tas group
an owl company

White Paper

PCI DSS impacts to your company

If an organization is involved in the storage, processing or transmission of cardholder data, then it is subject to the requirements of PCI DSS (Payment Card Industry Data Security Standard).

For an organization to be considered compliant with the PCI DSS all requirements specified in the standard have to be in place or appropriate compensating controls must be in place.

Once an organization has achieved PCI DSS compliance, they must ensure that they continue to be compliant.

Full and detailed information on PCI DSS can be obtained from the PCI SSC (Payment Card Industry Security Standards Council) web site www.pcisecuritystandards.org .

INDEX

INTRODUCTION

Back in the years the different payment card schemas each had their minimum set of security programs with which all actors involved in electronic payments were prompted to comply with.

Subsequently, the major credit card companies (Visa, MasterCard, Discover, American Express, and JCB) came together and formed the PCI Security Standards Council (PCI SSC), a neutral organization that aligned the distinct policies and in December 2004 released PCI DSS version 1.0 creating one uniform set of requirements with which all parties could easily comply.

There are 12 PCI DSS requirements that impact different security aspects. Areas of focus include building and maintaining a secure network, protecting stored cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining information security policies. As all standards, PCI DSS entails a minimum set of requirements and over the years, the standard has undergone clarifications, revisions, addition of guidelines on areas such as wireless, virtualization, personal identification number (PIN) entry devices, and of course, version updates: the most recent. PCI DSS version 2.0 was released in October 2010 and went into effect January 1, 2011. PCI DSS version 3.0 has been published in November 2013 and will be fully effective from January 2015.

The PCI DSS framework is all about assessment, remediation, and reporting and may be subdivided into 6 areas.

Goals	PCI DSS Requirements
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Assign unique ID to each person with computer access. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

The following table identifies the various data elements or items of sensitive cardholder information. The table also indicates whether it is permissible under PCI DSS for each data element to be stored on the system, if protection is required and if it needs to be rendered unreadable as per PCI DSS Requirement 3.4.

	Data Element	Storage Permitted	Render Stored Account Data Unreadable per Req. 3.4
Cardholder Data	Primary Account Number (PAN)	Yes	**Yes**
	Cardholder Name	Yes	No
	Service Code	Yes	No
	Expiration Date	Yes	No
Sensitive Authentication Data	Full Magnetic Stripe Data 2	No	Cannot store per Req. 3.2
	CAV2/CVC2/CVV2/CID	No	Cannot store per Req. 3.2
	PIN/PIN Block	No	Cannot store per Req. 3.2

ACHIEVING PCI DSS COMPLIANCE

The PCI DSS requirements apply to all “system components”, defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP servers. Applications include all purchased and custom applications, including internal and external web applications. The cardholder data environment is a combination of all the system components that come together to store and provide access to sensitive user financial information.

The aim of this white paper is to outline the processes which an organization abiding to PCI DSS compliance should have in place. For each of the 12 PCI DSS requirements you will find an explanatory paragraph and the relevant actions that should be undertaken.

When throughout the document the “cardholder environment” is mentioned, the term is referred to the company infrastructure dealing with cardholder data.
All policies and process mentioned are primarily intended applicable to the cardholder environment.

BUILD AND MAINTAIN A SECURE NETWORK

REQUIREMENT 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 company’s cardholder network . These devices are either software or hardware devices that block unwanted access and manage authorized access into and out of the network and as such, these must be configured so to ensure the first line of defense in the protection cardholder data remains strong.

Your actions
A company policy must be defined outlining the formal process concerning testing and approval of all network connections and all configuration changes for both firewalls and routers. Network and data flow diagrams, including virtual system components and intra-host data flows, must also be defined and constantly kept up to date; such documents/diagrams must outline that no direct connection is allowed for traffic between the Internet and the cardholder data environment.
The policy must also include requirements for firewall configuration at each Internet connection and between any DMZ and the cardholder network.
Firewall and router configuration standards must list services, protocols and ports necessary for business and if any insecure services, protocols or ports are allowed these should be have a thorough business justification Review of firewall rule sets must be carried out at least twice a

year and personnel responsibilities for such duties, must be specified and duly acknowledged. Document how inbound and outbound traffic is limited to what is strictly required by the cardholder data environment and detail all restrictions in place.

Define system components that provide authorized publicly accessible services, protocols, and ports and specify which firewall/router configurations ensure that the DMZ limits inbound traffic to only those system components. Define authorized outbound traffic from the cardholder data environment to the Internet and detail firewall/router configurations allowing only explicitly authorized traffic
Define methods in place to prevent the disclosure of private IP addresses and routing information from internal networks to the Internet. Report any firewall/router configurations implementing that. Define whether mobile and/or employee-owned computers with direct connectivity to the Internet are used to access the organization's network and have personal firewall software installed and active.

REQUIREMENT 2: DO NOT USE VENDOR-SUPPLIED DEFAULTS FOR SYSTEM PASSWORDS AND OTHER SECURITY PARAMETERS

Malicious individuals (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.

Your actions
Define a company policy to require the following:

- if wireless encryption is used within the cardholder environment, the keys must be changed from their default values at installation and whenever anyone with knowledge of the keys leaves the organization or changes positions; firmware on wireless devices must be updated to support strong encryption for both transmission and authentication
- default SNMP community strings and default passwords/passphrases on access points must be changed
- any other security-related vendor defaults must be changed prior deployment
- the process for updating system configuration standards as new vulnerability issues are identified
- the process for applying system configuration standards to new systems.

Document system configuration standards so that all types of system components are covered, all known security vulnerabilities are addressed.
Specify industry-accepted hardening standards for all components within the cardholder environment and ensure that:

- only one primary function is implemented per server, including virtual system components for devices, as applicable
- only necessary services or protocols are enabled and security features are implemented for any required services, protocols or daemons considered insecure and specify for which

business reason each enabled service, daemon and protocol is necessary for the specific component
- system security parameters are configured to prevent misuse
- all unnecessary functionalities (for example, scripts, drivers, features, subsystems, file systems, etc.) are removed
- for each insecure service, daemon, or protocol identified a proper and thorough business justification is given and define security features for the insecure service, daemon or protocol
- common security parameter settings are defined and all authorized functions allowed are listed and documented.

PROTECT CARDHOLDER DATA

REQUIREMENT 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.

Your actions

Define a company policy concerning legal, regulatory, business requirements for data retention. The policy should also entail:

- PAN display, requiring that PAN be masked when displayed, except for those with a legitimate business need to see full PAN
- PAN storage, describing the implemented methods used to render the PAN unreadable, using any of the PCI DSS accepted methods
- procedures for encryption keys used to render cardholder data unreadable: generation of strong keys, secure key distribution and storage, periodic key changes at the end of each crypto-period, retirement of keys when their integrity has been weakened, replacement of known or suspected compromised keys; unauthorized substitution of keys
- if the company under assessment is a service provider specify whether keys are shared with customers for transmission or storage of cardholder data; if this is the case then, provide customers with guidance on how to securely transmit, store, and update customers' keys in accordance with PCI DSS Requirements 3.6.1-8 and define how the document is being provided to customers
- in case of clear-text cryptographic key management define procedures requiring split knowledge of keys and dual control of keys
- define procedures for key custodians to acknowledge that they understand and accept their key-custodian responsibilities.

Make sure that processes listed below are regularly carried out and reviewed at least on a quarterly basis:

- secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data
- if your company is not n an issuer and/or a company supporting issuing services, ensure that sensitive authentication data is exclusively retained for the time interval required to complete the authorization transaction
- ensure that stored cardholder data does not exceed requirements defined in the data retention policy

- identify and list personnel with a legitimate business need to see full PAN
- identify whether retired or replaced cryptographic keys are retained; if retired or replaced cryptographic keys are retained, require that these keys be securely archived and not used for encryption operations.

REQUIREMENT 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.

Your actions

Define a company policy requiring that PAN and Sensitive Authorization be encrypted when transmitted over open public networks. For each communication link report methodology in use and vendor recommendations/best practices for encryption strength.

Document all wireless networks transmitting cardholder data or connected to the cardholder data environment and for each specify the industry best practices used to implement:

- Strong encryption for authentication
- Strong encryption for transmission

Explicitly mandate that unprotected PANs must not be sent via end-user messaging technologies.

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

REQUIREMENT 5: USE AND REGULARLY UPDATE ANTI-VIRUS SOFTWARE OR PROGRAMS

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.

Your actions

Define a company policy specifying the need for of anti-virus software to be installed on all cardholder environment’s servers desktops and laptops. Also require that:

- Anti-virus software is configured for periodic scans
- Anti-virus software log generation is enabled
- Anti-virus logs are suitably retained.

REQUIREMENT 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.

Your actions

Define a vulnerability management policy to:

- identify the risk ranking method enforced to classify risks and address high priority risk items quickly
- list outside sources to be used in identifying new security vulnerabilities.
- specify all vendors’ repositories which define security patch lists
- require that all critical new security patches be installed within one month.

Define a software development policy specifying how software applications are developed in accordance with PCI DSS requirements, based on industry standards and/or best practice such

as OWASP and SANS CVE Top 25 and entailing information security throughout the software development life cycle. The same policy must specify that developers follow a training program in secure coding techniques specifying the industry best practices and guidance that program is based upon.

The software development process must:

- require removal of custom application accounts, user IDs and/or passwords before the system goes into production or is released to customers
- require that all custom application code changes be reviewed
- detail processes used for reviewing custom application code changes (acceptable methods may be manual or automated, or a combination of both), so that:
  - all custom application code changes are reviewed by individuals other than the original author and have proven experience and knowledge about code review techniques and secure coding practices
  - any remediation identified during the code review are implemented prior to release
  - code review results are reviewed by management prior to release
- define how the development/test environment is separated from the production environment, define access controls to enforce separation of environments, require separation of duties between personnel assigned to the development/test environment and those assigned to the production environment and describe how separation of duties is implemented
- define processes for ensuring that live PANs are not used for development/testing
- define processes for removing test data and test accounts before a production system becomes active
- define change control procedures for implementation of security patches and software modifications, in a way that they require the following for all changes:
- documentation of impact
- documented approval by authorized parties
- testing of functionality to ensure the change does not introduce impact the security of the system
- back-out procedures
- define the process for ensuring tha applications are not vulnerable to:
  - injection flaws, particularly SQL injection
  - buffer overflow
  - insecure cryptographic storage
  - insecure communications
  - improper error handling
  - “High” vulnerabilities as identified in PCI DSS Requirement 6.2
  - cross-site scripting (XSS)
  - improper access control
  - cross-site request forgery

Furthermore, for public-facing web applications the company policy should define if web application vulnerability security assessments, web application firewalls, or both methods are implemented. If application vulnerability security assessments are performed, describe the tools

and/or methods used (manual or automated, or a combination of both). Require that assessments be carried out at least annually and after any changes.

IMPLEMENT STRONG ACCESS CONTROL MEASURES

REQUIREMENT 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.

Your actions

Define a data control policy specifically aimed at cardholder environment requiring:

- that privileges be assigned to individuals based on job classification and function
- that access rights for privileged user IDs be restricted to the least privileges necessary to carry out job responsibilities
- documented approval by authorized parties for any access
- that documented approval must specify the required privileges
- that access controls be implemented using an automated access control system.

For each access control system in use, describe job classifications and functions, and the associated privilege assignments. Also, specify that any access control system is required to have a default “deny-all” setting.

REQUIREMENT 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.

Your actions

Define a company policy:

- requiring that users are assigned a unique ID before being allowed to access system components or cardholder data.
- outlining the authentication method(s) used, for example, a password or passphrase, a token device or smart card, a biometric, etc.;
- requiring both users to be authenticated using a unique ID and additional authentication for access to the cardholder data environment
- for each type of system component within the cardholder environment describe the

authentication methods used

- specifying the two-factor authentication technologies implemented for remote access to the network and, also, specify which two factors out of the following are used: something you know, something you are, something you have
- when issuing first-time passwords to new users, define procedures to require that first-time passwords must be set to a unique value for each user and that these must be changed at the first logon
- outlining procedures for resetting existing users' passwords to require that passwords must be set to a unique value for each user and that these must be changed after the first use
- specifying the following guidance rules concerning passwords management and characteristics:
  - passwords must be changed periodically,
  - outline circumstances requiring a password change
  - passwords must have minimum length requirements and use both numeric and alphabetic characters
  - new passwords must not be the same as the previous four passwords
  - passwords to be temporarily locked out after not more than six invalid access attempts
  - explicitly prohibit group passwords or other authentication method and shared passwords or other authentication methods
- specifying the non-face-to-face method used for password reset requests, requiring the user's identity to be verified before the password is reset
- requiring that access be immediately revoked for any terminated users and that inactive user accounts over 90 days old are either removed or disabled.
- once a user account is locked out, require that it remains locked for a minimum of 30 minutes or until a system administrator resets the account.
- specifying in the system configuration standards the time (in minutes) that system and/or session idle time-out features are set and requiring the user to re-authenticate to re-activate the terminal or session.
- requiring that accounts used by vendors to access, support and maintain system components are disabled when not in use, enabled only needed and monitored when in the enabled state.

Define authorization forms for both administrator and general user IDs, which would reflect their exact implementation on all involved systems. Make sure all the appropriate signatures for authorization are included.

REQUIREMENT 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.

Your actions

Define a company policy for:

- assigning badges to onsite personnel, to include granting new badges, changing access requirements and revoking badges for terminated onsite personnel
- assigning badges to visitors, to include granting new badges, changing access requirements and revoking badges for terminated onsite personnel
- the management of the visitor log to contain visitor name, firm represented, onsite personnel authorizing physical access
- specifying personnel authorized to access the badge system
- specifying the defined retention period for visitor logs (should be 3 months as a minimum, unless otherwise restricted by law)
- specifying the procedures for protecting cardholder data, in a way they would include controls for physically securing all media
- reviewing the security of each storage location at least annually
- specifying controls for distribution of media, in a way that it covers all media distributed to individuals.
- specifying how media is classified to determine sensitivity of data
- specifying requirements for controlling storage of all media, controlling maintenance of all media and periodic inventories for all media
- specifying a process on conducting media inventories at least annually
- specifying media destruction requirements for all involved media, hardcopy materials and f electronic media, detailing methods and industry-accepted standards used for secure wiping of media, and/or physical destruction of media.

REGULARLY MONITOR AND TEST NETWORKS

REQUIREMENT 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.

Your actions

Define a company policy:

- specifying the time synchronization technologies in use within the cardholder environment
- describing the processes in place to ensure time synchronization technologies are kept current as per PCI DSS Requirements 6.1 and 6.2
- describing the processes in place for acquiring, distributing, and storing the correct time within the organization, requiring that only designated central time servers (more than one) receive time signals from different external sources in turn based on International Atomic Time or UTC; require that designated central time servers peer with each other to keep accurate time and other internal servers receive time only from the central time servers; require that access to time data is restricted to only personnel with a business need and list such personnel; require that changes to time settings on critical systems are logged, monitored and reviewed
- specifying the file-integrity monitoring (FIM) or change-detection software in use
- specifying and describing the centralized log server or media that audit trail files are backed up to, how frequently the audit trail files are backed up (in a way that the frequency is appropriate) and the measures in place to grant that the centralized log server or media is difficult to alter
- describing how logs for external-facing technologies (e.g. wireless, firewalls, DNS, mail) are offloaded or copied onto a secure centralized internal log server or media
- requiring all system components logs to be reviewed at least daily, including those that perform security functions, and to follow-up on exceptions
- specifying the audit log retention in place and these be carried at least once a year
- specifying the process for immediate restoring of at least the last three months' logs for analysis
- specifying the methods used to protect audit trail files from unauthorized modifications (e.g., via access control mechanisms, physical segregation, and/or network segregation)
- listing personnel having a job-related need to view audit trail files or are responsible for monitoring FIM and/or change detection software.

REQUIREMENT 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.

Your actions

Define a company policy :

- specifying the methods and processes to detect wireless access points and identify unauthorized wireless access points, ; these activities should be carried out at least on a quarterly basis; describe the methodology for detection and identification of unauthorized wireless access points, including:
  - WLAN cards inserted into system components
  - Portable wireless devices connected to system components
  - Wireless devices attached to a network port or network device
  - Any other unauthorized wireless access points
- specifying the Incident Response Plan defining response procedures in the event unauthorized wireless devices are detected
- explicitly requiring that internal scans must occur at least quarterly in a 12-month period or when there has been a change within the cardholder environment network; specify whether internal and/or external resources perform internal quarterly scans, describing how these resources are actually qualified to perform such scans and how organizational independence of the tester is proved to exist; require rescans until passing results are obtained, or all “High” vulnerabilities as defined in PCI DSS Requirement 6.2 have been taken care of
- explicitly requiring that quarterly external scans must occur within a 12-month period, or after any significant change in the cardholder environment, and the relevant reports satisfy the ASV Program Guide requirements ; require rescans until no vulnerabilities with a CVSS score greater than 4.0 is found; define the PCI SSC Approved Scanning Vendor (ASV) used
- requiring that:
  - internal penetration tests are performed annually and include both network-layer penetration tests and application-layer penetration tests which in turn include at least vulnerabilities listed in PCI DSS Requirement 6.5
  - external penetration tests are performed annually and include application-layer penetration tests which in turn include at least vulnerabilities listed in PCI DSS Requirement 6.5
  - network layer penetration tests include all components supporting network functions and all operating systems, and are performed after significant internal or external infrastructure or application upgrade
  - noted exploitable vulnerabilities must be corrected and testing repeated
- specifying the implemented intrusion-detection and/or intrusion-prevention systems, describing how these are positioned within the cardholder environment to ensure that all traffic is monitored; outline how IDS/IPS are configured to alert personnel of suspected compromises;

define vendor instructions for configuring, maintaining and updating IDS/IPS devices

- specifying the file-integrity monitoring (FIM) tools deployed; describe how FIM is configured to monitor changes to critical system, system, and configuration files,; describe how FIM is configured to alert personnel when unauthorized modification of critical files is detected and require that critical file comparison be carried out at least weekly.

MAINTAIN AN INFORMATION SECURITY POLICY

REQUIREMENT 12: MAINTAIN A POLICY THAT ADDRESSES INFORMATION SECURITY FOR ALL PERSONNEL

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.

Your actions

Define an information security policy to address all applicable PCI DSS requirements pertaining to the company’s cardholder environment; ensure the policy is published and disseminated to all relevant personnel and also to all relevant vendors and business partners. Require that the information security policy be reviewed at least annually and be updated when necessary to reflect changes to business objectives or to company’s cardholder environment. Clearly define information security responsibilities for all personnel.

Define a company policy for the annual risk assessment process which must identify threats and vulnerabilities and produce a forma risk assessment

List daily operational security procedures outlining how these are consistent with PCI DSS requirements.

Define a company policy listing all critical technologies in use within the cardholder environment. For each critical technology:

- define a policy outlining proper use of the technology and requiring explicit approval from authorized parties to use the technology
- require that use of the technology be authenticated with user ID and password or other authentication item
- list of all devices and personnel authorized to use the devices
- require that each device be labeled with information that can be correlated to owner, contact information and purpose
- for each identified critical technology describe acceptable uses for the technology, describe acceptable network locations for the technology and report a list of company-approved products

Define a company policy listing all remote-access technologies used. Specify the remote-access technologies used by vendors and business partners. For each remote-access technology,

require automatic disconnect of sessions after a specific period of inactivity, activation of the technology only when needed and immediate deactivation of the technology after use.

Define a company policy to :

- explicitly Prohibit the following for personnel accessing cardholder data via remote-access technologies:
  - copying of cardholder data onto local hard drives and removable electronic media
  - moving of cardholder data onto local hard drives and removable electronic media
  - storage of cardholder data onto local hard drives and removable electronic media
- specify whether any authorized business need for copying, moving, or storing cardholder data onto local hard drives or removable electronic media via remote-access technologies exists; for each defined business need, require the protection of cardholder data in accordance with PCI DSS Requirements, for all personnel with proper authorization.

Formally assign responsibility to specific personnel for :

- information security to a Chief Security Officer or other security-knowledgeable member of management
- defining and distributing security policies and procedures
- monitoring and analyzing security alerts and distributing information to appropriate information security and business unit management personnel
- defining security incident response and escalation procedures and distributing security incident response and escalation procedures
- administering user account and authentication management
- monitoring and controlling all access to cardholder data
- security breaches and ensure they are periodically trained.

Define a company policy for formal security awareness program to personnel within cardholder environment and specifying methods of communicating awareness and educating personnel; require that all personnel attend awareness training upon hire and at least annually; where applicable by local laws require, prior to hiring personnel, that background checks be conducted on potential personnel who will have access to cardholder data or the cardholder data environment .

List all service providers with whom cardholder data is shared and require that the list be kept up-to-date. For each service provider with whom cardholder data is shared, define the document that includes service provider acknowledgment of their responsibility for securing cardholder data. Define procedures for proper due diligence prior to engaging any service provider.

Define an incident response plan and require that it be tested at least annually. Define incident response plan documents and appoint personnel to be available on a 24/7 basis for incident monitoring and response concerning any evidence of unauthorized activity, detection of unauthorized wireless access points, critical IDS alerts and unauthorized critical system or content file changes.

Define how the following are monitored:
- alerts from intrusion-detection/intrusion-prevention
- alerts from file-integrity monitoring systems
- detection of unauthorized wireless access points.

Define how the following are responded to:
- alerts from intrusion-detection/intrusion-prevention
- alerts from file-integrity monitoring systems
- detection of unauthorized wireless access points.

Define processes to modify and evolve the incident response plan:
- according to lessons learned
- to incorporate industry developments.

SUPPORT ON PCI DSS COMPLIANCE FROM TAS

TAS is a world known Independent Software Vendor with a wide variety of products within the e-Payments scope, all of which are compliant to PCI DSS requirements.

For PCI DSS compliance, TAS has enhanced its e-Payments suite of products implementing a solution compliant to PCI DSS Requirement 3 and Requirement 10.

The solution has the following characteristics:

- modular and platform independent
- compliant to sensitive authorization data requirements defined in PCI DSS Requirement 3.2
- compliant to PAN display requirements defined in PCI DSS Requirement 3.3
- compliant to PAN protection requirements defined in PCI DSS Requirement 3.4: this specific requirement compliance is achieved via “SECURE PCI”, a TAS owned platform independent tool which segregates and protects PAN data via encryption, generates a token to replace the PAN within the organization’s PCI DSS scope and thus limits overall IT compliance impacts
- aligned with encryption key management requirements defined in PCI DSS Requirements 3.5 and 3.6: these specific compliance requirements are achieved via TAS Key Management products
- facilitates renewal of data protection keys and the related migration phases, necessary to translate the encrypted data elements from the previous protection key to the latest one
- aligned with audit trails tracking ad defined in PCI DSS Requirement 10.3.

TAS is also available to support on PCI DSS requirements by providing professional consulting services to guide your organization to reach and maintain PCI DSS compliance.

Disclaimer

This document is a brief explanation about PCI DSS to assist your organization in compliance efforts and should be treated as a guide only. There is no guarantee that you will be compliant by simply following these recommendations. You should seek professional advice to assess your organization's specific situation and determine exactly what needs to be done to achieve compliance. Your status in regards to PCI DSS compliance will ultimately be determined by your QSA.

About TAS

TAS Group is the strategic partner for the business innovation of payments, cards and securities for Financial Industry Players operating on a Pan-European or Global landscape.
With over 20 years of experience, TAS Group offers leading technology solutions including applications, project implementation, consultancy and ICT services to develop and optimize customers' procedures and infrastructures.
Listed on the Italian Stock Exchange, TAS Group operates globally and creates value for a long-term relationship, listening to customer needs and providing innovative, cost-effective, quality solutions.
For more information visit us at **www.tasgroup.eu**

Copyright @ 2013 TAS SpA - All Rights Reserved