **安全警报识别-例如订阅安全警报，如微软和计算机应急响应小组（CERT）** * **系统组件更新识别，会影响操作系统，软件驱动程序和固件组件的可支持性和稳定性。** * **现有系统的清单包括安装软件组件的信息和服务运行。** |
| 5.6 远程访问 | **澄清**-此章节适用卡商的远程管理，不是发卡人相关。 |
| 5.6.2 远程访问（VPN） | **增加条款-**   * **关于远程访问，VPN必须从原始设备开始（例如，PC或专门为安全远程访问设计的现成设备）和终止于目标设备或个人化防火墙。如果终止点是防火墙，它对目标设备必须至少用一个与PCI数据安全要求4.1一致的TLS连接。** * **对于DMZ区的远程访问，VPN必须在目标设备终止。** * **SSL和TLS1.0明确地禁止上述的连接**。 |
| 5.8.3 安全测试和监控：入侵检测系统 | **详细说明**-有明文PIN的网络不可配置允许获取清晰的PIN值 |
| 6系统安全 | |
| 6.2 变更管理 | **澄清**-变更控制程序处理，至少：   * **确保变更需求由授权的用户提交** * **会变更的组件识别** * **影响的文件和撤销程序** * **当有要求时，成功测试的证据** * **所有变更请求的审核追踪的维护** * **记录变更是否成功** |
| 6.4 审核日志 | **详细说明**-所有在卡商环境的网络和网络设备必须存在审计日志；系统和连接云基础供应网络的应用必须存在审计日志。包括操作系统日志、安全软件日志或产品日志和包括安全事件的应用日志。  **详细说明**-**有文件化的流程用于审计日志检查依据**；**用于报告非正常活动**。日志检查可以是自动或手动的，必须包括鉴别、授权、和目录服务器。至少日志检查频率必须遵循以下：   * 实时反映威胁（指定作为高风险相关事件的警报） * IDS和IPS系统的**日常检查** * 无线访问点和鉴别服务器的**周检查** * 路由器**月度检查** * 数据库、应用、和操作系统的用户账户审计日志**月度检查**   **详细说明**-**卡商必须实施一个安全事件和事件日志机构。** |
| 6.5 移动供应网络的备份和恢复 |  |
| 6.6.3配置和补丁管理：开发 | **详细说明-卡商必须**   * **保证开发环境和生产环境员工的职责分离** * **保证软件源代码仅限于授权员工。员工访问源代码必须遵循文件化的流程。授权和批准必须记录下来。** |
| 6.7发卡行接口使用网页服务 |  |
| 7用户管理和系统访问控制 | |
| 7.1用户管理 | **详细说明**-**卡商必须**   * **保证有文件化的流程用于安全人员负责准许访问卡商网络、应用，和信息** * **在访问准许前，对有业务需求的员工限制批准和访问级别。至少，在账户激活时保留审批记录。** * **保证访问控制执行职责分离** * **对基于云供应，限制发卡行访问和给予仅发卡行自己的持卡数据** * **严格限制特权的或管理的访问，保证此访问经过用户的经理和安全经理审批。** * **建立特权访问的管理监督以确保符合职责分离** * **保证所有特权的管理访问被日志记录和每周检查一次。** |
| 7.2.2密码控制：特征和使用 | **增加密码最少长度为8位。**  **详细说明-密码在传输时必须是加密的，在存储时必须不可读取。**  **详细说明-身份验证凭据的符号化过程足以安全地防非授权的泄露和使用** |
| 7.3会话锁定 | **澄清-如果系统不允许会话锁定，用户必须在没有活动的时间里退出登录。** |
| 8密钥管理：机密数据 | |
| 8.1通用原则 | **澄清**-明文密钥部件输入PC时，PC必须是专用的和加固的。  详细说明-用于连接基于云供应的产品或服务的数字证书必须由CA或直接在发卡行或应用供应商PKI发放。 |
| 8.2对称密钥 | **详细说明-**每个具体持有人的密钥部件必须存储在分开的安全的箱子里，只有持有人和/或备份人员可以访问此箱子。 |
| 8.3非对称密钥 | **澄清**-没有一个人可以访问或使用所有一处私有加密密钥的部件或公用部分。 |
| 8.4.2密钥管理安全管理员：密钥经理 | **澄清**-密钥经理必须是卡商的雇员。 |
| 8.4.4密钥管理设备PINS | **澄清**-所有与密钥管理活动相关的设备，如铜钥匙和智能卡，禁止任何在单控下可以使用令牌操作密钥管理活动的单个人掌控。这些令牌必须与密钥部件相似的安全保管，包括在出入安全存储时使用门禁控制日志。 |
| 8.5密钥生成 | 明确– 密钥部件，如果打印出来，必须以此方式创建：密钥部件不可以被除授权密钥持有人之外的人看到此过程 |
| 8.5密钥生成 | 定义–当授权密钥持有人还未使用时，密钥部件或等份必须放置在预序号、防篡改的信封里 |
| 8.7密钥加载 | **新增要求-**  自2018年1月起，所有新部署的密钥加载设备的物理安全必须是SCDs，或者PCI批准的 或FIPS140-2 3级 或更高认证的 |
| 8.9密钥使用 | 重新定义要求：   * 私钥必须只用于创建数字签名或执行解密操作。私钥必须从不用来加密其它密钥。 * RSA签名（私）密钥必须禁止用来加密数据或其它密钥，类似地RSA加密（公）密钥必须禁止用来生成签名。 * 公钥必须只用来核对数字签名或执行加密操作。 * 密钥加密密钥必须从不用来作为工作密钥（密钥段），相反也是如此。   定义– 发卡行密钥禁止使用比发卡行规定到期日期更长的时间。  说明– 在卡商管理下的密钥清单必须得到维护以决定是否不再使用。  定义– 所有导出的密钥必须是发卡行唯一的密钥。 |
| 8.9密钥使用 | **明确要求**–用于移动供应的传输密钥必须是每台设备唯一的。 |
| 8.11密钥销毁 | 明确– 退役程序为安全密钥方法  明确 -销毁要求适用于密钥部件而不是密钥。 |
| 8.11密钥销毁 | 定义– 所有密钥销毁必须记录下来，保留日志以备检查。 |
| 8.13密钥泄露 | 明确– 除有其它说明，要求适用于卡商自己的密钥。  明确– 卡商必须删除操作性使用所有泄露的密钥在提前定义时间范围内，并提供一个方法迁移新密钥，若密钥是发卡行持有的，必须立即通知发卡行作进行一步说明。 |