PCI DSS v4.0 变更系列之四

——第一大类要求点

要求点变更的说明之第一大类：建立和维护安全网络和系统

要求 1：安装并实施网络安全控制

该章节的主要变化，是将原来防火墙（firewall）的术语，变更为网络安全控制（network security control），以适用于各种访问控制机制。这些安全控制可以是虚拟设备、云访问控制、虚拟化或容器系统以及 SDN 技术等。

另外一个明确的变化，是需要按要求 6 的变更控制要求进行网络安全控制机制的变更。

v4.0 要求点的英文原文	对应的 v3.2.1 要求点	与 v3.2.1 的变化/新要求说明
1.1 确定和理解安装和维护网络安全控制的流程和机制。		
1.1.1 All security policies and operational procedures that are identified in Requirement 1 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	1.4	在原 1.4 要求的基础上，增加了策略和流程需要保持更新的要求。
1.1.2 Roles and responsibilities for performing activities in Requirement 1 are documented, assigned, and understood.	1.1.5	删除了对组（group）职责的维护要求。
1.2 配置和维护网络安全控制（NSC）。		
1.2.1 Configuration standards for NSC rulesets are: • Defined. • Implemented. • Maintained.	1.1	将原来 1.1 的配置维护要求，调整为定义、实施并维护针对网络安全控制规则的配置标准。
1.2.2 All changes to network connections and to configurations of NSCs are approved and managed in accordance with the change control process defined at Requirement 6.5.1.	1.1.1	重申对于网络连接及安全控制设备的变更应基于要求 6.5.1 进行审批和管理。
1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.	1.1.2	与原来要求拓扑图维护的要求保持不变。

1.2.4 An accurate data-flow diagram(s) is maintained that meets the following: • Shows all account data flows across systems and networks. • Updated as needed upon changes to the environment.	1.1.3	与原来要求的对数据流向图维护的要求保持不变。
1.2.5 All services, protocols, and ports allowed are identified, approved, and have a defined business need.	1.1.6	该要求将原来 1.1.6 拆分为此要求及 1.2.6。此要求是服务、协议及端口的识别、审批及必要性。
1.2.6 Security features are defined and implemented for all services, protocols, and ports that are in use and considered to be insecure, such that the risk is mitigated.	1.1.6	该要求将原来 1.1.6 拆分为此要求及 1.2.5。此要求是对所开启的服务、协议及端口进行安全性加固和风险降低。
1.2.7 Configurations of NSCs are reviewed at least once every six months to confirm they are relevant and effective.	1.1.7	此要求与原 1.1.7 的要求基本保持一致。概念上由原来对 router 的要求，调整为安全控制设备的要求。
1.2.8 Configuration files for NSCs are: • Secured from unauthorized access. • Kept consistent with active network configurations.	1.2.2	此要求与原 1.2.2 要求保持一致。概念上由原来对 router 的要求，调整为安全控制设备的要求。进一步明确了防止非授权访问及与当前配置保持一致性的要求。
1.3 限制持卡人数据环境的网络访问权限。		
1.3.1 Inbound traffic to the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	1.2.1 1.3.4	把原 1.3.4 与 1.2.1 重叠的要求做了整合，同时把原 1.2.1 中关于入站和出站的访问控制要求做了分解，拆分为新的 1.3.1 入站要求和 1.3.2 出站要求。
1.3.2 Outbound traffic from the CDE is restricted as follows: • To only traffic that is necessary. • All other traffic is specifically denied.	1.2.1 1.3.4	把原 1.3.4 与 1.2.1 重叠的要求做了整合，同时把原 1.2.1 中关于入站和出站的访问控制要求做了分解，拆分为新的 1.3.1 入站要求和 1.3.2 出站要求。
1.3.3 NSCs are installed between all wireless networks and the CDE, regardless of whether the wireless network is a CDE, such that: • All wireless traffic from wireless networks into the CDE is denied by default. • Only wireless traffic with an authorized business purpose is allowed into the CDE.	1.2.3	在原 1.2.3 要求的基础上强调是无线网络与持卡人数据环境间必须进行授权控制。 把原来防火墙的说法变为网络安全控制（NSC），使得在控制机制的选择上更具灵活性。
1.4 控制可信网络和不可信网络之间的网络连接。		

1.4.1 NSCs are implemented between trusted and untrusted networks.	1.3	在原 1.3 要求在互联网和持卡人数据环境组件间禁止直接访问的基础上，概括为在信任网络和不可信网络间部署网络安全控制（NSC），要求呈现更清晰，实现的控制机制的选择也更灵活。
1.4.2 Inbound traffic from untrusted networks to trusted networks is restricted to: • Communications with system components that are authorized to provide publicly accessible services, protocols, and ports. • Stateful responses to communications initiated by system components in a trusted network. • All other traffic is denied.	1.3.1 1.3.2 1.3.5	此要求把原来 1.3.1、1.3.2 和 1.3.5 的要求进行了融合，把入站请求要求的仅访问授权的公开服务、对内访问的状态控制、任何其它流量均禁止整合在这一个要求，控制的思路要求更清晰。
1.4.3 Anti-spoofing measures are implemented to detect and block forged source IP addresses from entering the trusted network.	1.3.3	与原 1.3.3 的要求保持不变。
1.4.4 System components that store cardholder data are not directly accessible from untrusted networks.	1.3.6	相较于原 1.3.6 的要求，新要求重点在于存储持卡人数据的组件不可被非信任网络所直接访问，控制的思路要求更清晰。
1.4.5 The disclosure of internal IP addresses and routing information is limited to only authorized parties.	1.3.7	文字做了调整，目标与原要求一致。
1.5 减轻能够连接到不可信网络和 CDE 的计算设备对 CDE 产生的风险。		
1.5.1 Security controls are implemented on any computing devices, including company- and employee-owned devices, that connect to both untrusted networks (including the Internet) and the CDE as follows: • Specific configuration settings are defined to prevent threats being introduced into the entity's network. • Security controls are actively running. • Security controls are not alterable by users of the computing devices unless specifically documented and authorized by management on a case-by-case basis for a limited period.	1.4	整体思路与原 1.4 的要求不变，新的要求主要用安全控制（security controls）替换了原来的个人防火墙（personal firewall），使得控制机制的选择上更灵活。 另外，新要求也强调了适用于同时访问到非信任访问和持卡人数据环境的设备。

要求 2：安全配置应用于所有系统组件

该章节的除了文档中关于角色和职责的要求外，这一部分主要加强了系统组件配置标准的要求。

值得注意的变化是要求 2.2.3，新版本中进行了详细的阐述，以满足所开启的功能处于不同安全级别时的安全保护需要。

v4.0 要求点的英文原文	对应的 v3.2.1 要求点	与 v3.2.1 的变化/新要求说明
2.1 Processes and mechanisms for applying secure configurations to all system components are defined and understood.		
2.1.1 All security policies and operational procedures that are identified in Requirement 2 are: • Documented. • Kept up to date. • In use. • Known to all affected parties.	2.5	在原 2.5 要求的基础上，增加了策略和流程需要保持更新的要求。
2.1.2 Roles and responsibilities for performing activities in Requirement 2 are documented, assigned, and understood.	新要求	记录、分配及理解执行要求 2 的管理活动所对应的角色及职责。
2.2 System components are configured and managed securely.		
2.2.1 Configuration standards are developed, implemented, and maintained to: • Cover all system components. • Address all known security vulnerabilities. • Be consistent with industry-accepted system hardening standards or vendor hardening recommendations. • Be updated as new vulnerability issues are identified, as defined in Requirement 6.3.1. • Be applied when new systems are configured and verified as in place before or immediately after a system component is connected to a production environment.	新要求	这个要求是基于组件的配置标准提出的，综合了原 2.2，6.4.6 等要求，对组件的配置标准提出了更高的要求，比如在基于要求 6.3.1 识别到新漏洞时更新配置标准。
2.2.2 Vendor default accounts are managed as follows: • If the vendor default account(s) will be used, the default password is changed per	2.1	基于原 2.1 要求的改进，进一步澄清了对于默认账号的管理要求，即要么禁用或删除默认账号，要么允许默认账号，

Requirement 8.3.6. • If the vendor default account(s) will not be used, the account is removed or disabled.		但密码必须修改为符合最小 12 位及复杂度要求。 新的修改使要求更合理。
2.2.3 Primary functions requiring different security levels are managed as follows: • Only one primary function exists on a system component, **OR** • Primary functions with differing security levels that exist on the same system component are isolated from each other, **OR** • Primary functions with differing security levels on the same system component are all secured to the level required by the function with the highest security need.	2.2.1	对原 2.2.1 的要求做了进一步的澄清，给出了对于系统组件完成不同主要功能的实施方案，使得这个要求更具有可执行性。
2.2.4 Only necessary services, protocols, daemons, and functions are enabled, and all unnecessary functionality is removed or disabled.	2.2.2 2.2.5	对原来 2.2.2 禁用不需要功能和原来 2.2.4 仅启用必要的服务、协议、端口及功能的要求进行了整合。
2.2.5 If any insecure services, protocols, or daemons are present: • Business justification is documented. • Additional security features are documented and implemented that reduce the risk of using insecure services, protocols, or daemons.	2.2.3	对原来 2.2.3 的要求进一步进行了澄清，限定于在启用不安全服务、协议或守护进程的情况。 同时，也将原来的 1.1.6 中关于对业务必要性论证进行记录的要求进行了融合。
2.2.6 System security parameters are configured to prevent misuse.	2.2.4	对原 2.2.4 的要求重新进行了描述。
2.2.7 All non-console administrative access is encrypted using strong cryptography.	2.3	对原 2.3 的要求重新进行了描述。
2.3 Wireless environments are configured and managed securely.		
2.3.1 For wireless environments connected to the CDE or transmitting account data, all wireless vendor defaults are changed at installation or are confirmed to be secure, including but not limited to: • Default wireless encryption keys. • Passwords on wireless access points. • SNMP defaults.	2.1.1	把原 2.1.1 无线环境管理中除了无线密钥管理部分的要求，形成了这个要求，同时也增加了更改其它安全相关的默认厂商参数的要求。

• Any other security-related wireless vendor defaults.		
2.3.2 For wireless environments connected to the CDE or transmitting account data, wireless encryption keys are changed as follows: • Whenever personnel with knowledge of the key leave the company or the role for which the knowledge was necessary. • Whenever a key is suspected of or known to be compromised.	2.1.1	把原来 2.1.1 中关于无线密钥管理的要求进行了扩展，形成了本要求，要求在知晓密钥的人员离职、角色替换以及怀疑密钥被泄露时进行无线环境密钥的替换。