Policy	Description
Build and Maintain a Secure Network	
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 Firewall and Router Configurations	The purpose is to ensure the organization builds a firewall and router 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 prohibits direct public access between the Internet and any system component in the cardholder data environment to eliminate, or minimally reduce, the chance of the systems being compromised.
Install Personal Firewall Software	The purpose is to ensure the organization installs personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet.
Do Not Use Vendor-Supplied Default Passwords for System Passwords and Other Security Parameters	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 encrypts all non-console administrative access.
Shared Hosting Providers Must Protect Each Entity's Hosted Environment and Data	The purpose is to ensure that shared hosting providers must protect each entity's hosted environment and data.
Protect Cardholder Data	
Protect Stored 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 keeps cardholder data storage to a minimum.
Do Not Store Sensitive Authentication Data	The purpose is to ensure the organization does not store

Policy	Description
after Authorization	sensitive authentication data after authorization (even if encrypted).
Mask PAN When Displayed	The purpose is to ensure the organization masks the 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 renders the PAN, at minimum, unreadable anywhere it is stored including data on portable digital media, backup media, and in logs.
Protect Any Keys Used to Secure Cardholder Data against Disclosure and Misuse	The purpose is to ensure the organization protects any keys, including 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 fully documents and implements all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
Encrypt Transmission of Cardholder Data across Open, Public Networks	The purpose is to ensure the organization keeps 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 uses 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 never transmits unencrypted PANs by end-user messaging technologies.
Maintain a Vulnerability Management Program	
Use and Regularly Update Anti-virus Software or Programs	The purpose is to ensure that 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 Generating Audit Logs	The purpose is to ensure that the organization's anti-virus mechanisms are current, actively running and capable of generating audit logs.
Develop and Maintain Secure Systems and Applications	The purpose is to ensure the organization installs the latest vendor-supplied patches on all system components and software.

Policy	Description
Ensure that all System Components and Software have the Latest Vendor-Supplied Security Patches 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 and Assign a Risk Ranking Newly Discovered Security Vulnerabilities	The purpose is to ensure that the organization establishes a process to identify and assign a risk ranking to newly discovered security vulnerabilities.
Develop Software Applications in Accordance with PCI DSS	The purpose is to ensure that 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 that the organization follows change control procedures for all changes to system components.
Develop Applications Based on Secure Coding Guidelines	The purpose is to ensure that the organization uses secure coding guidelines to develop all applications so that common coding vulnerabilities are prevented.
For Public-Facing Web Applications, Address New Threats and Vulnerabilities on an Ongoing Basis	The purpose is to ensure that for public-facing web applications, the organization addresses new threats and vulnerabilities on an ongoing basis and ensures that their applications are protected against known attacks.
Implement Strong Access Control Measures	
Restrict Access to Cardholder Data by Business Need to Know	The purpose is to ensure that the organization restricts access to cardholder data by business need to know.
Limit Access to System Components and Cardholder Data	The purpose is to ensure that the organization limits access to system components and cardholder data to only those individuals whose job requires such access.
Establish an Access Control System for System Components with Multiple Users	The purpose is to ensure that the organization establishes a mechanism for system components with multiple users that restricts access based on a user's need to know and is set to "deny all" unless specifically allowed.
Assign a Unique ID to Each Person with Computer Access	The purpose is to assign a unique ID to each person the with access to system components or cardholder data.
Assign All Users a Unique ID	The purpose is to ensure that the organization assigns a unique User ID to all users before allowing them to access the organization's 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 to help protect the unique IDs from being compromised.

Policy	Description
Incorporate Two-Factor Authentication for Remote Access	The purpose is to ensure that the organization incorporates 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 Identification and Authentication Management	The purpose is to ensure proper user identification and authentication management for non-consumer users and administrators on all system components so that an unauthorized user cannot exploit an unused account to access cardholder data.
Restrict Physical Access to Cardholder Data	The purpose is to ensure that the organization uses appropriate controls to limit and monitor physical access to systems in the cardholder data environment.
Use Appropriate Facility Entry Controls	The purpose is to ensure that the organization uses appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
Develop Procedures to Easily Distinguish Between Onsite Personnel and Visitors	The purpose is to ensure that the organization develops procedures to help all personnel easily distinguish between onsite personnel (example: 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 that all of the organization's visitors are handled according to policy.
Use a Visitor Log to Maintain a Physical Audit Trail of Visitor Activity	The purpose is to ensure that the organization uses a visitor log to maintain a physical audit trail of visitor activity.
Store Media backups in a Secure Location	The purpose is to ensure that 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 Media	The purpose is to ensure that the organization physically secures all paper and electronic media that contains cardholder data.
Maintain Strict Control over the Internal or External Distribution of Any Kind of Media	The purpose is to ensure that the organization maintains strict control over the internal or external distribution of any kind of media that contains cardholder data.
Ensure Management Approves any and all Media Containing Cardholder Data Moved from a Secured Area	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	The purpose is to ensure that the organization maintains

Policy	Description
and Accessibility of Media that Contains Cardholder Data	strict control over the storage and accessibility of media that contains cardholder data.
Destroy Media Containing Cardholder Data When it is No Longer Needed	The purpose is to ensure that the organization destroys media containing cardholder data when it is no longer needed for business or legal reasons.
Monitor and Test Networks	
Track and Monitor all Access to Network Resources and Cardholder Data	The purpose is to ensure that the organization tracks and monitors all access to network resources and cardholder data.
Establish a Process for Linking All Access to System Components to Each Individual User	The purpose is to ensure that the organization establishes a process for linking all access to system components to each individual user.
Implement Automated Audit Trails for all System Components to Reconstruct Events	The purpose is to ensure that the organization implements automated audit trails for all system components to reconstruct events.
Record Audit Trails for All System Components for Each Event	The purpose is to ensure that 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 that the organization synchronizes all critical system clocks and times to facilitate the accurate coordination of logged events.
Secure Audit Trails	The purpose is to ensure that the organization secures audit trails so they cannot be altered.
Review Logs for all System Components at Least Daily	The purpose is to ensure that 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 that 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 that the organization regularly tests security systems and processes for the protection of cardholder data.
Test for the Presence of Wireless Access Points at Least Quarterly	The purpose is to ensure that the organization tests for the presence of wireless access points by using a wireless analyzer at least quarterly or by 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 that the organization runs internal and external network vulnerability scans at least quarterly and after any significant change affecting the network.

Policy	Description
s	The purpose is to ensure that 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 that 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 Tools	The purpose is to ensure that 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	
Maintain a Policy that Addresses Information Security for All Personnel	The purpose is to ensure that the organization develops and maintains a strong information security policy.
Establish, Publish, Maintain, and Disseminate a Security Policy	The purpose is to ensure that the organization establishes, publishes, maintains, and disseminates a security policy.
Develop Daily Operational Security Procedures	The purpose is to ensure that the organization develops daily operational security procedures.
Develop Usage Policies for Critical Employee-Facing Technologies	The purpose is to ensure that the organization develops usage policies for critical employee-facing technologies and to define proper use of these technologies for all employees and contractors.
Ensure that the Security Policy and Procedures 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 to an Individual or Team Information Security Management Responsibilities	The purpose is to ensure that the organization assigns information security management responsibilities to a specific individual or team.
Implement a Formal Security Awareness Program	The purpose is to ensure that 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 that the organization screens potential employees prior to hire to minimize the risk of attacks from internal sources.

Policy	Description
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 maintains and implements policies and procedures to manage these service providers.
Shared Hosting Providers Must Protect Cardholder Data Environment	This policy applies to shared hosting providers who wish to provide their merchant and/or service provider customers with a PCI DSS compliant hosting environment. These steps should be met, in addition to all other relevant PCI DSS requirements, if applicable.
Protect Each Entity's Hosted Environment and Data	The purpose is to ensure that each entity's hosted environment and data is protected.
Implement an Incident Response Plan	The purpose is to ensure that the organization implements an incident response plan.