**How to Comply to Requirement 3 of PCI DSS**

**PCI DSS Requirement 3: Protect stored cardholder data.**

The requirement 3 of the PCI DSS states that stored cardholder data should be protected at all levels. Some of the protection techniques include encryption, masking, hashing and truncation. But the biggest problem faced with complying to this requirement is that merchants exactly need to know the data flow right from the start till the end.

The best and easiest way to comply is to identify all systems including servers, laptops, databases, etc that include cardholder data and encrypt any information available. Any system that is related to cardholder data eventually becomes a part of PCI DSS scope and compliance validation.

Furthermore, it is important to develop an understanding of how cardholder systems use firewalls and filter controls over the network. This would help to find out if any nearby systems come under the scope of PCI DSS compliance or not. Systems that retain cardholder data actually come out to be quite large, and include backup systems, development servers, middleware, data warehouses, etc.

**3.1. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage:**

* **Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements.**
* **Processes for secure deletion of data when no longer needed.**
* **Specific retention requirements for cardholder data.**
* **A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention**

Compliance to this requirement can be achieved by formulating a formal policy of data retention. This policy should indicate which type of data should be retained and which data needs to be destroyed when it is not needed anymore. The PCI DSS defines the Primary Account Number (PAN), cardholder name, expiration date and service code to be sensitive pieces of information that need to be protected after being stored. Either a manual or an automatic process should be set up which identifies which data needs to be stored and which needs to be destroyed and immediate action should be taken on data that needs to be deleted.

**3.2. Do not store sensitive authentication data after authorization (even if encrypted). If sensitive authentication data is received, render all data unrecoverable upon completion of the authorization process.**

For complying to PCI DSS, data that is termed as authentication data should not be stored beyond the retention period. This data includes magnetic strip contents, verification code and PIN. The deletion of such data is important as this data is extremely valuable for scammers as they can make fake duplicate payment cards based upon this information. If sensitive authentication data is received, follow the company procedure for safely deleting the data and verify that no recovery of the data is possible.

To verify that no data from magnetic stripe, verification code and Personal Identification Number is stored even after authorization, examine all data sources such as incoming and outgoing transaction details, logs, history files, trace files, database contents, etc.

**3.3. Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see the full PAN.**

Compliance to this requirement entails written policies and procedures for masking the display of Personal Account Number (PAN). These should enlist which roles are authorized to view full PAN and the legitimate reason of why they need to do so. Only the individuals with the roles enlisted should be able to see full PAN and any unauthorized individual should see PAN in masked form. PAN, if fully displayed on computer screens, receipts, fax or print out can be used for fraudulent purposes. Hence, it is a must to verify that PAN should be masked when it appears to any of the unauthorized individuals. System configurations and screens, receipts, etc., must be examined to achieve compliance.

**3.4. Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches:**

* **One-way hashes based on strong cryptography, (hash must be of the entire PAN)**
* **Truncation (hashing cannot be used to replace the truncated segment of PAN)**
* **Index tokens and pads (pads must be securely stored)**
* **Strong cryptography with associated key-management processes and procedures.**

According to PCI DSS, the Primary Account Number (PAN) can be stored after a transaction but it must be made illegible by using techniques such as encryption, truncation or hashing. If the PAN stores the cardholder name, expiration date and service code, additional efforts to protect the data should be adopted. But if they are stored separately from the PAN then no additional efforts are required. Hence, the storage plan of these pieces of information must be carefully planned to minimize the complexity.

Key management is also important when encryption is being used for compliance purposes. To make encryption more effective, limit the access to keys used for decrypting the cipher text. By limiting the key backup location, not only can we restore the key easily in time of need, we can also put a limit to number of individuals who can acquire and restore the keys.

**3.5. Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.**

It is extremely important to protect cryptographic keys as any access to key by a fraudulent individual means that the information can be decrypted by them and used for all the wrong purposes. Strict policies and procedures should be implemented and should ensure the following:

* Keys are only access by the fewest possible individuals
* Key-encrypting keys are as strong as the data encrypting keys
* Key-encrypting keys and data encrypting keys are stored in separate locations
* Keys are stored in fewest possible locations

**3.6. Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.**

Management of cryptographic keys is as important as the implementation of the encryption process itself. For compliance purposes it is important to develop and examine the documentation that is provided to customers as a guidance to protect the cryptographic keys. They should have a complete understanding of how to securely store, transmit and update the keys without disclosing them to an unauthorized entity.

An effective key management procedure must address the following areas:

* Generation of strong cryptographic keys
* Secure distribution of keys
* Secure storage of keys
* Cryptographic period for keys, after which the keys should be changed
* Deletion or replacement of keys whenever the need arises
* Dual control and split knowledge of clear text cryptographic key management operations
* Prevention of unauthorized key substitution
* Acknowledgement of key custodians that they understand their key-custodian responsibilities

Each of these procedures must then be examined and verified to ensure compliance.

**3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.**

In order to comply with this requirement, it is necessary that personnel are well aware of security policies and procedures to manage the safe storage of cardholder data on a regular basis. Personnel should be interviewed from time to time to verify that they understand and implement those policies and operational procedures in their routine work involving cardholder data handling.