**How to Comply to Requirement 8 of PCI DSS**

**PCI DSS Requirement 8: Identify and authenticate access to system components.**

When a unique ID is assigned to every individual, it helps to trace those responsible for breach of data, if it ever happens. This also ensures that individuals refrain from committing any malicious act as they can be held accountable.

**8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components.**

It is essential to assign unique IDs to all users before enabling their access to the system. If the organization lacks the ability to uniquely identify every individual, it becomes impossible to hold any single individual responsible in case of any wrong action within the network. For compliance to this requirement, it is important that all administrative employees should be interviewed to ensure that every employee has been assigned a unique ID number. For verification of accounts that access a system, a strong process should be developed to manage any changes to the ID such as addition, modification or deletion of existing IDs.

If an employee is no longer working for the company and his/her user ID is still functional, there is a possibility of access to cardholder data from their side with a malicious intent. To address this issue, a sample of employees who left in the past six months should be taken and compared against the current account lists to ensure that those who have left the organization are no longer a part of the current list of functional IDs.

All user accounts should be examined to check for activity. If a user account has remained inactive for more than 90 days, it should be deleted as inactive users are more prone to being accessed by hackers because changes in these accounts go unnoticed for a long time.

Vendors should not be allowed to have access to your network at all times because it increases the chances of unofficial access either from an employee of the vendor or an outsider who discovers this full time available entry point. The access should thus only be available for specified time periods and disabled when the access is no longer required. Personnel should be interviewed to verify that accounts accessible by vendors are monitored to check that access is only done on systems where it is required and only during the approved timings.

A sample of system configuration settings should be checked to verify that user accounts be locked after six failed attempts to log on. Without such settings, an attacker can continue to attempt to log on by trying out password multiple times till he is successful. Re-activation should not be enabled at once and a minimum time period of 30 seconds should be set up after which account can be re-activated. When reactivation is requested, the admin must ensure that the actual user is making the request. The system configuration settings should also be checked for re-activation in case a system has been idle for more than 15 minutes as unattended systems can also invite people to misuse the confidential information in that system.

**8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users:**

* **Something you know, such as a password or passphrase**
* **Something you have, such as a token device or smart card**
* **Something you are, such as a biometric**

It is important to verify that users should be authenticated along with the provision of unique IDs. When cardholder data is being accessed, additional authentication must be applied. There should be a proper documentation that describes the authentication process and each system component, authentication should be observed to check that it is being implemented according to the documented methods. This helps the accounts from being used by outsiders since it requires not only the ID but also the authentication method such as a password, etc.

Strong cryptography should be applied so that messages transmitting through a medium are unreadable for third party. Messages that are transmitted unencrypted across a network or unencrypted passwords stored in a system are easily sniffed by malicious users to gain illegal access to data.

Before modifying an authentication credential, verification must be done so as to avoid the possibility of social engineering. Social engineering is an attempt by a malicious user to act as a legitimate authorized individual to extract important information, for example, requesting the helpdesk to change a particular password for a user ID. In such cases, a secret code or secret question should be asked which can only be known to and answered by the real user.

A sample of system components should be checked to see that passwords must be of a minimum length of seven characters, alphanumeric, and are changed after every 90 days at least. No user should be allowed to keep a password same as any of the previous four passwords.

**8.3 Incorporate two-factor authentication for remote network access originating from outside the network by personnel (including users and administrators) and all third parties, (including vendor access for support or maintenance).**

The requirement of two factor authentication relates to all users that access the network from a remote location such as vendors and administrators. This two factor authentication is required only when remote users can access cardholder data. Otherwise, when the network is segmented such that remote users cannot access the cardholder data, two factor authentication is not required.

For compliance, system configurations should be tested for remote access systems and server to check that any remote access by an employee or a vendor requires two factor authentication. It should also be checked that at least two out of the three authentication methods are being used.

**8.4 Document and communicate authentication procedures and policies to all users including:**

* **Guidance on selecting strong authentication credentials**
* **Guidance for how users should protect their authentication credentials**
* **Instructions not to reuse previously used passwords**
* **Instructions to change passwords if there is any suspicion the password could be compromised.**

Personnel should be interviewed to verify that they have been communicated all the above mentioned policies and procedures. Communication of authentication procedures and passwords helps to understand and follow the policies. Selection of strong authentication credentials means that a strong password should be used which is hard to guess by someone else. Protection of authentication credentials means that users should be guided that they should not write passwords in notepads or in insecure files, etc. Previously used passwords should not be used and in case of any warning of a login attempt, password must be immediately changed.

**8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows:**

* **Generic user IDs are disabled or removed.**
* **Shared user IDs do not exist for system administration and other critical functions.**
* **Shared and generic user IDs are not used to administer any system components.**

For compliance, a sample of user ID’s should be examined to verify that the above mentioned requirements are met and interview network administrators to ensure that shared IDs are not distributed even at the request of someone. When multiple users are using same passwords and/or user account, it is not possible to trace the responsible individual in case of breach of security. To prevent this, vendors that have remote access to customer CDE should have different authentication measures for every customer.

**8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows:**

* **Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts.**
* **Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.**

If the user authentication methods such as smart cards, tokens and certificates are allowed for use by multiple accounts, it is not possible to trace a single user at a certain time period. Physical or logical controls such as a password, biometric data or PIN must be applied so that every user is uniquely identified and unauthorized user cannot access through a shared authentication mechanism.

**8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows:**

* **All user access to, user queries of, and user actions on databases are through programmatic methods.**
* **Only database administrators have the ability to directly access or query databases.**
* **Application IDs for database applications can only be used by the applications (and not by individual users or other non-application processes).**

Database and application configuration settings should be reviewed to ensure that every user is authenticated before being granted access. Without authentication, the chances of a malicious individual getting into the system increase. What is more threatening is that the user cannot even be traced since that user is an unknown individual. Instead of providing direct access of the database to end users, the access should be provided through programmatic methods only, e.g. through stored procedures.

**8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.**

Personnel should be aware of security policies and procedures for identification and authentication on a regular basis.