**How to Comply to Requirement 7 of PCI DSS**

This requirement aims to achieve the objective of implementing strong access control measures to the cardholder data environment. The main goal of this requirement is to make it clear that only those personnel should be given access to the cardholder data environment that need this access as a part of completion of their job requirements.

**PCI DSS Requirement 7: Restrict access to cardholder data by business need to know.**

In order to make sure that sensitive information is only accessed by authorized individuals, all processes and systems should be configured for limited access on a need to know basis. PCI DSS has put forth specific requirements of how the access should be given and to which extent the access should be provided. Cardholder data is a valuable asset and it is important to control who accesses it, why it is accessed and how it is accessed.

**7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.**

This requirement is based on the fact that the fewer the number of people who can access the cardholder data, the least likely would be the violation of the PCI DSS. If more people are allowed to have access to the data, greater would be the risk of leakage of this data in malicious user’s hands. It is thus directed to limit access to only those individuals who have a genuine reason of doing so. Hence, the exploitation of cardholder data because of inexperience or deliberate bad intentions is prevented.

For limiting access to authorized individuals on a need to know basis, it is important to define the roles that have access needs, the devices they need to access and the extent to which each role needs the access. This is important to define how much access is allowed to every particular individual or job role within an organization.

To undergo a compliance procedure, a sample of roles should be selected and verification should be done against each role for the three aforementioned steps. It is also important to document the privileges of every role for reference purpose whenever an authorization to access needs to be done.

Every role should be given the least access privilege up to their requirement only. E.g. the database administrator should not be given the same access as a network administrator. This helps any unintentional changes in an application or security settings and also helps to reduce the scope of damage in case of an unauthorized access to a user account. The principle of least privilege (POLP) means that limited access up to a minimal extent is provided to the employees, processes and programs.

Speaking in the context of personal computing, security can also be increased by using an account other than that of the administrator. In administrator mode, the system becomes more vulnerable to online malicious coding that is not granted access when an account with lower privilege level is being used.

Another related principle known as privilege bracketing allows access permission level to be raised for some brief amount of time for a particular user. For example, a user can log in as an administrator for carrying out some task and as soon as the task is completed he/she can log out of the administrator account and log in from their own account with lesser privilege.

Personnel with the responsibility of assigning these privileges should be interviewed to verify that the access assigned to every role is on a need basis and with least required privilege.

**7.2 Examine written policy for access control, and verify that the policy incorporates 7.1.1 through 7.1.4 as follows:**

* **Defining access needs and privilege assignments for each role**
* **Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities**
* **Assignment of access based on individual personnel’s job classification and function**
* **Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved.**

There should be a proper mechanism to restrict user access as without it, an individual may be granted access even if it is not required for that particular user. For this purpose, a written policy is required to define allowed access along with every role and to automate the process of assigning privilege and restricting access. This is actually a technical control and it imposes the theory of Least Privileged Access Control. The multiple users of a system should be configured such that every user is provided the access appropriate to their specific job roles only. In other words, only because a system has multiple users, it does not mean that all of them should have the same level of access to information.

Security breach often occurs at the hands of insiders or employees of the organization in reality. In a few cases, it is done unintentionally or accidentally. In most cases, however, it is done with an intentional cause of bringing harm to the system and by misusing privileged access granted to the user. The least privilege principle thus helps to minimize the threats and possibility of damage through an accident or intentional unauthorized use of information.

There are various standards and interpretations that can be used for access control. A widely used standard is the ISO 17799 – Information Technology Code of Practice for Information Security Management. The ISO 17799 standard lays down information security management recommendations and also terms “access control” as one of the important risk mitigation controls.

To ensure compliance, all system settings and vendor documentation regarding the access control system needs to be verified for the following:

* Access control systems are applied to all system components.
* Access control systems are configured to provide restricted privileged access according to the job roles.
* Access control systems have a “deny-all” setting by default.

**7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.**

As with all other requirements of PCI DSS, compliance to the requirement 7 also demands that all the security policies and operational procedures regarding the restricted access to cardholder data should be put in a documented format, implemented and communicated to all the parties involved.