

Policy/Procedure	Description
PCI DSS Policies	
Install and Maintain a Firewall Configuration to Protect Cardholder Data	The purpose is to ensure the organization installs and maintains a firewall configuration to protect cardholder data.
Establish Firewall and Router Configuration Standards	The purpose is to ensure the organization establishes firewall and router configuration standards.
Build a Firewall Configuration	The purpose is to ensure the organization will build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.
Prohibit Direct Public Access	The purpose is to ensure the organization will prohibit direct public access between the Internet and any system component in the cardholder data environment.
Install Personal Firewall Software	The purpose is to ensure the organization will install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.
Do Not Use Vendor-Supplied Default Passwords	The purpose is to ensure the organization does not use vendor-supplied defaults for system passwords and other security parameters.
Always Change Vendor-Supplied Defaults	The purpose is to ensure the organization always changes vendor supplied defaults before installing a system on the network.
Develop Configuration Standards for all System Components	The purpose is to ensure the organization develops configurations standards for all system components.
Encrypt All Non-Console Administrative Access	The purpose is to ensure the organization will encrypt all non-console administrative access.
Shared Hosting Providers Protection Requirements	The purpose is to ensure that shared hosting providers must protect each entity's hosted environment and data.
Protect Cardholder Data	The purpose is to ensure the protection of cardholder data at all times.
Keep Cardholder Data Storage to a Minimum	The purpose is to ensure the organization will keep cardholder data storage to a minimum.
Do Not Store Sensitive Authentication Data	The purpose is to ensure the organization will not

	store sensitive authentication data after authorization (even if encrypted).
Mask PAN When Displayed	The purpose is to ensure the organization will mask PAN when displayed. The first six and last four digits are the maximum number of digits that can be displayed.
Render PAN, at Minimum, Unreadable Anywhere It Is Stored	The purpose is to ensure the organization will render PAN, at minimum, unreadable anywhere it is stored including data on portable digital media, backup media, in logs.
Protect Cryptographic Keys	The purpose is to ensure the organization will protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.
Fully Document and Implement All Key-Management Processes and Procedures	The purpose is to ensure the organization will fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
Encrypt Transmission of Cardholder Data	The purpose is to ensure the organization will keep sensitive information encrypted during transmission over networks that are easily accessed by malicious or unauthorized individuals.
Use Strong Cryptography and Security Protocols	The purpose is to ensure the organization will use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks.
Never Send Unencrypted PANs by End-User Messaging Technologies	The purpose is to ensure the organization will never send unencrypted PANs by end-user messaging technologies.
Maintain a Vulnerability Management Program	The purpose is to ensure the organization uses and regularly updates anti-virus software or programs.
Deploy Anti-Virus Software on All Systems Commonly Affected by Malicious Software	The purpose is to ensure the organization deploys anti-virus software on all systems commonly affected by malicious software.
Ensure that All Anti-Virus Mechanisms are Current, Actively Running and Capable of Generating Audit Logs	The purpose is to ensure the organization has all anti-virus mechanisms current, actively running and capable of generating audit logs.
Develop and Maintain Secure Systems and Applications	The purpose is to ensure the organization will have the latest vendor-supplied patches installed on all system components and software.

Ensure that the Latest Vendor-Supplied Security Patches are Installed	The purpose is to ensure that all system components and software have the latest vendor-supplied security patches installed.
Establish a Process to Identify Newly Discovered Security Vulnerabilities	The purpose is to ensure the organization establishes a process to identify newly discovered security vulnerabilities.
Develop Software Applications in Accordance with PCI DSS	The purpose is to ensure the organization develops software applications in accordance with PCI DSS requirements.
Follow Change Control Procedures for all Changes to System Components	The purpose is to ensure the organization will follow change control procedures for all changes to system components.
Develop All Web Applications Based on Secure Coding Guidelines	The purpose is to ensure the organization will develop all web applications including internal and external, as well as including web administrative access to applications based on secure coding guidelines.
Address New Threats and Vulnerabilities for Public-Facing Web Applications	The purpose is to ensure the organization will, for public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks.
Implement Strong Access Control Measures	The purpose is to ensure the organization will restrict access to cardholder data by business need to know.
Limit Access to System Components and Cardholder Data	The purpose is to ensure the organization will limit access to system components and cardholder data to only those individuals whose job requires such access.
Establish a Mechanism for System Components with Multiple Users	The purpose is to ensure the organization will establish a mechanism for system components with multiple users that restricts access based on user's need to know and is set to "deny all" unless specifically allowed.
Assign a Unique ID to Each Individual	The purpose is to assign all users a unique ID before allowing them to access system components or cardholder data.
Assign All Users a Unique ID	The purpose is to ensure the organization will assign all users a unique User ID prior to allowing them to access system components or cardholder data.
Employ a Method to Authenticate All Users	The purpose is to employ at least one method to authenticate all users in addition to assigning a unique

	ID.
Incorporate Two-Factor Authentication for Remote Access	The purpose is to ensure the organization will incorporate two-factor authentication for remote access to the network by employees, administrators, and third parties.
Render All Passwords Unreadable During Transmission and Storage	The purpose is to ensure that all passwords are rendered unreadable during transmission and storage on all system components using strong cryptography.
Ensure Proper User Authentication and Password Management	The purpose is to ensure proper user authentication and password management for non-consumer users and administrators on all system components.
Restrict Physical Access to Cardholder Data	The purpose is to ensure the organization will use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
Use Appropriate Facility Entry Controls	The purpose is to ensure the organization will use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
Develop Procedures to Help All Personnel Easily Distinguish Between Employees and Visitors	The purpose is to ensure the organization will develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible.
Make Sure All Visitors are Handled According to Policy	The purpose is to ensure the organization will make sure all visitors are handled according to policy.
Utilize a Visitor Log	The purpose is to ensure the organization will use a visitor log to maintain a physical audit trail of visitor activity.
Store Media backups in a Secure Location	The purpose is to ensure the organization stores media backups in a secure location such as an alternate or back-up site, or a dedicated commercial storage facility.
Physically Secure All Paper and Electronic Media	The purpose is to ensure the organization physically secures all paper and electronic media that contains cardholder data.
Maintain Strict Control over the Internal or External Distribution of Media	The purpose is to ensure the organization maintains strict control over the internal or external distribution of any kind of media that contains cardholder data.
Ensure Management Approves Media Removal	The purpose is to ensure that management approves

	any and all media containing cardholder data that is moved from a secured area.
Maintain Strict Control over the Storage and Accessibility of Media	The purpose is to ensure the organization maintains strict control over the storage and accessibility of media that contains cardholder data.
Destroy Unneeded Media Containing Cardholder Data	The purpose is to ensure the organization destroys media containing cardholder data when it is no longer needed for business or legal reasons.
Regularly Monitor and Tests Networks	The purpose is to ensure the organization will track and monitor all access to network resources and cardholder data.
Establish a Process for Linking All Access to System Components to an Individual User	The purpose is to ensure the organization will establish a process for linking all access to system components to each individual user.
Implement Automated Audit Trails	The purpose is to ensure the organization implements automated audit trails for all system components to reconstruct events.
Record Audit Trails for All System Components	The purpose is to ensure the organization records audit trail entries for all system components for each event.
Synchronize All Critical System Clocks and Times	The purpose is to ensure the organization synchronizes all critical system clocks and times.
Secure Audit Trails	The purpose is to ensure the organization secures audit trails so they cannot be altered.
Review Logs for all System Components	The purpose is to ensure the organization reviews logs for all system components at least daily.
Retain Audit Trail History for at Least One Year	The purpose is to ensure the organization retains an audit trail history for at least one year with a minimum of three months immediately available for analysis.
Regularly Test Security Systems and Processes	The purpose is to ensure the organization will regularly test security systems and processes for the protection of cardholder data.
Test for the Presence of Wireless Access Points	The purpose is to ensure the organization will test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use.
Run Internal and External Network Vulnerability Scans at Least Quarterly	The purpose is to ensure the organization will run internal and external network vulnerability scans at

	least quarterly and after any significant change affecting the network.
Perform External and Internal Penetration Testing at Least Once a Year	The purpose is to ensure the organization performs external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification.
Use Intrusion Detection Systems to Monitor All Traffic	The purpose is to ensure the organization uses intrusion detection systems, and/or intrusion prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises.
Deploy File-Integrity Monitoring Software	The purpose is to ensure the organization deploys file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files, and configure the software to perform critical file comparisons at least weekly.
Maintain an Information Security Policy	The purpose is to ensure the development and maintenance of an information security policy.
Establish, Publish, Maintain, and Disseminate a Security Policy	The purpose is to ensure the organization will establish, publish, maintain, and disseminate a security policy.
Develop Daily Operational Security Procedures	The purpose is to ensure the organization will develop daily operational security procedures.
Develop Usage Policies for Critical Employee-Facing Technologies	The purpose is to ensure the organization will develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors.
Clearly Define Information Security Responsibilities	The purpose is to ensure that the security policy and procedures clearly define information security responsibilities for all employees, contractors, and other members of the workforce.
Assign Information Security Management Responsibilities	The purpose is to ensure that individuals or teams are assigned to information security management responsibilities.
Implement a Formal Security Awareness Program	The purpose is to ensure the organization implements a formal security awareness program to make all employees aware of the importance of cardholder data security.

Screen Potential Employees Prior to Hire	The purpose is to ensure the organization screens potential employees prior to hire to minimize the risk of attacks from internal sources.
Maintain and Implement Policies and Procedures to Manage Service Providers	The purpose is to ensure that if cardholder data is shared with service providers, the organization will maintain and implement policies and procedures to manage service providers.
Implement an Incident Response Plan	The purpose is to ensure the organization implements an incident response plan.
Shared Hosting Providers Must Protect Cardholder Data Environment	The purpose is intended for shared hosting providers who wish to provide their merchant and/or service provider customers with a PCI DSS compliant hosting environment.
Protect Each Entity's Hosted Environment and Data	The purpose is to ensure that each entity's hosted environment and data is protected.

Figure 1: Summary of PCI DSS Policies