**How to Comply to Requirement 9 of PCI DSS**

**Requirement 9: Restrict physical access to cardholder data**

If physical access to devices and systems that hold cardholder data is not restricted, it can easily allow malicious individuals to get their hands on the data and even lead them to take hardcopies of sensitive data along with them. Physical access should be restricted for all onsite personnel, visitors and media personnel. Onsite personnel include all individuals who work as employees of the company in any way, visitors are outsiders who visit the faculty because of any work related issue or as guests, and media includes all print and electronic media.

**9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.**

The term “appropriate” is a relative term and its interpretation differs from organization to organization. What may be appropriate for one organization may not be the same for another. The geography, architecture, security technology, etc. of an organization play a part in developing and executing security controls to reduce and monitor access to cardholder data. Without these controls, such as, ID badges and biometric verification, unidentified people can enter a facility and steal important data.

To achieve compliance, presence of physical security controls should be verified in every data center, server rooms and all other facilities holding confidential data. Entry to such areas should be verified for security through keys, badges or other mechanisms. A sample of systems should be selected and the administrator should try to log in to these systems to check whether they are locked by the user or not.

Furthermore, verification must be done to ensure physical security through the following means:

* Installation of video cameras or other access control mechanisms to keep an eye on entry and exit areas. These should have mechanisms to prevent tampering and disablement.
* Restricted access to publicly available networks.
* Restricted access to wireless networks, handheld devices, gateways, telecommunication lines and all other hardware.

**9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include:**

* **Identifying new onsite personnel or visitors (for example, assigning badges)**
* **Changes to access requirements**
* **Revoking or terminating onsite personnel and expired visitor identification (such as ID badges).**

Any visitor entering the facility must be verified for being authorized to pay a visit and there must be some mechanism to differentiate outsiders from the employees.

Documented policies and procedures for visitors must be reviewed to verify that:

* New onsite individuals are distinguished from the regular employees .e.g by assigning a badge.
* Access to the distinguishing mechanism such as assigning badges, is limited to only authorized staff.
* Visitor identification mechanism, e.g. badge, is cancelled as soon as the visitor leaves. For example, the authorized staff has the responsibility to take back the badge before the visitor leaves.

**9.3 Control physical access for onsite personnel to the sensitive areas as follows:**

* **Access must be authorized and based on individual job function.**
* **Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards, etc., are returned or disabled.**

Access must be controlled in such a manner that only those employees should be allowed to visit the sensitive areas, who have a work-related need and are properly authorized. The following elements must be considered before granting access to cardholder data environment:

* The duration of access
* Permissible level of access
* Purpose of access

When a visit of an authorized individual to a sensitive area ends, it should be ensured that all access permissions are taken back from him/her and they cannot get access to the CDE again without authorized approval. It should also be verified that none of the recently terminated employees of the organization are trying to gain access to these areas.

**9.4 Implement procedures to identify and authorize visitors.**

There should be strong procedures to recognize the identity of visitors to check whether they are authorized to enter the sensitive areas of the facility or not. This helps to reduce unauthorized access of malicious individuals to the cardholder data environment. To achieve compliance in this area, the following requirements must be met and verified by the authority:

* All visitors should be verified before granting access and must be escorted throughout their visit to areas holding cardholder data.
* Visitor identification such as visitor badges must be identifiable from the inside personnel and should be expired after a certain condition is met.
* Visitors must be asked to return their badges before leaving the facility.
* Maintain a visitor log to keep a record of all individuals visiting the areas holding sensitive information. These logs must mention the name of the visitor, the company on whose behalf they are visiting and the inside personnel who granted them access.
* Keep the log records for a minimum of three months.

**9.5 Physically secure all media.**

A media backup consists of valuable information of cardholder data environment as well as other confidential data of the organization. Cardholder data is prone to being compromised if it is kept unprotected in a system, on a piece of paper on a desk or even kept unsecured in portable media. Storing backup media in a safe offsite location also prepares the organization to prepare for a business continuity plan to cater for safe backup in times of disaster.

It should be verified that the storage media is kept in a secure location, and its security is reviewed at least once a year.

**9.6 Maintain strict control over the internal or external distribution of any kind of media.**

Any media, in electronic or paper format, containing cardholder data should not be allowed for distribution unless deemed necessary. For compliance, it should be verified that a strict policy exists for media distribution. The following requirements must be verified to ensure safe distribution of data:

* All media devices should be classified so that it is easier to identify which once contains sensitive data.
* A log should be maintained for every media sent outside the company and it should be verified that it was sent through a reliable courier via and can be tracked.

**9.7 Maintain strict control over the storage and accessibility of media.**

If a secure inventory of the media is not maintained, lost or stolen media may go unnoticed for a long and indefinite time period. There must be a documented policy for storing media and a periodic inventory should be kept.

**9.8 Destroy media when it is no longer needed for business or legal reasons.**

Before disposing off any information lying in a device such as CD/DVD, hard disk or portable drive, it must first be completely destroyed so that it does not reach the hands of a malicious individual. An example of this is known as “dumpster diving” in which malicious individuals go through the trash cans of the company to search out for any valuable confidential information. For print media, use of paper shredders must be regulated while for electronic media methods such as wiping, grinding, degaussing, etc must be used for safely destroying the data.

For compliance to this requirement, the media destruction policy should be reviewed to verify the following:

* Cardholder data on electronic media must be securely wiped out according to the standard procedures or physically destroyed.
* Hardcopy data must be shredded and storage bins for material intended for destruction must be locked..

**9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.**

This requirement is related to skimming prevention in the payment card industry. Skimming is a process by which malicious individuals try to steal cardholder information by extracting information directly from debit and credit cards through device tampering or card reading devices.

For compliance to this requirement, a sample of devices and terminals should be tested to verify that they have not been tampered with. Additionally, all personnel should be trained to keep an eye on any mysterious behavior and immediately report any tampering or substitution of a device.

An updated list of devices should be maintained and the model, location and serial number of the devices should be enlisted. All devices should be examined at periodic intervals to look out for any tampering or replacement.

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

For compliance, it is necessary that all security policies and operational procedures for physical access restriction to cardholder data are formally documented, applied within the organization and communicated to all parties directly or indirectly involved in the storing, processing and transmitting cardholder data.