NTT SECURITY

THE 12 PCI DSS REQUIREMENTS IN A NUTSHELL

By NTT Security

12 steps to compliance with the guidance of NTT Security

* BUILD AND MAINTAIN A SECURE NETWORK

Req. (1) Install and maintain a firewall configuration to protect cardholder data

Req. (2) Do not use vendor-supplied defaults for system passwords and other security parameters

* PROTECT CARDHOLDER DATA

Req. (3) Protect stored cardholder data

Req. (4) Encrypt transmission of cardholder data across open, public networks

* MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Req. (5) Use and regularly update anti-virus software

Req. (6) Develop and maintain secure systems and applications

* IMPLEMENT STRONG ACCESS CONTROL MEASURES

Req. (7) Restrict access to cardholder data by business need-to-know

Req. (8) Assign a unique ID to each person with computer access

Req. (9) Restrict physical access to cardholder data

* REGULARLY MONITOR AND TEST NETWORKS

Req. (10) Track and monitor all access to network resources and cardholder data

Req. (11) Regularly test security systems and processes

* MAINTAIN AN INFORMATION SECURITY POLICY

Req. (12) Maintain a policy that addresses information security

The Payment Card Industry Data Security Standard (as such the acronym PCI DSS) defines a security baseline for any organisation that processes, transmits or stores cardholder data. The idea behind the standard is to guide organisations towards applying a layered approach to the security of the Card Holder Data. It has to be kept clear in mind that the PCI DSS is a selfish standard which only takes into consideration the confidentiality of the data at risk (Namely Account Data, Card Holder Data, PAN, CVx Codes and so on), the availability of such data is not taken into consideration while the Integrity is addressed only around historical data needed for eventual forensics purposes.

PCI DSS STANDARD HAS THE AIM TO PROTECT THE CONFIDENTIALITY OF CARD HOLDER DATA TO REDUCE THE RISK OF FINANCIAL AND IMAGE LOSS AT ALL THE LEVELS OF THE CARD PAYMENT'S CHAIN.

PCI DSS is divided in 12 macro areas defined as requirements, each one addressing security controls at different layers. Let's first make a list of the specific 12 requirements to have a full perspective, thus let's analyze each one of them.

	REQUIREMENTS	DESCRIPTION
BUILD AND MAINTAIN A SECURE NETWORK	(1) Install and maintain a firewall configuration to protect cardholder data	Firewalls and routers are key components of the architecture that controls entry to and exit from the network. These devices are software or hardware devices that block unwanted access and manage authorized access into and out of the network. Because of that, they should be configured so to ensure that the organization's first line of defense in the protection of its data remains strong.
BUILD AND MAINTAIN A SECURE NETWORK	(2) Do not use vendor-supplied defaults for system passwords and other security parameters	Malicious individuals, both external and internal to a company, often use vendor default settings, account names, and passwords to compromise systems. These settings are well known in hacker communities and leave your system highly vulnerable to attack, as they are easily determined via public information.
PROTECT CARDHOLDER DATA	(3) Protect stored cardholder data	Protection methods such as encryption, truncation, masking, and hashing are critical components of cardholder data protection. If an intruder circumvents other security controls and gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person. Other effective methods of protecting stored data should be considered as potential risk mitigation opportunities. For example, methods for minimizing risk include not storing cardholder data unless absolutely necessary, truncating cardholder data if full PAN is not needed, and not sending unprotected PANs using end-user messaging technologies, such as e-mail and instant messaging.
PROTECT CARDHOLDER DATA	(4) Encrypt transmission of cardholder data across open, public networks	Sensitive information must be encrypted during transmission over networks that are easily accessed by malicious individuals. Misconfigured wireless networks and vulnerabilities in legacy encryption and authentication protocols continue to be targets of malicious individuals who exploit these vulnerabilities to gain privileged access to cardholder data environments.
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	(5) Use and regularly update anti-virus software	Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business- approved activities including employee e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect systems from current and evolving malicious software threats.

	REQUIREMENTS	DESCRIPTION
MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM	(6) Develop and maintain secure systems and applications	Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software. Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.
IMPLEMENT STRONG ACCESS CONTROL MEASURES	(7) Restrict access to cardholder data by business need-to-know	To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities. “Need to know” is when access rights are granted to only the least amount of data and privileges needed to perform a job.
IMPLEMENT STRONG ACCESS CONTROL MEASURES	(8) Assign a unique ID to each person with computer access	Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users. These requirements are applicable for all accounts, including point-of-sale accounts, with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data.
IMPLEMENT STRONG ACCESS CONTROL MEASURES	(9) Restrict physical access to cardholder data	Any physical access to data or systems that house cardholder data provides the opportunity for individuals to access devices or data and to remove systems or hardcopies, and should be appropriately restricted. For the purposes of Requirement 9, “onsite personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are physically present on the entity’s premises. A “visitor” refers to a vendor, guest of any onsite personnel, service workers, or anyone who needs to enter the facility for a short duration, usually not more than one day. “Media” refers to all paper and electronic media containing cardholder data.

	REQUIREMENTS	DESCRIPTION
REGULARLY MONITOR AND TEST NETWORKS	(10) Track and monitor all access to network resources and cardholder data	Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.
REGULARLY MONITOR AND TEST NETWORKS	(11) Regularly test security systems and processes	Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.
MAINTAIN AN INFORMATION SECURITY POLICY	(12) Maintain a policy that addresses information security	A strong security policy sets the security tone for the whole entity and informs personnel what is expected of them. All personnel should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this Requirement 12, “personnel” refers to full-time and part-time employees, temporary employees, contractors and consultants who are “resident” on the entity’s site or otherwise have access to the cardholder data environment.

NTT SECURITY

mail@ntt.ie - sales@ntt.ie

ITALY
NTT Security Srl
Viale Luca Gaurico 9/11
00143 Roma
Tel. e Fax +39 06 92958418
www.ntt-security.it

IRELAND
Headquarters
NTT Security ltd
120/121 Baggot Street Lower
Dublin - Ireland
T. +353(0)15065556
www.ntt-security.com

UKRAINE
NTT Security CIS
Str. Petra Sagaidachnogo, 25B
Poshtova Ploscha (249 m)
Kiev Ukraine
T. +380 44 4985151
Fax +380 44 4985100