PrimeFactors™
APPLIED DATA PROTECTION

PCI Requirements Checklist – Issuance & Processing

How BCSS Helps with PCI Data Security Compliance

The Payment Card Industry (PCI) Data Security Standard (DSS) is a comprehensive security standard that includes requirements for security management policies, procedures, network architecture, software design, and other critical protective measures. Every organization which stores or processes confidential data — and that includes just about everyone in the payments space — could use the PCI security requirements as a guide to establish their data protection policies and procedures.

BCSS helps comply with DSS in the area of cryptography and key management. There are twelve security requirements outlined by PCI DSS (listed below). Six of these requirements specifically address encryption and key management, and BCSS helps to address five of them – DSS security requirements numbers 2, 3, 4, 8, and 10 (**in bold below**). The other requirements of PCI DSS are related to policies, procedures, and network architecture.

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.**
3. **Protect stored cardholder data.**
4. **Encrypt transmission of cardholder data across open, public networks.**
5. Protect all systems against malware and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
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.
10. **Track and monitor all access to network resources and cardholder data.**
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security for all personnel.

The following is a requirement-by-requirement overview of how BCSS helps to specifically address PCI DSS compliance:

PCI Requirement #2

Do not use vendor-supplied defaults for system passwords and other security parameters.

BCSS 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.

PCI Requirement #3

Protect stored cardholder data.

BCSS complies with this requirement in each of the following specifics:

Requirements	BCSS Compliance
3.3 Mask PAN when displayed.	PANs are not recorded in logs and are masked when they appear in diagnostic trace files.

Requirements	BCSS Compliance
3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	BCSS requires a User ID and password for all users. Each user is assigned to one (or more) groups. Each group is assigned access privileges within the BCSS administration application, including the ability to view or maintain keys and other information. BCSS optionally enforces a quorum of logged on users for any administration function and dual sign-on specifically for key management.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data. 3.6.1 Generate strong cryptographic keys.	BCSS supports 3DES 2-key and 3DES 3-key, as well as AES 128, 192 and 256 algorithms.
3.6.2 Secure cryptographic key distribution.	BCSS supports 3DES as well as the use of cryptographic key blocks (AES and TR-31) for the secure exchange of keys.
3.6.3 Secure cryptographic key storage.	When used in conjunction with a payShield HSM, keys in the BCSS database are encrypted using a local master key (LMK) of that HSM. In addition, the BCSS database is protected by the LMK of the BCSS software which restricts access to licensed computers only.
3.6.4 Periodic cryptographic key changes.	BCSS allows you to change key values manually and to optionally generate future keys with specific validity date ranges.
3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys.	BCSS allows you to mark a key as revoked so that applications will not attempt to use the key but will instead return a nonzero response code indicating that the key has been revoked.
3.6.6 Split knowledge and establishment of dual control of keys (so that it requires two or three people, each knowing only their part of the key, to reconstruct the whole key).	BCSS provides the ability to require up to nine different users to enter key components. You also have the ability to require a quorum of users to be logged on and the ability to enforce concurrent dual sign-on during component or key entry, where one person enters the component or key while the other person observes.
3.6.7 Prevent unauthorized substitution of cryptographic keys.	Key values cannot be substituted by unauthorized people. Every user should be assigned a unique User ID and password. Every key change is logged in the BCSS secure audit log

PCI Requirement #4

Encrypt transmission of cardholder data across open, public networks.

Although this requirement talks about using SSL and TLS security over networks, BCSS does help you consistently encrypt sensitive data for transport across public networks by supporting PIN block generation and translation.

BCSS supports ten different PIN Block formats for standard PIN transport needs and chip card processing.

PCI Requirement #8

Assign a unique ID to each person with computer access.

BCSS helps you comply with this requirement in each of the following specifics:

Requirements	BCSS Compliance
8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	BCSS allows for all users to have a unique User ID and password. This is used not only for access to the BCSS database, but also for access to cryptography for your defined user data records and fields.
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	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.
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	Only user administrators can add, delete and change users. In addition this can be further controlled by requiring a quorum of logged on users so no single person can maintain user information without supervision.
8.5.2 Verify user identity before performing password resets.	Passwords can only be changed by a user if the user also enters the current password.
8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.	BCSS defaults to forcing the user to change their password anytime an administrator sets or changes a user's password.
8.5.4 Immediately revoke access for any terminated users. 8.5.5 Remove/disable inactive user accounts at least every 90 days. 8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.	Users can be temporarily disabled or entirely deleted by user administrators at any time.
8.5.9 Change user passwords at least every 90 days. 8.5.10 Require a minimum password length of at least seven characters. 8.5.11 Use passwords containing both numeric and alphabetic characters. 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used. 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.5.14 Set the lockout duration to 30 minutes or until administrator enables the user ID.	BCSS provides a password policy that can specify the following: • Maximum and minimum password age. • Minimum password length. • 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. • Bad attempts lockout count, and the duration of the lockout.
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.	BCSS does not access any database, and API use can require user authentication. This means that in order for an application to use the BCSS, a User ID and password has to be given to the library for verification. With this, BCSS fetches the access rights the user has.

PCI Requirement #10

Track and monitor all access to network resources and cardholder data.

BCSS helps you comply with this requirement in each of the following specifics:

Requirements	BCSS Compliance
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	BCSS allows for all users to have a unique User ID and password.
10.2 Implement automated audit trails for all system components to reconstruct the following events.	An audit log entry is made for Invalid access attempts and for all changes made to definitions within BCSS.
10.3 Record at least the following audit trail entries for all system components for each event.	The BCSS audit log contains the User ID, the type of message, date and time, the workstation name, and the name of the affected data or key.
10.5 Secure audit trails so they cannot be altered.	The BCSS audit log is secure. Each entry is hashed and encrypted. The ability to view the audit log can be assigned to groups of users.