**Introduction to PCI DSS**

The Payment Card Industry – Data Security Standard (PCI – DSS) consists of a minimum set of necessary requirements that every merchant and/or service provider must meet in order to protect the cardholder data of their customers. This standard has been formulated by the PCI Security Standard Council which was formed by the five major card companies MasterCard, American Express, VISA, JCB and Discover. This set of requirements serves as a guideline to ensure the protection and security of their card information. Compliance to the PCI DSS is mandatory for all organizations that store, process and transmit cardholder data in order to allow their users to carry out secure card transactions.

**Purpose of PCI DSS**

The basic purpose of implementing the PCI DSS is to prevent any compromise of cardholder information at the hands of a malicious user. It helps merchants to protect their clients from facing any fraud over the internet, or in day to day credit card transactions by fulfilling all the requirements. By having a proactive approach towards the security of cardholder data, merchants decrease the probability of any potential online theft, fraud and security breach, which in turn helps prevent them from undergoing financial loss in the long run.

**Basic Requirements of PCI DSS**

The PCI Data Security Standard consists of 12 requirements that have been laid down under 6 different categories.

|  |  |
| --- | --- |
| **Objectives** | **PCI DSS Requirements** |
| Build and Maintain a Secure Network and Systems | 1. Install and maintain a firewall configuration to protect cardholder data |
| 1. Do not use vendor-supplied defaults for system passwords and other security parameter |
| Protect Cardholder Data | 1. Protect stored cardholder data |
| 1. Encrypt transmission of cardholder data across open, public networks |
| Maintain a Vulnerability Management Program | 1. Protect all systems against malware and regularly update anti-virus software or programs |
| 1. Develop and maintain secure systems and applications |
| Implement Strong Access Control Measures | 1. Restrict access to cardholder data by business need to know |
| 1. Identify and authenticate access to system components |
| 1. Restrict physical access to cardholder data |
| Regularly monitor and test networks | 1. Track and monitor all access to network resources and cardholder data |
| 1. Regularly test security systems and processes. |
| Maintain an Information Security Policy Maintain a policy that addresses information security for all personnel | 1. Maintain a policy that addresses information security for all personnel |

The table above only shows the basic set of requirements for PCI DSS compliance. Each of these requirements has further been sub divided into more specific requirements.

The six basic requirements of the PCI DSS can be summarized as below:

1. Secure networks must be implemented and regularly maintained in order to carry out safe transactions. This objective can be achieved by using user-friendly firewalls that help protect the information without causing any inconvenience to the cardholders. In addition to that, all passwords and PIN codes must be changed from default to passwords and PIN codes of your own choice as default passwords and codes can easily be guessed by hackers.
2. The cardholder information such as birth date, social security number, phone number postal address, etc., needs to be kept secure whenever and wherever it gets stored. If the cardholder data needs to be transmitted publicly, it must be encrypted.
3. All systems should have their anti-virus and anti-spyware programs regularly updated. This is necessary to prevent a malicious user from acquiring important information from the system. In order to ensure the maximum level of security and clear the applications of any possible vulnerabilities, patches provided by operating systems and software programs should be installed on a regular basis.
4. Restricted access to the systems should be exercised. Sensitive cardholder information should only be allowed to be accessed by authorized personnel. Every individual using the system should be given a unique ID in order to keep a track of their activities. Apart from protecting cardholder information electronically, physical protection must also be ensured. The use of document shredders and locks on dumpsters should be enforced within the organization.
5. All networks should be regularly monitored and tested in order to make sure that all systems are updated and not prone to any vulnerability. Applications, RAM’s and storage areas should be regularly scanned to detect any potential threat.
6. A complete information security policy should be formulated and maintained, and must be regulated to all concerned bodies. A system should be developed to ensure that the policy is understood and followed by every individual and strict penalty should be specified in case of non compliance. Regular audits must be conducted for this purpose.

**How to comply to PCI DSS?**

In order to comply to the PCI Data Security Standard, the following basic steps must be considered:

1. **Evaluate your Business Processes**

* Understand and develop know-how of the detailed requirements of the PCI DSS.
* Perform an audit of the cardholder data environment against the PCI DSS either with the help of a PCI Qualified Security Assessor (QSA), a Self-Assessment Questionnaire (SAQ), or by conducting vulnerability scan with the help of an Approved Scanning Vendor (ASV). The choice of audit type depends upon the company volume and compliance requirement.
  + A Self Assessment Questionnaire (SAQ) is a compliance validation method for those merchants who are not required to conduct on-site assessment for PCI DSS.
  + Qualified Security Assessors are independent experts who provide skilled consultants to assess and ensure compliance with the PCI DSS.
  + Approved Scanning Vendors conduct vulnerability scans by providing commercial software tools.

1. **Remediate the Vulnerabilities**

The vulnerabilities found after the evaluation need to be fixed as a part of the compliance process.

* Review the vulnerabilities found in the evaluation process.
* Classify and prioritize the vulnerabilities in order of the most serious to the least one.
* Apply patches and fixes to any technical flaws or unsecure practices.
* Re-evaluate the system.

1. **Report the Compliance Process**

Finally, a report needs to be compiled in order to validate the compliance according to the PCI DSS and submit it to the banks and payment brands with which business is carried out.

1. Acquire or prepare a Report on Compliance (ROC), based upon your audit method.
2. Implement required actions in the system according to the ROC, to comply with the PCI DSS requirements and again validate the steps according to the standard.
3. Communicate with only those third parties that are also compliant with the PCI Data Security Standard.

Since compliance is an ongoing process, it is recommended to perform annual audits to ensure real time safety and security of the systems. Compliance needs to be monitored constantly and enhanced according to needs within the organizational policies and procedures.