PCI DSS Requirements Checklist – General Data Protection

How EncryptRIGHT Helps Reduce PCI DSS Audit Scope and Facilitates Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive framework that defines requirements for security management policies, procedures, network architecture, software design, and other critical safeguards to protect cardholder data. While the standard was designed for bank card information security, the recommendations apply to general data protection needs. Any organization that stores or processes confidential data – and that includes just about everyone in the payments space – can use the PCI security requirements as a guide to establish their data protection policies and procedures.

The latest release (PCI DSS 4.0.01) establishes new mandates, making previously recommended best practices for data protection, required items needed to achieve compliance. The latest framework now mandates robust protection of cardholder data not only in storage, but also in transit and in use, along with new guidance on crypto-agility to ensure that organizations can adapt cryptographic methods as threats and standards evolve.

PCI DSS establishes 12 broad security requirements ranging from installation and maintenance of network security controls to documented reviews of cryptographic ciphers and protocols to ensure outdated or weak methods are identified and replaced. Of the 12 PCI DSS security requirements, seven address data protection, access controls, key management, and crypto-agility.

EncryptRIGHT helps organizations that store, process, or transmit sensitive cardholder data simplify their data security and comply and / or reduce the scope of each of the seven requirements (**in bold below**):

1. Install and maintain network security controls.
2. **Apply secure configurations to all system components.**
3. **Protect stored account data.**
4. **Protect cardholder data with strong cryptography during transmission over open, public networks.**
5. Protect all systems and networks against malicious software.
6. Develop and maintain secure systems and software.
7. **Restrict access to system components and cardholder data by business need-to-know.**
8. **Identify users and authenticate access to system components.**
9. Restrict physical access to cardholder data.
10. **Log and monitor all access to system components and cardholder data.**
11. Test security of systems and networks regularly.
12. **Support information security with organizational policies and programs.**

EncryptRIGHT delivers the broad security techniques needed to protect and control access to sensitive cardholder data in storage, in transit, and in use. It is built on a crypto-agile architecture that abstracts data protection from the applications that create, process, and store cardholder data, enabling organizations to adapt seamlessly to evolving regulatory demands and future PCI DSS changes. EncryptRIGHT reduces development costs, minimizes complexity, and simplifies updating security to comply with PCI DSS 4.0.1 and beyond.

The following outline breaks down each of the seven requirements into simplified terms and explains how EncryptRIGHT's capabilities address them, covering data protection, access controls, key management, and the ability to upgrade or replace cryptographic ciphers.

PCI Requirement #2

Apply Secure Configurations to All System Components.

Requirements	EncryptRIGHT Compliance
2.2.2 Change and use strong passwords whenever vendor default accounts are used.	✓ EncryptRIGHT does not have a default User ID or password. On installation a user ID and password must be created and given administrative rights before installation can continue.
2.2.5 Document and implement additional security features that reduce the risk of using insecure services, protocols, or daemons.	✓ EncryptRIGHT provides strong cryptography and key management to protect your data. This includes strong hashing (SHA 2 and SHA 3 256/384/512) and encryption (Triple DES 2/3 key, and AES 128/192/256).
2.2.7 Encrypt all non-console administrative access using strong cryptography.	✓ EncryptRIGHT encrypts all sensitive information (user IDs, passwords, names, descriptions, key material) using the cryptographic algorithms outlined above.

PCI Requirement #3

Protect stored account data.

Requirements	EncryptRIGHT Compliance
3.3.3 Limit storage of authentication data to that needed for legitimate business needs and secure using strong cryptography.	✓ EncryptRIGHT provides strong cryptography and key management to protect your data. This includes strong hashing (SHA-2 and SHA-3 256/384 /512) and encryption (Triple DES 2/3 key, and AES 128/192/256).
3.4.1 Mask portions of the primary account number (PAN) when displayed such that only personnel with legitimate business need can see complete number.	✓ EncryptRIGHT provides dynamic masking to uniquely obscure any parts of sensitive data in accordance with individual privilege that user has to access and unsecure the data. ✓ EncryptRIGHT also provides the capability to define a group of users that only have rights to view a masked portion of a data field. This includes applications that decrypt the data, the EncryptRIGHT audit log, and EncryptRIGHT trace files.
3.5.1 Render PAN unreadable anywhere it is stored using one-way hashing, truncation, or index tokens with strong cryptography and associated key management. **3.5.1.1** Hashes used to render PAN unreadable are keyed cryptographic hashes of the entire PAN, with associated key-management. Cryptographic keys used to protect stored account data are secured across their lifecycle. **3.5.1.2** Disk or partition encryption alone cannot be the only mechanism used to protect PAN.	✓ EncryptRIGHT delivers strong hashing using SHA-2 or SHA-3. Public keys can be up to 4096 bits. ✓ EncryptRIGHT requires a user ID and password for all users. Each user is assigned to one (or more) groups. Each group is assigned the types of access within the EncryptRIGHT administration application. This includes the ability to view or maintain keys and other information. In addition, EncryptRIGHT allows you to require a quorum of logged on users for administration functions. ✓ EncryptRIGHT, when used with an HSM, will store the key encryption key (KEK) used to encrypt keys stored within the EncryptRIGHT database within the hardware module. Keys may optionally be stored on the server and fetched when needed by Client computers. ✓ EncryptRIGHT delivers a broad-spectrum data protection capabilities beyond encryption to protect PAN and reduce audit scope.
3.7.1 Key management includes the generation of strong cryptographic keys used to protect stored account data.	✓ EncryptRIGHT supports Triple DES 2/3 keys. AES 128, 192 and 256. RSA public keys from 1024 to 4096 bits. When used with an HSM, EncryptRIGHT will generate and store robust hardware keys within the cryptographic module.
3.7.2 Secure the distribution of cryptographic keys used to protect stored account data.	✓ Secure key distribution is provided in EncryptRIGHT when the client/server option is licensed. This provides for a Primary Server where keys are maintained, and one or more Client connected through a TCP/IP network. Each Client computer is registered to the Primary Server that automatically distributes key changes to the Clients. All key distributions are double encrypted during transmission, once using an EncryptRIGHT Client key, and once using TLS.
3.6. Secure the cryptographic keys used to protect stored account data.	✓ EncryptRIGHT hashes and encrypts all records within the EncryptRIGHT security database using a randomly generated local master key (LMK). The LMK is protected by the software license which is restricted to licensed computers only. Additionally, if an HSM is in use by EncryptRIGHT, the LMK is encrypted using a hardware-based KEK.
3.7.5 Retire, replace, or destroy keys used to protect stored account data when: • Key reaches end of cryptoperiod.	✓ EncryptRIGHT allows you to change key values manually or automatically. Automatic key changes can be set to occur on a flexible schedule from 1-99 days, weeks, months, quarters, or

Requirements	EncryptRIGHT Compliance
• Key integrity has been weakened. • Key is suspected or known to be compromised.	years.
3.6.5 Retire, replace, or revoke keys when its integrity may have weakened due to an employee departure or suspected compromise.	✓ EncryptRIGHT allows you to designate when a key can be destroyed. The choices are never (for long term data storage), on expiration, or expiration plus 1 to 99 days, weeks, months, quarters, or years. ✓ Any key that is compromised or invalid can be marked as revoked. A new value can be easily created. Every production key value is assigned a unique key version number. When a specific key value is marked as revoked or is otherwise superseded, a new version is created. Both keys still exist in the database, so if an application attempts to use a revoked key, they will receive an indication that the key is revoked.
3.7.1 Generate strong cryptographic keys used to protect stored account data. 3.7.2 Securely distribute cryptographic keys used to protect stored account data. 3.7.3 Securely store cryptographic keys used to protect account data in storage. 3.7.6 Implement split knowledge and dual controls when key management operations are performed.	✓ EncryptRIGHT provides the ability for up to three different people to enter key components. Additionally, you can require that the components be entered by different users. You also have the ability to require a quorum of users to be logged on. For example, you can require that two people with rights for key management be logged on at the same time to enter a key component, where one person enters the key and the other observes. ✓ EncryptRIGHT encrypts all sensitive information (user IDs, passwords, names, descriptions, key material). In addition, data in shared memory is authenticated using the database LMK to detect unauthorized changes.
3.7.7 Key management policies and procedures are implemented to prevent unauthorized substitution of cryptographic keys.	✓ Key values cannot be substituted by unauthorized users. Every user is assigned a unique ID and password, and EncryptRIGHT securely logs every key change. When a key is selected for use, its check value is validated before using the key to secure or unsecure data.

PCI Requirement #4

Protect cardholder data with strong cryptography during transmission over open, public networks.

Requirements	EncryptRIGHT Compliance
4.2.1 Implement strong cryptography and security protocols to safeguard PAN during transmission over open, public networks: • Only trusted keys and certificates are accepted. • Certificates used to safeguard PAN during transmission over open, public networks are confirmed as valid and are not expired or revoked. • The protocol in use supports only secure versions or configurations and does not support fallback to, or use of insecure versions, algorithms, key sizes, or implementations. • The encryption strength is appropriate for the encryption methodology in use.	✓ EncryptRIGHT delivers a broad spectrum of security techniques to protect PANs in storage, in transit, and in use. Symmetric algorithms including 3DES and AES 256 are used to encrypt and tokenize PANs and TLS 1.3 to secure all connections between EncryptRIGHT instances. (Primary, Redundant, and Expansion Servers and Clients). ✓ For secure synchronization of keys, user information, and data protection policies, additional encryption is employed at the field level (such as key material and passwords). TLS 1.3 is also used to secure the browser sessions used with EncryptRIGHT's administration application. ✓ For secure protection of user interface selections, each session has a unique number and session key. This key is used to encrypt the HTML selection field to tie each to specific user, session, and item being maintained. ✓ EncryptRIGHT's crypto-agile architecture allows you to migrate to new, stronger algorithms and seamlessly adapt to changing

	threats and evolving regulatory requirements.

PCI Requirement #7

Restrict access to system components and cardholder data by business need to know.

EncryptRIGHT provides the ability to define the level of data access for each user. Access can be specified at the record and/or data field level. The type of access that can be defined is no access, masked access (specifying the mask character, the position and length of the clear data), read only, or read/write. By default, no one is allowed access when creating record definitions. In order to use a definition, you must provide access definitions.

Requirements	EncryptRIGHT Compliance
7.3.3 Set access control system to "deny all" by default.	✓ At the moment when EncryptRIGHT is first installed using the web-based administration application, access is restricted to the first IP address used. From there, you may expand access as needed. ✓ EncryptRIGHT enables the user making the installation to define the first administrative user ID and password for the installation. Access from the web-based administration application is initially restricted to only the installation directory and the temp directory on the host computer. Additional directories may be added.

PCI Requirement #8

Identify users and authenticate access to system components.

Requirements	EncryptRIGHT Compliance
8. Identify users and authenticate access to system components.	✓ EncryptRIGHT can optionally require a user ID and password for API use. This means that, for an application to use EncryptRIGHT to protect any data, a user ID and password must be given to the library for verification. With this, EncryptRIGHT fetches the access rights for the user., and when a data record definition is used to encrypt or decrypt data, the user's access rights are checked to determine if they can decrypt, and if so, do they only see a masked version of the data or if they can view and update the data.
8.2.1 Assign all users a unique ID before access to system components or cardholder data is allowed.	✓ EncryptRIGHT allows all users to have a unique User ID and password. This is used not only for access to the EncryptRIGHT database, but also for access to cryptography for your defined user data records and fields.
8.2.4 Addition, deletion, and modification of user IDs, authentication factors, and other identifier objects are managed as follows: • Authorized with the appropriate approval. • Implemented with only the privileges specified in the documented approval.	✓ EncryptRIGHT only allows administrators to add, delete, and change users. In addition, this can be further controlled by requiring a quorum of logged on users, so no single individual can maintain user information without supervision.

Requirements	EncryptRIGHT Compliance
8.2.5 Immediately revoke access for terminated users. **8.2.6** Remove or disable inactive user accounts within 90 days of inactivity.	✓ Users can be temporarily disabled or entirely deleted by user administrators at any time.
8.2.8 If a user session has been idle for more than 15 minutes, the user is required to re-authenticate to re-activate the terminal or session.	✓ EncryptRIGHT allows you to set the automatic timeout period for the web-based administration application. The default is 15 minutes.
8.3.1 Authenticate user access to system components for all users and administrators via at least one of the following authentication factors: • Something you know (password or passphrase). • Something you have (token device or smart card). • Something you are (biometric element). **8.3.2** Use strong cryptography to render all authentication factors unreadable during transmission and storage on all system components. **8.3.3** Verified user ID before modifying any authentication factors. **8.3.4** Invalid authentication attempts are limited by: locking out user ID after not more than 10 attempts; setting the lockout duration to a minimum of 30 minutes or until the user's identity is confirmed. **8.3.5** Passwords/passphrases used as authentication factors must be set and reset for each user as follows: • Set to unique value for first-time use and upon reset. • Forced to be changed immediately after the first use. **8.3.6** Passwords/passphrases used as authentication factors must meet the following minimum level of complexity: • A minimum length of 12 characters (or IF the system does not support 12 characters; a minimum length of eight characters). • Contain both numeric and alphabetic characters. **8.3.7** Do not allowed individuals to submit a new password/passphrase that is the same as any of the last four passwords/passphrases used. **8.3.9 and 8.3.10.1** Change passwords/passphrases at least once every 90 days.	✓ EncryptRIGHT provides a password policy that can specify: • Maximum and minimum password age. • Minimum password length (default is 7 characters). • Password uniqueness. This includes how many passwords to remember, the maximum characters that can be repeated from the previous password, and a password dictionary. • Required special characters, upper/lower case and numbers (default is both numeric and alphabetic characters). • Bad attempts lockout count, and the duration of the lockout (default is 6 attempts, 30-minute lockout, and 30 minutes to reset). ✓ Passwords are stored self-encrypted. This means that they are encrypted using a key derived from the password itself. These passwords cannot be decrypted. The only way to verify a password is to enter the same password, which is encrypted and then compared to the original encrypted password. ✓ Passwords can only be changed by a user if the user also enters the current password. ✓ EncryptRIGHT defaults to forcing the user to change their password anytime an administrator sets or changes a user's password.
8.4.3 MFA is implemented for all remote access originating from outside the entity's network that could access or impact the cardholder data environment.	✓ EncryptRIGHT allows you to use two-factor authentication applications supporting time-based one-time passwords (TBOTPs) and HMAC-based one-time passwords (HOTP), such as Google Authenticator.

PCI Requirement #10

Log and monitor all access to systems and networks regularly.

Requirements	EncryptRIGHT Compliance
10.2.1 Audit logs are enabled and active for all system components and cardholder data.	✓ EncryptRIGHT provides the ability to create secure audit log entries for: • Access to data down to the field level. • Invalid access attempts. • All changes made to definitions within EncryptRIGHT. • User logons and logoffs (optional).
10.2.1.1 Capture all individual user access to cardholder data in audit log.	✓ EncryptRIGHT allows all users to have a unique User ID and password.
10.2.2 Record following details in audit logs for each auditable event: • User identification. • Type of event. • Date and time. • Success and failure. • Origination of event. • Identity or name of affected data.	✓ EncryptRIGHT audit log contains the User ID, the type of message, date and time, the EncryptRIGHT subsystem name and the success or failure message.
10.3.2 Protect audit log files to prevent modifications.	✓ EncryptRIGHT audit log is secure. Each entry contains a sequence number, and the entire entry is hashed and encrypted. When viewing the log, each entry hash and sequence number is verified. The ability to view the audit log can be assigned to groups of users.

PCI Requirement #12

Support information security with organizational policies and programs.

Requirements	EncryptRIGHT Compliance
12.3.3 Document and regularly review all cryptographic ciphers and protocols being used to ensure outdated or weak methods are identified and replaced to strength overall security. (Became mandatory after March 31, 2025)	✓ EncryptRIGHT's crypto-agile architecture enables you to quickly update, replace, or retire cryptographic algorithms to ensure effective response to evolving threats. Crypto-agility addresses advancements in computing technology, as well as any security, regulatory, or business demand requiring a change in how data is protected. An agile and flexible architecture is critical to stay secure and compliant, enabling you to swap out algorithms without rewriting applications.
12.10.5 The security incident response plan includes monitoring and responding to alerts from security monitoring systems.	✓ EncryptRIGHT may be configured to provide automatic notifications for various events. These notifications are via a script the customer writes, which may include sending an e-mail or SMS message. Events include: • Bad password attempts (configurable threshold). • Client update synchronization errors. • EncryptRIGHT database scan errors. • Report of keys about to expire. • EncryptRIGHT API function errors (in customer applications). • A system heartbeat message • User defined notifications via an API call.