Policy Pack Cross Reference to PCI DSS 3.2

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

PCI DSS Requirements	Policy Pack Reference
1.1 Establish and implement firewall and router configuration standards that include the following:	**P05 - Operational Policy.**
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	**P05 - Operational Policy.** Section 5.3.6.5 Adding/Modifying Router Configuration and Firewall Rules.
1.1.2 Current network diagram that identifies all connections between the cardholder data environment and other networks, including any wireless networks	**P05 - Operational Policy.** Section 5.3.7. Network and Data Flow Diagrams.
1.1.3 Current diagram that shows all cardholder data flows across systems and networks	**P05 - Operational Policy.** Section 5.3.7. Network and Data Flow Diagrams.
1.1.4 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone	**P05 - Operational Policy.** Section 5.3.6.1 Firewall and Router Configuration Standards. Section 5.3.6.2 De-militarised Zone Separation. Section 5.3.6.3 Card Holder Data De-militarised Zone. Section 5.3.6.4 Internal Network Separation.
1.1.5 Description of groups, roles, and responsibilities for management of network components	**P05 - Operational Policy.** Section 5.3.6.1 Firewall and Router Configuration Standards.
1.1.6 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	**P05 - Operational Policy.** Section 5.3.6.6 Firewall Rule Justification.
1.1.7 Requirement to review firewall and router rule sets at least every six months	**P05 - Operational Policy.** Section 5.3.6.7 - Review of Rules. **PR07 - Firewall & Router Security Review Procedure** Section 4.2 - Firewall Configuration.
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	**P05 - Operational Policy.** Section 5.3.6, Firewalls.
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic.	
1.2.2 Secure and synchronize router configuration files.	
1.2.3 Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment.	
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment**.**	**P05 - Operational Policy.** Section 5.3.6.3 Cardholder Data De-Militarised Zone Separation.

PCI DSS Requirements	Policy Pack Reference
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	
1.3.3 Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network. (For example, block traffic originating from the Internet with an internal source address.)	
1.3.4 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	
1.3.5 Permit only "established" connections into the network.	**P05 - Operational Policy.** Section 5.3.6.1 Firewall and Router Configuration Standards.
1.3.6 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	**P05 - Operational Policy.** Section 5.3.6.3 Cardholder Data De-Militarised Zone Separation.
1.3.7 Do not disclose private IP addresses and routing information to unauthorized parties.	**P05 - Operational Policy.** Section 5.3.6.4 Internal Network Separation.
1.4 Install personal firewall software or equivalent functionality on any portable computing devices (including company and/or employee/owned) that connect to the Internet when outside the network (for example, laptops used by employees), and which are also used to access the CDE. Firewall (or equivalent) configurations include: Specific configuration settings are defined. Personal firewall (or equivalent functionality) is actively running. Personal firewall (or equivalent functionality) is not alterable by users of the portable computing devices.	**P05 - Operational Policy.** Section 5.2, Remote and Non-Physical Access Services.
1.5 Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2, Review and Update of the Policy Statement.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PCI DSS Requirements	Policy Pack Reference
2.1 Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network. This applies to ALL default passwords, including but not limited to those used by operating systems, software that provides security services, application and system accounts, point-of-sale (POS) terminals, payment	**P05 - Operational Policy.** Section 5.3.8 New Equipment/Software Installation.

PCI DSS Requirements	Policy Pack Reference
applications, Simple Network Management Protocol (SNMP) community strings, etc.).	
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	**P04 - Wireless Access Policy.** Section 5.3.2 Security.
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: • Center for Internet Security (CIS) • International Organization for Standardization (ISO) • SysAdmin Audit Network Security (SANS) Institute National Institute of Standards Technology (NIST).	**P05 - Operational Policy.** Section 5.3.4 Hardening Guides. F29 - SSL and TLS mitigation
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	
2.2.2 Enable only necessary services, protocols, daemons, etc., as required for the function of the system.	
2.2.3 Implement additional security features for any required services, protocols, or daemons that are considered to be insecure Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	
2.2.4 Configure system security parameters to prevent misuse.	
2.2.5 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	
2.3 Encrypt all non-console administrative access using strong cryptography. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	**P05 - Operational Policy.** Section 5.3.4 Hardening Guides. F29 - SSL and TLS mitigation
2.4 Maintain an inventory of system components that are in scope for PCI DSS.	**F25 - CDE Component Inventory.**
2.5 Ensure that security policies and operational procedures for managing vendor defaults and other security parameters are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2 Review and Update of the Policy Statement. **P04 - Wireless Access Policy.** Section 2.2 Review and Update of the Policy Statement.

PCI DSS Requirements	Policy Pack Reference
2.6 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in *Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.*	**P05 - Operational Policy.** Section 9 Shared Hosting Provider.

Requirement 3: Protect stored cardholder data

PCI DSS Requirements	Policy Pack Reference
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes that include at least the following for all cardholder data (CHD) storage: • Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements • Processes for secure deletion of data when no longer needed • Specific retention requirements for cardholder data • A quarterly process for identifying and securely deleting stored cardholder data that exceeds defined retention.	**P05 - Operational Policy.** Section 5.6.8 Data Retention & Disposal.
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. It is permissible for issuers and companies that support issuing services to store sensitive authentication data if: • There is a business justification and • The data is stored securely. Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:	P05 - Operational Policy. Section 5.6.6. Data Storage Restrictions.
3.2.1 Do not store the full contents of any track (from the magnetic stripe located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	
3.2.2 Do not store the card verification code or value (three-digit or four-digit number printed on the front or back of a payment card used to verify card-not-present transactions) after authorization.	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block after authorization.	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed), such that only personnel with a legitimate business need can see more than first six/last four digits of the PAN. Note: This requirement does not supersede stricter	**P11 – Systems and Applications Development Policy.** Section 5.2.2 Cardholder Data. **P08 - Information Classification Policy.** Section 5.2 Storage of Cardholder Data.

PCI DSS Requirements	Policy Pack Reference
requirements in place for displays of cardholder data—for example, legal or payment card brand requirements for point-of-sale (POS) receipts.	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: • One-way hashes based on strong cryptography, (hash must be of the entire PAN) • Truncation (hashing cannot be used to replace the truncated segment of PAN) • Index tokens and pads (pads must be securely stored) • Strong cryptography with associated key-management processes and procedures.	**P11 – Systems and Applications Development Policy.** Section 5.2.2 Cardholder Data. **P08 - Information Classification Policy.** Section 5.2 Storage of Cardholder Data.
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed separately and independently of native operating system authentication and access control mechanisms (for example, by not using local user account databases or general network login credentials). Decryption keys must not be associated with user accounts. Note: This requirement applies in addition to all other PCI DSS encryption and key management requirements..	**P05 – Operational Policy.** Section 5.6.5 Data Encryption.
3.5 Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse:	**P09 - Key Management Policy.** Section 5.3 Key Usage. Section 5.4.4 Key Encrypting Keys. Section 5.2 Key Storage.
3.5.1 Additional requirement for service providers only: Maintain a documented description of the cryptographic architecture that includes: • Details of all algorithms, protocols, and keys used for the protection of cardholder data, including key strength and expiry date • Description of the key usage for each key. • Inventory of any HSMs and other SCDs used for key management.	**P09 - Key Management Policy.** Section 5.10 Service Providers – Documentation of Cryptographic Architecture
3.5.2 Restrict access to cryptographic keys to the fewest number of custodians necessary.	**P09 - Key Management Policy.** Section 5.3 Key Usage.
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 key-encrypting key that is at least as strong as the data-encrypting key, and that is stored separately from the data-encrypting key • Within a secure cryptographic device (such as a hardware (host) security module (HSM) or PTS-approved point-of-interaction device)	**P09 - Key Management Policy.** Section 5.2 Key Storage.

PCI DSS Requirements	Policy Pack Reference
• As 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.	**P09 - Key Management Policy.** Section 5.2 Key Storage.
3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:	**P09 - Key Management Policy.** Section 5.9. Service Providers Sharing Keys with Customers.
3.6.1 Generation of strong cryptographic keys	**P09 – Key Management Policy.** Section 5.5 Key Strength and Ciphers.
3.6.2 Secure cryptographic key distribution	**P09 – Key Management Policy.** Section 5.6 Key Changes and Distribution.
3.6.3 Secure cryptographic key storage	**P09 – Key Management Policy.** Section 5.2 Key Storage.
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	**P09 – Key Management Policy.** Section 5.6 Key Changes and Distribution.
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 (for example, departure of an employee with knowledge of a clear-text key component), or keys are suspected of being compromised.	**P09 – Key Management Policy.** Section 5.6 Key Changes and Distribution.
3.6.6 If manual clear-text cryptographic key-management operations are used, these operations must be managed using split knowledge and dual control.	**P09 - Key Management Policy.** Section 5.4.1 Split Password.
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	**P09 - Key Management Policy.** Section 5.4 Cryptographic Key Schemes.
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	**P09 - Key Management Policy.** Section 5.3 Key Usage, Form F12 - Key Custodians Form.
3.7 Ensure that security policies and operational procedures for protecting stored cardholder data are documented, in use, and known to all affected parties.	**P09 - Key Management Policy.** Section 2. Review and Update of the Policy Statement.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

PCI DSS Requirements	Policy Pack Reference
4.1 Use strong cryptography and security protocols (for example, TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks, including the following: • Only trusted keys and certificates are accepted.	**P05 - Operational Policy.** Section 5.3.4 Hardening Guides. **P11 – Systems and Application Development Policy**. Section 5.6 Encryption Technologies.

PCI DSS Requirements	Policy Pack Reference
• The protocol in use only supports secure versions or configurations. • The encryption strength is appropriate for the encryption methodology in use. Note: Where SSL/early TLS is used, the requirements in Appendix A2 must be completed.	F29 - SSL and TLS mitigation
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.	**P04 - Wireless Access Policy.** Section 5.2 Approved Systems. **P05 - Operational Policy.** Section 5.3.4 Hardening Guides.
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, SMS, chat, etc.).	**P06 - Acceptable Use Policy.** Section 5.3.2 Internet Access.
4.3 Ensure that security policies and operational procedures for encrypting transmissions of cardholder data are documented, in use, and known to all affected parties.	**P06 - Acceptable Use Policy.** Section 2 -Review and Update of the Policy Statement. **P05 - Operational Policy.** Section 5.3.4 Hardening Guides. **P11 – Systems and Application Development Policy.** Section 5.6 Encryption Technologies.

Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs

PCI DSS Requirements	Policy Pack Reference
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	**P05 - Operational Policy.** Section 5.3.9.3. Anti-Virus & Spyware.
5.1.1 Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	
5.1.2 For systems considered to be not commonly affected by malicious software, perform periodic evaluations to identify and evaluate evolving malware threats in order to confirm whether such systems continue to not require anti-virus software.	
5.2 Ensure that all anti-virus mechanisms are maintained as follows: • Are kept current, • Perform periodic scans • Generate audit logs which are retained per PCI DSS Requirement 10.7.	
5.3 Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized by management on a case-by-case basis for a limited time period.	

PCI DSS Requirements	Policy Pack Reference
5.4 Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2. Review and Update of the Policy Statement. Section 5.3.9.3. Anti-Virus & Spyware.

Requirement 6: Develop and maintain secure systems and applications

PCI DSS Requirements	Policy Pack Reference
6.1 Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking (for example, as "high," "medium," or "low") to newly discovered security vulnerabilities.	**P05 - Operational Policy.** Section 5.3.9.1. Security Monitoring. **PR13 - Risk Ranking Procedure.**
6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release. Note: Critical security patches should be identified according to the risk ranking process defined in Requirement 6.1..	**P05 - Operational Policy.** Section 5.3.9.2. System Updates.
6.3 Develop internal and external software applications (including web-based administrative access to applications) securely, as follows: In accordance with PCI DSS (for example, secure authentication and logging) Based on industry standards and/or best practices. Incorporating information security throughout the software-development life cycle	**P11 - Systems and Application Development Policy.** Section 5.2.3. Industry Best-Practice Development Guidelines. Section 5.7 Software development lifecycle.
6.3.1 Remove development, test and/or custom application accounts, user IDs, and passwords before applications become active or are released to customers.	**P11 - Systems and Application Development Policy.** Section 5.8. Code Migration into Production Environment. Section 5.3 Testing Strategies. **PR05 - Change Control Procedure.** Section 4.2 Completion of the Change Control Form
6.3.2 Review custom code prior to release to production or customers in order to identify any potential coding vulnerability (using either manual or automated processes) to include at least the following: • Code changes are reviewed by individuals other than the originating code author, and by individuals knowledgeable about code-review techniques and secure coding practices. • Code reviews ensure code is developed according to secure coding guidelines • Appropriate corrections are implemented prior to release. • Code-review results are reviewed and approved by management prior to release.	**P11 - Systems and Application Development Policy.** 5.4. Code Reviews & Web Application Firewalls. 5.2.3. Industry Best-Practice Development Guidelines.
6.4 Follow change control processes and procedures for all changes to system components. The processes must	**P05 - Operational Policy.**

PCI DSS Requirements	Policy Pack Reference
include the following:	Section 5.7. Change Control 5.3.9.2. System Updates. **P11 – Systems and Application Development Policy.** Section 5.1.2 Separation of Environments. Section 5.1.1 Separation of Duties. Section 5.8. Code Migration into Production Environment. Section 5.3. Testing Strategies. Section 5.5. Rollout / Rollback Control.
6.4.1 Separate development/test environments from production environments, and enforce the separation with access controls.	**P11 – Systems and Application Development Policy.** Section 5.1.2 Separation of Environments.
6.4.2 Separation of duties between development/test and production environments	**P11 – Systems and Application Development Policy.** Section 5.1.1 Separation of Duties.
6.4.3 Production data (live PANs) are not used for testing or development	**P11 – Systems and Application Development Policy.** Section 5.1.2 Separation of Environments.
6.4.4 Removal of test data and accounts from system components before the system becomes active / goes into production	**P11 – Systems and Application Development Policy.** Section 5.8. Code Migration into Production Environment.
6.4.5 Change control procedures must include the following:	**P05 - Operational Policy.** Section 5.7. Change Control. **PR05 - Change Control Procedure.** Section 4.9 – PCI DSS Review For Significant Changes.
6.4.5.1 Documentation of impact.	
6.4.5.2 Documented change approval by authorized parties.	
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	
6.4.5.4 Back-out procedures.	
6.4.6 Upon completion of a significant change, all relevant PCI DSS requirements must be implemented on all new or changed systems and networks, and documentation updated as applicable.	**PR05 - Change Control Procedure.** Section 4.9 – PCI DSS Review For Significant Changes.
6.5 Address common coding vulnerabilities in software-development processes as follows: • Train developers at least annually in up-to-date secure coding techniques, including how to avoid common coding vulnerabilities. • Develop applications based on secure coding guidelines. Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. • Note: Requirements 6.5.1 through 6.5.6, below, apply to all applications (internal or external):	**P11 - Systems and Application Development Policy.** Section 5.2.3. Industry Best-Practice Development Guidelines. Section 5.7 Software Development Lifecycle. Section 5.3. Testing Strategies.
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XPath	**P11 - Systems and Application Development Policy.**

PCI DSS Requirements	Policy Pack Reference
injection flaws as well as other injection flaws.	Section 5.3. Testing Strategies.
6.5.2 Buffer overflows	
6.5.3 Insecure cryptographic storage	
6.5.4 Insecure communications	
6.5.5 Improper error handling	
6.5.6 All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).	
6.5.7 Cross-site scripting (XSS)	
6.5.8 Improper access control (such as insecure direct object references, failure to restrict URL access, directory traversal, and failure to restrict user access to functions).	
6.5.9 Cross-site request forgery (CSRF)	
6.5.10 Broken authentication and session management	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: • Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes • Installing an automated technical solution that detects and prevents web-based attacks (for example, a web-application firewall) in front of public-facing web applications, to continually check all traffic.	**P11 - Systems and Application Development Policy.** Section 5.4. Code Reviews & Web Application Firewalls.
6.7 Ensure that security policies and operational procedures for developing and maintaining secure systems and applications are documented, in use, and known to all affected parties.	**P11 - Systems and Application Development Policy.** Section 2. Review and Update of the Policy Statement.

Requirement 7: Restrict access to cardholder data by business need to know

PCI DSS Requirements	Policy Pack Reference
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access.	**P05 - Operational Policy.** Section 5.6.3. Roles Access. Section 5.4.1. Issuing of Accounts. Section 5.6.1 Ac;cess to Cardholder Data.
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 example, user, administrator, etc.) for accessing resources.	
7.1.2 Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.	
7.1.3 Assign access based on individual personnel's job classification and function.	
7.1.4 Require documented approval by authorized	

PCI DSS Requirements	Policy Pack Reference
parties specifying required privileges.	
7.2 Establish an access control system for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	**P05 - Operational Policy.** Section 5.6.3. Roles Access. Section 5.4.1. Issuing of Accounts. Section 5.6.1 Access to Cardholder Data.
7.2.1 Coverage of all system components	
7.2.2 Assignment of privileges to individuals based on job classification and function.	
7.2.3 Default "deny-all" setting.	
7.3 Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2. Review and Update of the Policy Statement

Requirement 8: Identify and authenticate access to system components

PCI DSS Requirements	Policy Pack Reference
8.1 Define and implement policies and procedures to ensure proper user identification management for non-consumer users and administrators on all system components as follows:	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
8.1.1 Assign all users a unique ID before allowing them to access system components or cardholder data.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
8.1.2 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
8.1.3 Immediately revoke access for any terminated users.	**P05 - Operational Policy.** Section 5.4.6 Termination/Suspension of Accounts.
8.1.4 Remove/disable inactive user accounts within 90 days.	**P05 - Operational Policy.** Section 5.4.6 Termination/Suspension of Accounts
8.1.5 Manage IDs used by third parties to access, support, or maintain system components via remote access as follows: • Enabled only during the time period needed and disabled when not in use. • Monitored when in use.	**P05 - Operational Policy.** Section 5.4.5 Vendor/Support User Accounts.
8.1.6 Limit repeated access attempts by locking out the user ID after not more than six attempts.	**P05 - Operational Policy.** Section 5.4.4 Password/Session Lockout and Resetting. **P11 - Systems and Applications Development Policy.** Section 5.2.4 Customer (non-consumer) passwords.
8.1.7 Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.	**P05 - Operational Policy.** Section 5.4.4 Password/Session Lockout and Resetting. **P11 - Systems and Applications Development Policy.** Section 5.2.4 Customer (non-consumer) passwords.
8.1.8 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	**P05 – Operational Policy.** Section 5.4.4 Password/Session Lockout and Resetting.

PCI DSS Requirements	Policy Pack Reference
	P11 - Systems and Applications Development Policy. Section 5.2.4 Customer (non-consumer) passwords.
8.2 In addition to assigning a unique ID, ensure proper user-authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: Something you know, such as a password or passphrase Something you have, such as a token device or smart card Something you are, such as a biometric.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
8.2.1 Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.	**P11 – System and Application Development Policy.** Section 5.6 Encryption Technologies.
8.2.2 Verify user identity before modifying any authentication credential—for example, performing password resets, provisioning new tokens, or generating new keys.	**P05 - Operational Policy.** Section 5.4.4 Password/Session Lockout & Resetting.
8.2.3 Passwords/phrases must meet the following: • Require a minimum length of at least seven characters. • Contain both numeric and alphabetic characters. Alternatively, the passwords/phrases must have complexity and strength at least equivalent to the parameters specified above.	**P05 - Operational Policy.** Section 5.4.4 Password/Session Lockout and Resetting. **P11 - Systems and Applications Development Policy.** Section 5.2.4 Customer (non-consumer) passwords.
8.2.4 Change user passwords/passphrases at least once every 90 days.	**P05 - Operational Policy.** Section 5.4.3 Changing/Resetting Passwords. **P11 - Systems and Applications Development Policy.** Section 5.2.4 Customer (non-consumer) passwords.
8.2.5 Do not allow an individual to submit a new password/phrase that is the same as any of the last four passwords/phrases he or she has used.	**P05 - Operational Policy.** Section 5.4.3 Changing/Resetting Passwords. **P11 - Systems and Applications Development Policy.** Section 5.2.4 Customer (non-consumer) passwords.
8.2.6 Set passwords/phrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
8.3 Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication Note: Multi-factor authentication requires that a minimum of two of the three authentication methods (see Requirement 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (for example, using two separate passwords) is not considered multi-factor authentication.	**P05 - Operational Policy.** Section 5.2.1 Remote Access to Services.
8.3.1 Incorporate multi-factor authentication for all non-	**P05 - Operational Policy.**

PCI DSS Requirements	Policy Pack Reference
console access into the CDE for personnel with administrative access. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	Section 5.2.1 Remote Access to Services.
8.3.2 Incorporate multi-factor authentication for all remote network access (both user and administrator, and including third party access for support or maintenance) originating from outside the entity's network.	**P05 - Operational Policy.** Section 5.2.1 Remote Access to Services.
8.4 Document and communicate authentication procedures and policies to all users including: • Guidance on selecting strong authentication credentials • Guidance for how users should protect their authentication credentials • Instructions not to reuse previously used passwords • Instructions to change passwords if there is any suspicion the password could be compromised.	**P01 - Information Security Policy.** Section 5.6.2. Security Training.
8.5 Do not use group, shared, or generic IDs, passwords, or other authentication methods as follows: • Generic user IDs are disabled or removed. • Shared user IDs do not exist for system administration and other critical functions. • Shared and generic user IDs are not used to administer any system components.	**P05 Operational Policy.** 5.3.8. New Equipment / Software Installation, Section 5.4.1 Issuing of Accounts. **P05 - Operational Policy.** Section 5.6.9. Remote Access to Customer CDE (Service Providers only).
8.5.1 ***Additional requirement for service providers only:*** Service providers with remote access to customer premises (for example, for support of POS systems or servers) must use a unique authentication credential (such as a password/phrase) for each customer.	**P05 - Operational Policy.** Section 5.6.9. Remote Access to Customer CDE (Service Providers only).
8.6 Where other authentication mechanisms are used (for example, physical or logical security tokens, smart cards, certificates, etc.), use of these mechanisms must be assigned as follows: • Authentication mechanisms must be assigned to an individual account and not shared among multiple accounts. • Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.	**P05 - Operational Policy.** Section 5.4.1. Issuing of Accounts
8.7 All access to any database containing cardholder data (including access by applications, administrators, and all other users) is restricted as follows: • All user access to, user queries of, and user actions on databases are through programmatic methods. • Only database administrators have the ability to directly access or query databases. • Application IDs for database applications can	**P11 - Systems and Applications Development Policy.** Section 5.2.1 Database Access.

PCI DSS Requirements	Policy Pack Reference
only be used by the applications (and not by individual users or other non-application processes).	
8.8 Ensure that security policies and operational procedures for identification and authentication are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2. Review and Update of the Policy Statement.

Requirement 9: Restrict physical access to cardholder data

PCI DSS Requirements	Policy Pack Reference
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	**P10 – Physical Security Policy.** Section 5.1.1 Physical Access Barriers, Internal Perimeter.
9.1.1 Use either video cameras or access control mechanisms (or both) to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: "Sensitive areas" refers to any data center, server room, or any area that houses systems that store, process, or transmit cardholder data. This excludes public-facing areas where only point-of-sale terminals are present, such as the cashier areas in a retail store..	**P10 – Physical Security Policy.** Section 5.1.1 Physical Access Barriers, Internal Perimeter. Section 5.3.2. Retention of Logs and Videos.
9.1.2 Implement physical and/or logical controls to restrict access to publicly accessible network jacks. For example, network jacks located in public areas and areas accessible to visitors could be disabled and only enabled when network access is explicitly authorized. Alternatively, processes could be implemented to ensure that visitors are escorted at all times in areas with active network jacks.	**P10 – Physical Security Policy.** Section 5.4.1 Communications Infrastructure.
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines.	**P10 – Physical Security Policy.** Section 5.4.1 Communications Infrastructure. Section 5.4.2 Mobile and Wireless Devices.
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, to include: • Identifying onsite personnel and visitors (for example, assigning badges) • Changes to access requirements • Revoking or terminating onsite personnel and expired visitor identification (such as ID badges)	**P10 - Physical Security Policy.** Section 5.1.2. Identification. **P10 - Physical Security Policy.** Section 5.1.1. Physical Access Barriers.
9.3 Control physical access for onsite personnel to the sensitive areas as follows: • Access must be authorized and based on individual job function. • Access is revoked immediately upon termination, and all physical access mechanisms, such as keys, access cards,	**P10 - Physical Security Policy.** Section 5.1.2. Identification.

PCI DSS Requirements	Policy Pack Reference
etc., are returned or disabled.	
9.4 Implement procedures to identify and authorize visitors. Procedures should include the following:	**P10 – Physical Security Policy.** Section 5.1.2 Identification. Section 5.3.2 Retention of Logs and Videos. **PR09 - Physical Security Procedure.**
9.4.1 Visitors are authorized before entering, and escorted at all times within, areas where cardholder data is processed or maintained.	
9.4.2 Visitors are identified and given a badge or other identification that expires and that visibly distinguishes the visitors from onsite personnel.	
9.4.3 Visitors are asked to surrender the badge or identification before leaving the facility or at the date of expiration.	
9.4.4 A visitor log is used to maintain a physical audit trail of visitor activity to the facility as well as computer rooms and data centers where cardholder data is stored or transmitted. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	
9.5 Physically secure all media.	**P10 - Physical Security Policy.** Section 4, Scope.
9.5.1 Store media backups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	**P10 - Physical Security Policy.** Section 5.2, Backup Security and Physical Media. **P10 - Physical Security Policy.** Section 5.2.2, Backups.
9.6 Maintain strict control over the internal or external distribution of any kind of media, including the following:	**P05 - Operational Policy.** Section 5.6.4 Transport of Data to Outside Bodies. **F07 Data Tracking Log.**
9.6.1 Classify media so the sensitivity of the data can be determined.	**P05 - Operational Policy.** Section 5.6.4 Transport of Data to Outside Bodies.
9.6.2 Send the media by secured courier or other delivery method that can be accurately tracked.	
9.6.3 Ensure management approves any and all media that is moved from a secured area (including when media is distributed to individuals).	
9.7 Maintain strict control over the storage and accessibility of media.	**P05 - Operational Policy.** Section 5.6.4 Transport of Data to Outside Bodies. **P10 - Physical Security Policy.** Section 5.2.2 Backups.
9.7.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	**P10 - Physical Security Policy.** Section 5.2.1 Logging.
9.8 Destroy media when it is no longer needed for business or legal reasons as follows:	**P10 - Physical Security Policy.** Section 5.2, Backup Security and Physical Media.

PCI DSS Requirements	Policy Pack Reference
	P10 - Physical Security Policy. Section 5.2.3 Security Disposal of Physical Media.
9.8.1 Shred, incinerate, or pulp hard-copy materials so that cardholder data cannot be reconstructed. Secure storage containers used for materials that are to be destroyed.	**P10 - Physical Security Policy.** Section 5.2.4 Hardcopy.
9.8.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	
9.9 Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.	**PR05 - Operational Procedure.** Section 5.6.2. Security Training. **P10 - Physical Security Policy.** Section 5.4.4. PIN Entry Device (PED) Protection.
9.9.1 Maintain an up-to-date list of devices. The list should include the following: • Make, model of device • Location of device (for example, the address of the site or facility where the device is located) • Device serial number or other method of unique identification.	**F22 - PED Device List.**
9.9.2 Periodically inspect device surfaces to detect tampering (for example, addition of card skimmers to devices), or substitution (for example, by checking the serial number or other device characteristics to verify it has not been swapped with a fraudulent device).	**P10 - Physical Security Policy.** Section 5.4.4. PIN Entry Device (PED) Protection.
9.9.3 Provide training for personnel to be aware of attempted tampering or replacement of devices. Training should include the following: • Verify the identity of any third-party persons claiming to be repair or maintenance personnel, prior to granting them access to modify or troubleshoot devices. • Do not install, replace, or return devices without verification. • Be aware of suspicious behavior around devices (for example, attempts by unknown persons to unplug or open devices). • Report suspicious behavior and indications of device tampering or substitution to appropriate personnel (for example, to a manager or security officer).	**P01 - Information Security Policy.** Section 5.6.2 Security Training.
9.10 Ensure that security policies and operational procedures for restricting physical access to cardholder data are documented, in use, and known to all affected parties.	**P10 - Physical Security Policy.** Section 2 Review and Update of the Policy Statement.

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI DSS Requirements	Policy Pack Reference
10.1 Implement audit trails to link all access to system components to each individual user.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.2 Implement automated audit trails for all system components to reconstruct the following events:	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.2.1 All individual user accesses to cardholder data	
10.2.2 All actions taken by any individual with root or administrative privileges	
10.2.3 Access to all audit trails	
10.2.4 Invalid logical access attempts	
10.2 5 Use of and changes to identification and authentication mechanisms—including but not limited to creation of new accounts and elevation of privileges—and all changes, additions, or deletions to accounts with root or administrative privileges	
10.2.6 Initialization, stopping, or pausing of the audit logs	
10.2.7 Creation and deletion of system-level objects	
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.	
10.4 Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. **Note:** One example of time synchronization technology is Network Time Protocol (NTP).	**P05 - Operational Policy.** Section 5.3.3. Time Synchronisation. **P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.4.1 Critical systems have the correct and consistent time.	
10.4.2 Time data is protected.	
10.4.3 Time settings are received from industry-accepted time sources.	
10.5 Secure audit trails so they cannot be altered.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
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.	

PCI DSS Requirements	Policy Pack Reference
10.5.5 Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	
10.6 Review logs and security events for all system components to identify anomalies or suspicious activity. **Note:** Log harvesting, parsing, and alerting tools may be used to meet this Requirement.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.6.1 Review the following at least daily: • All security events • Logs of all system components that store, process, or transmit CHD and/or SAD • Logs of all critical system components • Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.6.2 Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing. **P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing. **PR11 - Log Review Procedure**
10.6.3 Follow up exceptions and anomalies identified during the review process.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.8 Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems, including but not limited to failure of: • Firewalls • IDS/IPS • FIM • Anti-virus • Physical access controls • Logical access controls • Audit logging mechanisms • Segmentation controls (if used) Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
10.8.1 Additional requirement for service providers only: Respond to failures of any critical security controls in a timely manner. Processes for responding to failures in security controls must include: • Restoring security functions	**P03 - Disaster Recovery & Security Incident Response Policy.** Section 5.1.1 Disaster Situation

PCI DSS Requirements	Policy Pack Reference
• Identifying and documenting the duration (date and time start to end) of the security failure • Identifying and documenting cause(s) of failure, including root cause, and documenting remediation required to address root cause • Identifying and addressing any security issues that arose during the failure • Performing a risk assessment to determine whether further actions are required as a result of the security failure • Implementing controls to prevent cause of failure from reoccurring • Resuming monitoring of security controls Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	
10.9 Ensure that security policies and operational procedures for monitoring all access to network resources and cardholder data are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 2. Review and Update of the Policy Statement.

Requirement 11: Regularly test security systems and processes.

PCI DSS Requirements	Policy Pack Reference
11.1 Implement processes to test for the presence of wireless access points (802.11), and detect and identify all authorized and unauthorized wireless access points on a quarterly basis.	**P02 - Audit Policy.** Section 5.5 Wireless Access Point Scans. **P04 - Wireless Access Policy.** Section 5.8 Access Points.
11.1.1 Maintain an inventory of authorized wireless access points including a documented business justification.	**P02 - Audit Policy.** Section 5.5 Wireless Access Point Scans. **F23 - Wireless Access Point Inventory.**
11.1.2 Implement incident response procedures in the event unauthorized wireless access points are detected.	**PR08 - Security Incident Management Procedure.** Section 4.4 Security Incident Response.
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	**P05 - Operational Policy.** Section 5.1.4 Security Audits and Procedures.
11.2.1 Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high-risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking (per Requirement 6.1). Scans must be performed by qualified personnel.	
11.2.2 Perform quarterly external vulnerability scans, via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). Perform rescans as needed, until passing scans	

PCI DSS Requirements	Policy Pack Reference
are achieved.	
11.2.3 Perform internal and external scans, and rescans as needed, after any significant change. Scans must be performed by qualified personnel.	**PR05 - Change Control Procedure.** F04 - Change Control Form.
11.3 Implement a methodology for penetration testing that includes the following: • Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) • Includes coverage for the entire CDE perimeter and critical systems • Includes testing from both inside and outside the network • Includes testing to validate any segmentation and scope-reduction controls • Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 • Defines network-layer penetration tests to include components that support network functions as well as operating systems • Includes review and consideration of threats and vulnerabilities experienced in the last 12 months • Specifies retention of penetration testing results and remediation activities results.	**P12 - Penetration Testing Policy.** 5.1. General Approach to Testing. 5.2. Overall responsibility. 5.3. Testing Coverage. **PR12 -Penetration Testing Procedure.** Section 4.3.
11.3.1 Perform *external* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**P12 - Penetration Testing Policy.** Section 5.5. Frequency of Testing.
11.3.2 Perform *internal* penetration testing at least annually and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).	**P12 - Penetration Testing Policy.** Section 5.5. Frequency of Testing.
11.3.3 Exploitable vulnerabilities found during penetration testing are corrected and testing is repeated to verify the corrections.	**P12 - Penetration Testing Policy.** Section 5.7. Review and Processing of Results.
11.3.4 If segmentation is used to isolate the CDE from other networks, perform penetration tests at least annually and after any changes to segmentation controls/methods to verify that the segmentation methods are operational and effective, and isolate all out-of-scope systems from systems in the CDE.	**P12 - Penetration Testing Policy.** Section 5.5. Frequency of Testing.
11.3.4.1 Additional requirement for service providers only: If segmentation is used, confirm PCI DSS scope by performing penetration testing on segmentation controls at least every six months and after any changes to segmentation controls/methods. Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	**P12 - Penetration Testing Policy.** Section 5.5. Frequency of Testing.

PCI DSS Requirements	Policy Pack Reference
11.4 Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.	**P05 - Operational Policy.** Section 5.1.1 Security Monitoring Systems.
11.5 Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorized modification (including changes, additions and deletions) of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly. Note: For change-detection purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. Change-detection mechanisms such as file-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider)..	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
11.5.1 Implement a process to respond to any alerts generated by the change-detection solution.	
11.6 Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.	**P05 - Operational Policy.** Section 5.1.1 Security Monitoring Systems. **P12 - Penetration Testing Policy.** **PR12 -Penetration Testing Procedure**

Requirement 12: Maintain a policy that addresses information security for all personnel.

PCI DSS Requirements	Policy Pack Reference
12.1 Establish, publish, maintain, and disseminate a security policy.	**P01 - Information Security Policy.** Section 1 Policy Statement.
12.1.1 Review the security policy at least annually and update the policy when the environment changes.	**P01 – Information Security Policy.** Section 5.3 Annual Policy Review.
12.2 Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk Examples of risk-assessment methodologies include but are not limited to OCTAVE, ISO 27005 and NIST SP 800-30.	**P01 – Information Security Policy.** Section 5.3 Annual Policy Review.

PCI DSS Requirements	Policy Pack Reference
12.3 Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require the following:	
12.3.1 Explicit approval by authorized parties	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
12.3.2 Authentication for use of the technology	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
12.3.3 A list of all such devices and personnel with access	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
12.3.4 A method to accurately and readily determine owner, contact information, and purpose (for example, labeling, coding, and/or inventorying of devices)	**P05 - Operational Policy.** Section 5.3.2 Accountability and Auditing.
12.3.5 Acceptable uses of the technology	**P06 - Acceptable Use Policy.** Section 5.3.1 General Use and Ownership.
12.3.6 Acceptable network locations for the technologies	**P05 - Operational Policy.** Section 5.8 Networked Equipment. **P06 - Acceptable Use Policy.** Section 5.2 Acceptable Locations of Resources.
12.3.7 List of company-approved products	**P05 - Operational Policy.** Section 5.8 Networked Equipment.
12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity	**P05 - Operational Policy.** Section 5.3.5. Dial-In or Remote Access Services.
12.3.9 Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use	**P05 - Operational Policy.** Section 5.3.5. Dial-In or Remote Access Services.
12.3.10 For personnel accessing cardholder data via remote-access technologies, prohibit the copying, moving, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need. Where there is an authorized business need, the usage policies must require the data be protected in accordance with all applicable PCI DSS Requirements.	**P05 - Operational Policy.** Section 5.6.2 Remote Access to Cardholder Data.
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	**P06 - Acceptable Use Policy.** Section 5.1 Duty of Care. Section 4 Scope.
12.4.1 Additional requirement for service providers only: Executive management shall establish responsibility for the protection of cardholder data and a PCI DSS compliance program to include: • Overall accountability for maintaining PCI DSS compliance • Defining a charter for a PCI DSS compliance program and communication to executive management Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	**P01 – Information Security Policy.** Section 5.1 Reporting Structure for the Business. P13 - PCI Compliance Charter
12.5 Assign to an individual or team the following	**P01 - Information Security Policy.**

PCI DSS Requirements	Policy Pack Reference
information security management responsibilities:	Section 5.6.1 Policy Creation and Distribution.
12.5.1 Establish, document, and distribute security policies and procedures.	**P01 - Information Security Policy.** Section 5.6.1 Policy Creation and Distribution.
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	**P05 - Operational Policy.** Section 5.1.2 Alert Management. **P01 - Information Security Policy.** Section 5.1 Reporting Structure for the Business.
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	**P05 - Operational Policy.** Section 5.1.2 Alert Management.
12.5.4 Administer user accounts, including additions, deletions, and modifications.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
12.5.5 Monitor and control all access to data.	**P05 - Operational Policy.** Section 5.4.1 Issuing of Accounts.
12.6 Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.	**P01 - Information Security Policy.** Section 5.6.2 Security Training.
12.6.1 Educate personnel upon hire and at least annually. **Note:** Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	**P01 - Information Security Policy.** Section 5.6.2 Security Training.
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	**P01 - Information Security Policy.** Section 5.6.2 Security Training.
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history, and reference checks.) **Note:** For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	**P01 - Information Security Policy.** Section 5.6.3 Employment Checks.
12.8 Maintain and implement policies and procedures to manage service providers with whom cardholder data is shared, or that could affect the security of cardholder data, as follows:	**P07 - Third Parties Policy.** Section 5.1 Service Providers. Section 6.1 General.
12.8.1 Maintain a list of service providers including a description of the service provided.	**P07 - Third Parties Policy.** Section 5.1 Service Providers.
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess or otherwise store, process or transmit on behalf of the customer, or to the extent that they could impact the security of the customer's CDE. Note: The exact wording of an acknowledgement will depend on the agreement between the two parties, the details of the service being provided, and the responsibilities assigned to each party. The	**P07 - Third Parties Policy.** Section 5.1 Service Providers.

PCI DSS Requirements	Policy Pack Reference
acknowledgement does not have to include the exact wording provided in this requirement.	
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	**P07 - Third Parties Policy.** Section 6.1 General.
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	**P07 - Third Parties Policy.** Section 6.1 General.
12.8.5 Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity.	**P07 - Third Parties Policy.** Section 6.1 General. **F28 – Third Party Service Provider – Agreed Responsibilities Matrix**
12.9 ***Additional requirement for service providers only*:** Service providers acknowledge in writing to customers that they are responsible for the security of cardholder data the service provider possesses or otherwise stores, processes, or transmits on behalf of the customer, or to the extent that they could impact the security of the customer's cardholder data environment.	**P07 - Third Parties Policy.** Section 5.1 Service Providers.
12.10 Implement an incident response plan. Be prepared to respond immediately to a system breach.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: • Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum • Specific incident response procedures • Business recovery and continuity procedures • Data backup processes • Analysis of legal requirements for reporting compromises • Coverage and responses of all critical system components • Reference or inclusion of incident response procedures from the payment brands.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.2 Review and test the plan at least annually, including all elements listed in Requirement 12.10.1.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.4 Provide appropriate training to staff with security breach response responsibilities.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.5 Include alerts from security monitoring systems, including but not limited to intrusion-detection, intrusion-prevention, firewalls, and file-integrity monitoring systems.	**P05 – Operational Policy.** Section 5.5.2 Incident Response.
12.10.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	**P03 - Disaster Recovery & Security Incident Response Policy.** Section 5.2 Testing and Updating the Plan.
12.11 Additional requirement for service providers only:	**P05 – Operational Policy.**

PCI DSS Requirements	Policy Pack Reference
Perform reviews at least quarterly to confirm personnel are following security policies and operational procedures. Reviews must cover the following processes: • Daily log reviews • Firewall rule-set reviews • Applying configuration standards to new systems • Responding to security alerts • Change management processes Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement.	Section 5.3.9.4 – Service Provider Quarterly Review.
12.11.1 Additional requirement for service providers only: Maintain documentation of quarterly review process to include: • Documenting results of the reviews • Review and sign off of results by personnel assigned responsibility for the PCI DSS compliance program Note: This requirement is a best practice until January 31, 2018, after which it becomes a requirement	**P05 – Operational Policy.** Section 5.3.9.4 – Service Provider Quarterly Review.

Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers

PCI DSS Requirements	Policy Pack Reference
A1.1 If a shared hosting provider allows entities (for example, merchants or service providers) to run their own applications, verify these application processes run using the unique ID of the entity.	**P05 - Operational Policy.** Section 5.9 Shared Hosting Provider.
A1.2.a Verify the user ID of any application process is not a privileged user (root/admin).	
A1.2.b Verify each entity (merchant, service provider) has read, write, or execute permissions only for files and directories it owns or for necessary system files (restricted via file system permissions, access control lists, chroot, jailshell, etc.)	
A1.2.c Verify that an entity's users do not have write access to shared system binaries.	
A1.2.d Verify that viewing of log entries is restricted to the owning entity.	
A1.2.e To ensure each entity cannot monopolize server resources to exploit vulnerabilities.	
A1.3 Verify the shared hosting provider has enabled logging as follows, for each merchant and service provider environment: - Logs are enabled for common third-party applications. - Logs are active by default.	

PCI DSS Requirements	Policy Pack Reference
- Logs are available for review by the owning entity. - Log locations are clearly communicated to the owning entity.	
A1.4 Verify the shared hosting provider has written policies that provide for a timely forensics investigation of related servers in the event of a compromise.	**P03 - Disaster Recovery & Security Incident Response Policy.** Section 6.6 Forensic Investigation.

Appendix A2: Additional PCI DSS Requirements for Entities using SSL/early TLS

PCI DSS Requirements	Policy Pack Reference
A2.1 Where POS POI terminals (and the SSL/TLS termination points to which they connect) use SSL and/or early TLS, the entity must either: • Confirm the devices are not susceptible to any known exploits for those protocols. Or: • Have a formal Risk Mitigation and Migration Plan in place.	F29 - SSL and TLS mitigation
A2.2 Entities with existing implementations (other than as allowed in A.2.1) that use SSL and/or early TLS must have a formal Risk Mitigation and Migration Plan in place.	
A2.3 Additional Requirement for Service Providers Only: All service providers must provide a secure service offering by June 30, 2016. Note: Prior to June 30, 2016, the service provider must either have a secure protocol option included in their service offering, or have a documented Risk Mitigation and Migration Plan (per A.2.2) that includes a target date for provision of a secure protocol option no later than June 30, 2016. After this date, all service providers must offer a secure protocol option for their service.	

Completed by:	_____	Date:	_____
Print Name:	_____		
Approved by:	_____	Date:	_____
Print Name:	_____		