DataKeep™

SecurityFirst™ Protecting Critical Data

Compliance Bulletin

PCI DSS and the Value of DataKeep

Payment Card Industry Data Security Standard (PCI DSS)
PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. PCI DSS applies to all entities involved in payment card processing—including merchants, processors, acquirers, issuers, and service providers. PCI DSS provides a baseline of technical and operational requirements designed to protect account data.

PCI Data Security Standard – High Level Overview

Section	Requirement Description
Build and Maintain a Secure Network and Systems	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. Protect all systems against malware 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. Identify and authenticate access to system components
	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.

Figure 1 – Requirements List

PCI DSS Applicability Information

PCI DSS also applies to all entities that store, process or transmit cardholder data and/or sensitive authentication data. If cardholder name, service code, and/or expiration date are stored, processed or transmitted with the PAN, or are otherwise present in the cardholder data environment (CDE), only the PAN must be rendered unreadable according to PCI DSS Requirement 3.4. Sensitive authentication data must not be stored after authorization, even if encrypted, except under specified circumstances per PCI DSS Requirement 3.2. Cardholder data and sensitive authentication data are defined as follows in Figure 2.

Cardholder Data includes:	Sensitive Authentication Data includes:
Primary Account Number (PAN) Cardholder Name Expiration Date Service Codes	Full track data (magnetic-strip or chip) CAV2/CVC2/CVV2/CID PINs/PIN blocks

Fig. 2 – Types of Account Data

Scope of PCI DSS Requirements

The PCI DSS security requirements apply to all system components included in or connected to the CDE. The CDE is comprised of people, processes and technologies that store, process, or transmit cardholder data or sensitive authentication data. “System components” include network devices, servers, computing devices, and applications.

Best Practices for Implementing PCI DSS

To ensure security controls continue to be properly implemented, PCI DSS should be implemented into business-as-usual activities as part of an entity’s overall security strategy. This enables an entity to monitor the effectiveness of their security controls on an ongoing basis and maintain their PCI DSS compliant environment in between PCI DSS assessments. Examples of how to incorporate PCI DSS include but are not limited to:

- Monitoring of security controls to ensure they are operating effectively and as intended.
- Ensuring that all failures in security controls are detected and responded to in a timely manner.
- Reviewing changes to the environment prior to completion of the change.
- Changes to organizational structure (for example, a company merger or acquisition) resulting in formal review of the impact to PCI DSS scope and requirements.
- Performing periodic reviews and communications to confirm that PCI DSS requirements continue to be in place and personnel are following secure processes.
- Reviewing hardware and software technologies at least annually to confirm that they continue to be supported by the vendor and can meet the entity’s security requirements.

In addition to the above practices, organizations may also wish to consider implementing separation of duties for their security functions so that security and/or audit functions are separated from operational functions. In environments where one individual performs multiple roles (for example, administration and security operations), duties may be assigned such that no single individual has end-to-end control of a process without an independent checkpoint.

Detailed PCI DSS Requirements and Security Assessment Procedures

PCI DSS Requirements break down into twelve (12) distinct tasks or functions as outlined in Figure 1. There are numerous, very specific subsections under each requirement, that define what must be done to protect payment card related data. Many of them are outside the scope of what a data-centric security solution can impact, so the focus herein is on the specific Requirements related to data protection, primarily Requirements 3, 7 and 10. An organization’s answer to PCI compliance will most likely be comprised of documented processes, multiple software products and services that may include professional consulting.

This overview presents areas where DataKeep by SecurityFirst can help support certain requirements of the Payment Card Industry, Data Security Standard.

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.

PCI DSS REQUIREMENTS

3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes

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.

3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)

- One-way hashes based on strong cryptography
- Truncation
- Index tokens and pads (pads must be securely stored)
- Strong cryptography with associated key-management processes and procedures.

HOW DATAKEEP SUPPORTS REQUIREMENT 3

For issuers and/or companies that support issuing services and store sensitive authentication data, DataKeep assures confidentiality, data privacy and protection against brute force attacks. The SPxCore™ technology combines cryptographic splitting with AES-256 certified encryption and internal key management certified to be FIPS 140-2 compliant. DataKeep also takes full advantage of the AES-NI hardware acceleration available in most current processors for optimal performance.

With transparent, built-in key management capabilities, all phases of key lifecycle stay in your control. Automated key creation, rotation, and revocation/shred conform to industry compliance requirements. When data is no longer required, the customer can revoke the encryption key from the DataKeep system, leaving the data encrypted wherever it is stored, without the key ever being available again for decryption.

PCI DSS REQUIREMENTS

3.5 Document and implement procedures to protect keys used to secure stored cardholder data

3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.

3.5.3 Store secret and private keys used to encrypt/decrypt cardholder data in one (or more) of the following forms at all times:

- Encrypted with a KEK at least as strong as the DEK, and stored separately from the DEK
- Within a secure cryptographic device
- At least two full-length key components or key shares, in accordance with an industry-accepted method

3.5.4 Store cryptographic keys in the fewest possible locations.

HOW DATAKEEP SUPPORTS REQUIREMENT 3

The strength of all DataKeep keys is symmetric 256 bits, with each being randomly generated via a certified, random key generation module.

DataKeep agents create Data Encryption Keys (DEK). A volume agent will use a single set of keys for all data within the defined volume or partition, whereas a file agent will create a unique set of keys for each directory specified in an associated policy.

The Policy Encryption Key (PEK) is used to determine policy enforcement, as well as protect the underlying key structure as the key encryption key via wrapping the volume and file DEKs.

The Key Wrapping Key (KWK) is an externally generated and stored encryption key used whenever an external hardware key store is specified. It encrypts the PEKs. and allows the customer to both specify and control this highest-level key.

PCI DSS REQUIREMENTS

3.6 Fully document and implement all key- management processes and procedures for cryptographic keys used for encryption of cardholder data.
3.6.1 Generation of strong cryptographic keys
3.6.2 Secure cryptographic key distribution
3.6.3 Secure cryptographic key storage
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod as defined by the associated application vendor or key owner, and based on industry best practices and guidelines
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened or keys are suspected of being compromised.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.

HOW DATAKEEP SUPPORTS REQUIREMENT 3

For key generation, DataKeep relies on random system heuristics and FIPS-certified algorithms to generate symmetric 256 bit keys for each of the protection steps.

Key rotation operations are acted upon at the PEK layer where access controls are enforced. As a result, only the PEK is quickly rotated using just the header while keeping the data encrypted throughout the process.

Key shredding is similar to key rotation but deletes the key in PPM and forces a reboot of the agent, effectively crypto-shredding the data.

Within DataKeep, keys are stored in two locations for internal use and protection. Firstly, because the PEK is aligned with policy and access controls, it is stored in the Central Console database. As required, PEKs are securely sent to each agent, but they do not persist.

Secondly, the data encryption keys are stored in the header of the volume or file respectively dependent on the agent type.

When an optional KMIP compatible external key store is configured, the PPM supports the KMIP standard. In this case, the external device is used as a key store to replace the internal key store.

When a hardware key store is used, an externally generated and managed key (the KWK) is used to wrap the PEKs before they are stored in the PPM database.

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.

PCI DSS REQUIREMENTS

7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.

7.1.1 Define access needs for each role, including:

- System components and data resources that each role needs to access for their job function
- Level of privilege required for accessing resources.

7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.

7.2 Establish access control system(s) that restrict access based on a user's need to know and is set to "deny all" unless specifically allowed.

HOW DATAKEEP SUPPORTS REQUIREMENT 7

DataKeep provides the ability for customers to implement role-based access control, privileged access management and separation of security vs. administrative duties to prevent any one person or service provider from having complete system control.

Working with your existing directory services, Role-based access controls allow an administrator to define a second layer of data access control policies used to specify which filesystem functions (read, write, etc.), are authorized. Using a Least Privileged Access (LPA) approach, DataKeep automatically denies access to all users unless they have been specifically granted permissions.

In addition, Privileged Access Management restrictions can be enforced to prevent system administrators and root users from seeing clear text data.

By default, DataKeep creates two distinct roles – Product and Security Administrators. The Product Administrator role deploys the software and monitors the general health of the DataKeep system and all deployed agents. This role has no visibility into policy definitions, agent configurations, deployments or policy logs. The Security Administrator role determines and approves data access rights, manages keys, defines policies, sets logging parameters, and creates the multi-security administrator approval process.

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.

PCI DSS REQUIREMENTS

10.1 Implement audit trails to link all access to system components to each individual user.
10.2 Implement automated audit trails for all system components to reconstruct the following events:
10.2.1 All individual user accesses to cardholder data
10.2.2 All actions taken by any individual with root or administrative privileges
10.3 Record at least the following audit trail entries for all system components for each event:
10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource.
10.5 Secure audit trails so they cannot be altered.
10.5.1 Limit viewing of audit trails to those with a job-related need.
10.5.2 Protect audit trail files from unauthorized modifications.
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4 Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.

HOW DATAKEEP SUPPORTS REQUIREMENT 10

DataKeep provides the ability for customers to implement data access policies that protect encrypted data from unauthorized access, use or other malicious acts. In addition, it allows customers the flexibility to log data access events, whether permitted or denied for detection of potential harmful events.

These events are logged in real-time and can be exported to Security Information & Event Management (SIEM) systems for auditing and alerts. DataKeep supports several standard output formats such as Log Event Extended Format (LEEF), Common Event Format (CEF) and Cloud Auditing Data Federation (CADF) for easy integration.
This combination of DataKeep and SIEM products can make it possible to shorten the detection cycle, reducing the risk of data compromise.

When it comes to the account data itself, DataKeep by SecurityFirst addresses several key data security requirements in PCI DSS and helps payment card organizations ensure their data is protected and private in alignment with the regulation.

SecurityFirst™ delivers advanced security solutions that build a firewall around your data to protect against ever increasing threats and to aid in meeting regulatory requirements such as GDPR, HIPAA, NYCRR and many others. Our flagship product, **DataKeep™**, serves as your data firewall by using advanced encryption, scalable hierarchical key management, extensive policy enforcement and monitoring of unauthorized access to deliver the highest levels of availability, resiliency and time to value. Security requires a layered approach and protection of the data itself is your last line of defense.

SecurityFirst™
Protecting Critical Data

For a product demonstration or more information contact:
sales@securityfirstcorp.com
888-884-7152
securityfirstcorp.com