# PCI DSS v4.0 变更系列之七

## ——第四大类要求点

# 要求点变更的说明之第四大类：实施强有力的访问控制措施

## 要求 7：根据“必须知道”原则限制系统组件和持卡人数据的访问权限

要求 7.2.4 增加了对账号检查的要求。

要求 7.2.5.1 增加了对来自于应用和系统账号的访问的检查要求。

原 v3.2.1 的要求 8.7 整合到 v4.0 的要求 7.2.6。

| v4.0 要求点的英文原文 | 对应的<br>v3.2.1 要求 | 与 v3.2.1 的变化/新要求说明 |
|---|---|---|
| **7.1** Processes and mechanisms for restricting access to system components and cardholder data by business need to know are defined and understood. | | |
| **7.1.1** All security policies and operational procedures that are identified in Requirement 7 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | 7.3 | 在原 7.3 要求的基础上，增加了策略和流程需要保持更新的要求。 |
| **7.1.2** Roles and responsibilities for performing activities in Requirement 7 are documented, assigned, and understood. | 新要求 | 记录、分配及理解执行要求 7 的管理活动所对应的角色及职责。 |
| **7.2** Access to system components and data is appropriately defined and assigned. | | |
| **7.2.1** An access control model is defined and includes granting access as follows:<br>• Appropriate access depending on the entity’s business and access needs.<br>• Access to system components and data resources that is based on users’ job classification and functions.<br>• The least privileges required (for example, user, administrator) to perform a job function. | 7.1<br>7.1.1 | 将原来的 7.1 和 7.1.1 的要求进行了整合，形成该要求。 |
| **7.2.2** Access is assigned to users, including privileged users, based on:<br>• Job classification and function. | 7.1<br>7.1.2 | 将原来的 7.1，7.1.2 和 7.1.3 的要求进行了整合，形成该要求。 |

| | | |
|---|---|---|
| • Least privileges necessary to perform job responsibilities. | 7.1.3 | |
| **7.2.3** Required privileges are approved by authorized personnel. | 7.1.4 | 对原 7.1.4 的要求进行了描述。 |
| **7.2.4** All user accounts and related access privileges, including third-party/vendor accounts, are reviewed as follows:<br>• At least once every six months.<br>• To ensure user accounts and access remain appropriate based on job function.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate. | 新要求 | 添加了对用户账号及其权限每半年进行检查的要求。 |
| **7.2.5** All application and system accounts and related access privileges are assigned and managed as follows:<br>• Based on the least privileges necessary for the operability of the system or application.<br>• Access is limited to the systems, applications, or processes that specifically require their use. | 新要求 | 应用、系统账号及访问特权基于最小化原则进行授权，并限制到需要的系统、应用及进程。 |
| **7.2.5.1** All access by application and system accounts and related access privileges are reviewed as follows:<br>• Periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1).<br>• The application/system access remains appropriate for the function being performed.<br>• Any inappropriate access is addressed.<br>• Management acknowledges that access remains appropriate. | 新要求 | 添加了对应用系统账号及访问特权进行检查、评估的要求。检查的频率要求通过风险评估过程制定，评估其适宜性，并由管理层知晓。 |
| **7.2.6** All user access to query repositories of stored cardholder data is restricted as follows:<br>• Via applications or other programmatic methods, with access and allowed actions based on user roles and least privileges.<br>• Only the responsible administrator(s) can directly access or query repositories of stored CHD. | 8.7 | 对原 8.7 的要求进行了描述。 |

| | | |
|---|---|---|
| **7.3** Access to system components and data is managed via an access control system(s). | | |
| **7.3.1** An access control system(s) is in place that restricts access based on a user’s need to know and covers all system components. | 7.2.1 | 对原 7.2.1 的要求进行了描述。 |
| **7.3.2** The access control system(s) is configured to enforce permissions assigned to individuals, applications, and systems based on job classification and function. | 7.2.2 | 对原 7.2.2 的要求进行了描述。 |
| **7.3.3** The access control system(s) is set to “deny all” by default. | 7.2.3 | 对原 7.2.3 的要求进行了描述。 |

## 1.1 要求 8：识别用户并验证系统组件的访问权限

要求 8 的介绍章节强调了适用性，对应的要求适用于所有的系统组件账号，包括但不限于 POS 账号、管理账号、系统及应用账号、用于查看/访问持卡人数据及其系统的账号等。

主要变化的要求点如下：

要求 8.2.2 进一步明确了组、共享和通用账号的使用要求，限定于严格要求下的例外场景。

要求 8.3.9 和 8.3.10.1 使用密码登陆的情形，对密码变更有 90 天的频率要求，增加了可基于安全态势进行分析的选项，更具灵活性。

要求 8.6.1-8.6.3 对系统/系统账号用于交互式登陆的情形，提出了明确的要求。

| v4.0 要求点的英文原文 | 对应的 v3.2.1 要求 | 与 v3.2.1 的变化/新要求说明 |
|---|---|---|
| **8.1** Processes and mechanisms for identifying users and authenticating access to system components are defined and understood. | | |
| **8.1.1** All security policies and operational procedures that are identified in Requirement 8 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | 8.8 | 在原 8.8 要求的基础上，增加了策略和流程需要保持更新的要求。 |
| **8.1.2** Roles and responsibilities for performing activities in Requirement 8 are documented, assigned, and understood. | 新要求 | 记录、分配及理解执行要求 8 的管理活动所对应的角色及职责。 |
| **8.2** User identification and related accounts for users and administrators are strictly managed throughout an account’s lifecycle. | | |

| | | |
|---|---|---|
| **8.2.1** All users are assigned a unique ID before access to system components or cardholder data is allowed. | 8.1.1 | 在原要求 8.1.1 的基础上，进一步澄清这个要求并不针对一次只能访问到一个卡号的 POS 终端。 |
| **8.2.2** Group, shared, or generic accounts, or other shared authentication credentials are only used when necessary on an exception basis, and are managed as follows:<br>• Account use is prevented unless needed for an exceptional circumstance.<br>• Use is limited to the time needed for the exceptional circumstance.<br>• Business justification for use is documented.<br>• Use is explicitly approved by management.<br>• Individual user identity is confirmed before access to an account is granted.<br>• Every action taken is attributable to an individual user. | 8.5 | 在原要求 8.5 的基础上，添加了使用组、共享和通用账号的例外场景，并对该场景进行了具体的要求。 |
| **8.2.3** ***Additional requirement for service providers only:*** Service providers with remote access to customer premises use unique authentication factors for each customer premises. | 8.5.1<br>8.5 | 在原要求 8.5 和 8.5.1 的基础上，将这一要求独立于原 8.5 的要求。 |
| **8.2.4** Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows:<br>• Authorized with the appropriate approval.<br>• Implemented with only the privileges specified on the documented approval. | 8.1.2 | 在原要求 8.1.2 的基础上，添加了具体的权限管理要求。 |
| **8.2.5** Access for terminated users is immediately revoked. | 8.1.3 | 在原要求 8.1.3 的基础上，更新了描述。 |
| **8.2.6** Inactive user accounts are removed or disabled within 90 days of inactivity. | 8.1.4 | 在原要求 8.1.4 的基础上，更新了描述。 |
| **8.2.7** Accounts used by third parties to access, support, or maintain system components via remote access are managed as follows:<br>• Enabled only during the time period needed and disabled when not in use.<br>• Use is monitored for unexpected activity. | 8.1.5 | 在原要求 8.1.5 的基础上，侧重于来自第三方访问中异常行为的监控。 |

| | | |
|---|---|---|
| **8.2.8** If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session. | 8.1.8 | 在原要求 8.1.4 的基础上，更新了描述。 |
| **8.3** Strong authentication for users and administrators is established and managed. | | |
| **8.3.1** All user access to system components for users and administrators is authenticated via at least one of the following authentication factors:<br>• Something you know, such as a password or passphrase.<br>• Something you have, such as a token device or smart card.<br>• Something you are, such as a biometric element. | 8.2 | 在原要求 8.2 的基础上，更新了描述。 |
| **8.3.2** Strong cryptography is used to render all authentication factors unreadable during transmission and storage on all system components. | 8.2.1 | 在原要求 8.2.1 的基础上，把传输与存储强加密的适用对象由密码调整为认证因素，此要求变得更严格。 |
| **8.3.3** User identity is verified before modifying any authentication factor. | 8.2.2 | 在原要求 8.2.2 的基础上，更新了描述。 |
| **8.3.4** Invalid authentication attempts are limited by:<br>• Locking out the user ID after not more than 10 attempts.<br>• Setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. | 8.1.6<br>8.1.7 | 合并了原 8.1.6 和 8.1.7 的要求，无效尝试锁定的次数，由原来的 6 次以内，变为 10 次以内。 |
| **8.3.5** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they are set and reset for each user as follows:<br>• Set to a unique value for first-time use and upon reset.<br>• Forced to be changed immediately after the first use. | 8.2.6 | 在原 8.2.6 要求的基础上，更清晰的指出此要求针对将密码/口令在满足 8.3.1 要求时适用于该要求。 |
| **8.3.6** If passwords/passphrases are used as authentication factors to meet Requirement 8.3.1, they meet the following minimum level of complexity: | 8.2.3 | 在原 8.2.3 的基础上，将密码/口令的长度要求，由最低 7 位，调整为最低 12 |

| | | |
|---|---|---|
| • A minimum length of 12 characters (or IF the system does not support 12 characters, a minimum length of eight characters).<br>• Contain both numeric and alphabetic characters. | | 位（在不支持 12 位时，可接受至少 8 位）。 |
| **8.3.7** Individuals are not allowed to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. | 8.2.5 | 在原要求 8.2.5 的基础上，更新了描述。 |
| **8.3.8** Authentication policies and procedures are documented and communicated to all users including:<br>• Guidance on selecting strong authentication factors.<br>• Guidance for how users should protect their authentication factors.<br>• Instructions not to reuse previously used passwords/passphrases.<br>• Instructions to change passwords/passphrases if there is any suspicion or knowledge that the password/passphrases have been compromised and how to report the incident. | 8.4 | 在原要求 8.4 的基础上，更新了描述。 |
| **8.3.9** If passwords/passphrases are used as the only authentication factor for user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | 8.2.4 | 在原 8.2.4 的基础上，更清晰的指出此要求针对将密码/口令在满足 8.3.1 要求时适用于该要求。同时，指出了一个对账号进行动态分析的实现机制的选项。 |
| **8.3.10** ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access to cardholder data (i.e., in any single- factor authentication implementation), then guidance is provided to customer users including:<br>• Guidance for customers to change their user | 8.2.4.b | 将原 8.2.4.b 中关于服务供应商的额外要求，独立为单独的要求点。 |

| | | |
|---|---|---|
| passwords/passphrases periodically.<br>• Guidance as to when, and under what circumstances, passwords/passphrases are to be changed. | | |
| **8.3.10.1** ***Additional requirement for service providers only:*** If passwords/passphrases are used as the only authentication factor for customer user access (i.e., in any single-factor authentication implementation) then either:<br>• Passwords/passphrases are changed at least once every 90 days,<br>**OR**<br>• The security posture of accounts is dynamically analyzed, and real-time access to resources is automatically determined accordingly. | 8.2.4.b | 在 2025 年 3 月 31 日后，该要求将变为强制，替代 8.3.10。 |
| **8.3.11** Where authentication factors such as physical or logical security tokens, smart cards, or certificates are used:<br>• Factors are assigned to an individual user and not shared among multiple users.<br>• Physical and/or logical controls ensure only the intended user can use that factor to gain access. | 8.6 | 在原要求 8.6 的基础上，更新了描述。 |
| **8.4** Multi-factor authentication (MFA) is implemented to secure access into the CDE. | | |
| **8.4.1** MFA is implemented for all non-console access into the CDE for personnel with administrative access. | 8.3.1 | 在原要求 8.3.1 的基础上，更新了描述。 |
| **8.4.2** MFA is implemented for all access into the CDE. | 新要求 | 在 2025 年 3 月 31 日强制所有到 CDE 的访问均实施多因素认证。 |
| **8.4.3** MFA is implemented for all remote network access originating from outside the entity’s network that could access or impact the CDE as follows:<br>• All remote access by all personnel, both users and administrators, originating from outside the entity’s network.<br>• All remote access by third parties and vendors. | 8.3.2 | 在原要求 8.3.2 的基础上，更新了描述。 |
| **8.5** Multi-factor authentication (MFA) systems are configured to prevent misuse. | | |

|  |  |  |
|---|---|---|
| **8.5.1** MFA systems are implemented as follows:<br>• The MFA system is not susceptible to replay attacks.<br>• MFA systems cannot be bypassed by any users, including administrative users unless specifically documented, and authorized by management on an exception basis, for a limited time period.<br>• At least two different types of authentication factors are used.<br>• Success of all authentication factors is required before access is granted. | 新要求 | 对MFA机制的安全保护的要求，将在2025年3月31日强制实施。 |
| **8.6** Use of application and system accounts and associated authentication factors is strictly managed. |  |  |
| **8.6.1** If accounts used by systems or applications can be used for interactive login, they are managed as follows:<br>• Interactive use is prevented unless needed for an exceptional circumstance.<br>• Interactive use is limited to the time needed for the exceptional circumstance.<br>• Business justification for interactive use is documented.<br>• Interactive use is explicitly approved by management.<br>• Individual user identity is confirmed before access to account is granted.<br>• Every action taken is attributable to an individual user. | 新要求 | 对于交互式登陆用户，提出了额外的管理要求。 |
| **8.6.2** Passwords/passphrases for any application and system accounts that can be used for interactive login are not hard coded in scripts, configuration/property files, or bespoke and custom source code. | 新要求 | 对于交互式登陆的密码/口令，禁止存在于任何脚本/配置/属性文件及代码中。 |
| **8.6.3** Passwords/passphrases for any application and system accounts are protected against misuse as follows:<br>• Passwords/passphrases are changed periodically (at the frequency defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1) and upon suspicion or confirmation of compromise. | 新要求 | 增加了对密码/口令防止误用的要求，包括基于风险评估的结果以及怀疑泄露时进行定期变更，基于变更的频率确定相适宜的密码/口令的复杂性。 |

| | | |
|---|---|---|
| • Passwords/passphrases are constructed with sufficient complexity appropriate for how frequently the entity changes the passwords/passphrases. | | |

## 1.2 要求 9：限制持卡人数据的实体访问权限

要求 9 与之前的 v3.2.1 版本的内容基本一致，较显著的变化如下：

要求 9.5.1.2.1，通过风险评估确定对 POI 设备的检查频率，更具灵活性。

| v4.0 要求点的英文原文 | 对应的 v3.2.1 要求 | 与 v3.2.1 的变化/新要求说明 |
|---|---|---|
| **9.1** Processes and mechanisms for restricting physical access to cardholder data are defined and understood. | | |
| **9.1.1** All security policies and operational procedures that are identified in Requirement 9 are:<br>• Documented.<br>• Kept up to date.<br>• In use.<br>• Known to all affected parties. | 9.10 | 在原 9.10 要求的基础上，增加了策略和流程需要保持更新的要求。 |
| **9.1.2** Roles and responsibilities for performing activities in Requirement 9 are documented, assigned, and understood. | 新要求 | 记录、分配及理解执行要求 9 的管理活动所对应的角色及职责。 |
| **9.2** Physical access controls manage entry into facilities and systems containing cardholder data. | | |
| **9.2.1** Appropriate facility entry controls are in place to restrict physical access to systems in the CDE. | 9.1 | 在原要求 9.1 的基础上，更新了描述。 |
| **9.2.1.1** Individual physical access to sensitive areas within the CDE is monitored with either video cameras or physical access control mechanisms (or both) as follows:<br>• Entry and exit points to/from sensitive areas within the CDE are monitored.<br>• Monitoring devices or mechanisms are protected from tampering or disabling.<br>• Collected data is reviewed and correlated with other entries. | 9.1.1 | 在原要求 9.1 的基础上，细化了具体的监控/物理访问控制的要求。 |

| | | |
|---|---|---|
| • Collected data is stored for at least three months, unless otherwise restricted by law. | | |
| **9.2.2** Physical and/or logical controls are implemented to restrict use of publicly accessible network jacks within the facility. | 9.1.2 | 在原要求 9.1.2 的基础上，更新了描述。 |
| **9.2.3** Physical access to wireless access points, gateways, networking/communications hardware, and telecommunication lines within the facility is restricted. | 9.1.3 | 在原要求 9.1.3 的基础上，更新了描述。 |
| **9.2.4** Access to consoles in sensitive areas is restricted via locking when not in use. | 9.1 | 把原要求 9.1 的检查点，调整为一个独立的要求。 |
| **9.3** Physical access for personnel and visitors is authorized and managed. | | |
| **9.3.1** Procedures are implemented for authorizing and managing physical access of personnel to the CDE, including:<br>• Identifying personnel.<br>• Managing changes to an individual's physical access requirements.<br>• Revoking or terminating personnel identification.<br>• Limiting access to the identification process or system to authorized personnel. | 9.2<br>9.3 | 把原要求 9.2 和 9.3 中关于现场人员(onsite personnel)的要求，整合在此要求。 |
| **9.3.1.1** Physical access to sensitive areas within the CDE for personnel is controlled as follows:<br>• Access is authorized and based on individual job function.<br>• Access is revoked immediately upon termination.<br>• All physical access mechanisms, such as keys, access cards, etc., are returned or disabled upon termination. | 9.3 | 把原要求 9.3 中关于 onsite personnel 的控制要求，形成此要求。 |
| **9.3.2** Procedures are implemented for authorizing and managing visitor access to the CDE, including:<br>• Visitors are authorized before entering.<br>• Visitors are escorted at all times.<br>• Visitors are clearly identified and given a badge or other identification that expires. | 9.4.1<br>9.4.2 | 把原要求 9.2 和 9.3 中关于访客的要求，整合在此要求。 |

| | | |
|---|---|---|
| • Visitor badges or other identification visibly distinguishes visitors from personnel. | | |
| **9.3.3** Visitor badges or identification are surrendered or deactivated before visitors leave the facility or at the date of expiration. | 9.4.3 | 在原要求 9.4.3 的基础上，更新了描述。 |
| **9.3.4** A visitor log is used to maintain a physical record of visitor activity within the facility and within sensitive areas, including:<br>• The visitor’s name and the organization represented.<br>• The date and time of the visit.<br>• The name of the personnel authorizing physical access.<br>• Retaining the log for at least three months, unless otherwise restricted by law. | 9.4.4 | 在原要求 9.4.4 的基础上，更新了描述。 |
| **9.4** Media with cardholder data is securely stored, accessed, distributed, and destroyed. | | |
| **9.4.1** All media with cardholder data is physically secured. | 9.5 | 在原要求 9.5 的基础上，更新了描述。 |
| **9.4.1.1** Offline media backups with cardholder data are stored in a secure location. | 9.5.1 | 在原要求 9.5.1 的基础上，拆分为存储要求和检查的要求。 |
| **9.4.1.2** The security of the offline media backup location(s) with cardholder data is reviewed at least once every 12 months. | 9.5.1 | 在原要求 9.5.1 的基础上，拆分为存储要求和检查的要求。 |
| **9.4.2** All media with cardholder data is classified in accordance with the sensitivity of the data. | 9.6.1 | 在原要求 9.5 的基础上，更新了描述。 |
| **9.4.3** Media with cardholder data sent outside the facility is secured as follows:<br>• Media sent outside the facility is logged.<br>• Media is sent by secured courier or other delivery method that can be accurately tracked.<br>• Offsite tracking logs include details about media location. | 9.6.2 | 在原要求 9.6.2 的基础上，更新了描述。 |

| | | |
|---|---|---|
| **9.4.4** Management approves all media with cardholder data that is moved outside the facility (including when media is distributed to individuals). | 9.6.3 | 在原要求 9.6.3 的基础上，更新了描述。 |
| **9.4.5** Inventory logs of all electronic media with cardholder data are maintained. | 9.7 | 在原要求 9.7 的基础上，更新了描述。 |
| **9.4.5.1** Inventories of electronic media with cardholder data are conducted at least once every 12 months. | 9.7.1 | 在原要求 9.7.1 的基础上，更新了描述。 |
| **9.4.6** Hard-copy materials with cardholder data are destroyed when no longer needed for business or legal reasons, as follows:<br>• Materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.<br>• Materials are stored in secure storage containers prior to destruction. | 9.8.1 | 在原要求 9.8.1 的基础上，更新了描述。 |
| **9.4.7** Electronic media with cardholder data is destroyed when no longer needed for business or legal reasons via one of the following:<br>• The electronic media is destroyed.<br>• The cardholder data is rendered unrecoverable<br>so that it cannot be reconstructed. | 9.8.2 | 在原要求 9.8.2 的基础上，更新了描述。 |
| **9.5** Point-of-interaction (POI) devices are protected from tampering and unauthorized substitution. | | |
| **9.5.1** POI devices that capture payment card data via direct physical interaction with the payment card form factor are protected from tampering and unauthorized substitution, including the following:<br>• Maintaining a list of POI devices.<br>• Periodically inspecting POI devices to look for<br>tampering or unauthorized substitution.<br>• Training personnel to be aware of suspicious behavior and to report tampering or unauthorized substitution of devices. | 9.9 | 在原要求 9.9 的基础上，更新了描述。强调了适用于直接接触卡片的 POI 设备。 |

| | | |
|---|---|---|
| **9.5.1.1** An up-to-date list of POI devices is maintained, including:<br>• Make and model of the device.<br>• Location of device.<br>• Device serial number or other methods of unique identification. | 9.9.1 | 在原要求 9.9.1 的基础上，更新了描述。 |
| **9.5.1.2** POI device surfaces are periodically inspected to detect tampering and unauthorized substitution. | 9.9.2 | 在原要求 9.9.2 的基础上，更新了描述。 |
| **9.5.1.2.1** The frequency of periodic POI device inspections and the type of inspections performed is defined in the entity’s targeted risk analysis, which is performed according to all elements specified in Requirement 12.3.1. | 新要求 | 要求通过风险评估过程确定 POI 检查的频率。 |
| **9.5.1.3** Training is provided for personnel in POI environments to be aware of attempted tampering or replacement of POI devices, and includes:<br>• Verifying the identity of any third-party persons claiming to be repair or maintenance personnel, before granting them access to modify or troubleshoot devices.<br>• Procedures to ensure devices are not installed, replaced, or returned without verification.<br>• Being aware of suspicious behavior around devices.<br>• Reporting suspicious behavior and indications of device tampering or substitution to appropriate personnel. | 9.9.3 | 在原要求 9.9.3 的基础上，更新了描述。 |