PCI DSS Requirements - Security Controls and Processes

1. Build and maintain a secure network	1.1 Establish firewall and router configuration standards that formalize testing whenever configurations change; that identify all connections to cardholder data (including wireless); thatuse various technical settings for each implementation; and stipulate a review of configuration rule sets at least every six months
	1.2 Build firewall and router configurations that restrict all traffic from "untrusted" networks and hosts,except for protocols necessary for the cardholder data environment
	1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.
	1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the organization's network
2. Do not use vendor-supplied defaults for system passwords and other security parameters	2.1 Always change vendor-supplied defaults before installing a system on the network. This includes wireless devices that are connected to the cardholder data environment or are used to transmit cardholder data.
	2.2 Develop configuration standards for all system components that address all known security vulnerabilities and are consistent with industry-accepted definitions. Update system configuration standards as new vulnerability issues are identified
	2.3 Encrypt using strong cryptography all non-console administrative access such as browser/web-based management tools.
	2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data
3. Protect stored cardholder data	3.1 Limit cardholder data storage and retention time to that required for business, legal, and/or regulatory purposes, as documented in your data retention policy. Purge unnecessary stored data at least quarterly.
	3.2 Do not store sensitive authentication data after authorization (even if it is encrypted). See guidelines in table below. Issuers and related entities may store sensitive authentication data if there is a business justification, and the data is stored securely
	3.3 Mask PAN when displayed; the first six and last four digits are the maximum number of digits you may display. Not applicable for authorized people with a legitimate business need to see the full PAN. Does not supersede stricter requirements in place for displays of cardholder data such as on a point-of-sale receipt
	3.4 Render PAN unreadable anywhere it is stored – including on portable digital media, backup media, in logs, and data received from or stored by wireless networks. Technology solutions for this requirement may include strong one-way hash functions of the entire PAN, truncation, index tokens with securely stored pads, or strong cryptography. (See PCI DSS Glossary for definition of strong cryptography.)

PCI DSS Requirements - Security Controls and Processes

3. Protect stored cardholder data (con't)	3.5 Protect any keys used for encryption of cardholder data from disclosure and misuse 3.6 Fully document and implement all appropriate key management processes and procedures forcryptographic keys used for encryption of cardholder data
4. Encrypt transmission of cardholder data across open, public networks	4.1 Use strong cryptography and security protocols such as SSL/TLS, SSH or IPSec to safeguard sensitive cardholder data during transmission over open, public networks. Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. The use of WEP as a security control is prohibited. 4.2 Never send unprotected PANs by end user messaging technologies
5. Use and regularly update anti-virus software or programs	5.1 Deploy anti-virus software on all systems affected by malicious software (particularly personal computers and servers). 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs
6. Develop and maintain secure systems and applications	6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Deploy critical patches within a month of release 6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Risk rankings should be based on industry best practices and guidelines. 6.3 Develop software applications (internal and external, and including web-based administrative access) in accordance with PCI DSS and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.4 Follow change control processes and procedures for all changes to system components 6.5 Develop applications based on secure coding guidelines and review custom application code to identify coding vulnerabilities. Follow up-to-date industry best practices to identify and manage vulnerabilities 6.6 Ensure all public-facing web applications are protected against known attacks, either by performing code vulnerability reviews at least annually or by installing a web application firewall in front of public-facing web applications.
7. Restrict acess to cardholder data by business need to know	7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
8. Assign a unique ID to each person with computer access	8.1 Assign all users a unique user name before allowing them to access system components or cardholder data.

PCI DSS Requirements - Security Controls and Processes

8. Assign a unique ID to each person with computer access (con't)	8.2 Employ at least one of these to authenticate all users: something you know, such as a password or passphrase; something you have, such as a token device or smart card; or something you are, such as a biometric
	8.3 Implement two-factor authentication for remote access to the network by employees, administrators, and third parties. . Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.
	8.4 Render all passwords unreadable during storage and transmission, for all system components, by using strong cryptography
	8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components.
9. Restrict physical access to cardholder data	9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.
	9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible
	9.3 Ensure all visitors are authorized before entering areas where cardholder data is processed or maintained; given a physical token that expires and that identifies visitors as not onsite personnel; and are asked to surrender the physical token before leaving the facility or at the date of expiration.
	9.4 Use a visitor log to maintain a physical audit trail of visitor information and activity, including visitor name and company, and the onsite personnel authorizing physical access. Retain the log for at least three months unless otherwise restricted by law
	9.5 Store media back-ups in a secure location, preferably off site.
	9.6 Physically secure all media.
	9.7 Maintain strict control over the internal or external distribution of any kind of media. Classify media so the sensitivity of the data can be determined.
	9.8 Ensure that management approves any and all media moved from a secured area, especially when media is distributed to individuals.
	9.9 Maintain strict control over the storage and accessibility of media
	9.10 Destroy media when it is no longer needed for business or legal reasons.
10. Track and monitor all access to network resources and cardholder data	10.1 Establish a process for linking all access to system components to each individual user – especially access done with administrative privileges

PCI DSS Requirements - Security Controls and Processes

10. Track and monitor all access to network resources and cardholder data (con't)	10.2 Implement automated audit trails for all system components for reconstructing these events: all individual user accesses to cardholder data; all actions taken by any individual with root or administrative privileges; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of the audit logs; creation and deletion of system-level objects. 10.3 Record audit trail entries for all system components for each event, including at a minimum: user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, system component or resource 10.4 Using time synchronization technology, synchronize all critical system clocks and times and implement controls for acquiring, distributing, and storing time 10.5 Secure audit trails so they cannot be altered 10.6 Review logs for all system components related to security functions at least daily. 10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis.
11. Regularly test security systems and processes	11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Typical methods are wireless network scans, physical/logical inspections of system components and infrastructure, network access control (NAC), or wireless IDS/IPS. 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network. After passing a scan for initial PCI DSS compliance, an entity must, in subsequent years, pass four consecutive quarterly scans as a requirement for compliance. Quarterly external scans must be performed by an Approved Scanning Vendor (ASV). Scans conducted after network changes may be performed by internal staff. 11.3 Perform external and internal penetration testing, including network- and application-layer penetration tests, at least annually and after any significant infrastructure or application upgrade or modification 11.4 Use network intrusion detection systems and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. IDS/IPS engines, baselines, and signatures must be kept up to date 11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files. Configure the software to perform critical file comparisons at least weekly.
12. Maintain a policy that addresses information security for all personnel	12.1 Establish, publish, maintain, and disseminate a security policy that addresses all PCI DSS requirements, includes an annual process for identifying vulnerabilities and formally assessing risks, and includes a review at least once a year and when the environment changes.

PCI DSS Requirements - Security Controls and Processes

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

12.2 Develop daily operational security procedures that are consistent with requirements in PCI DSS

12.3 Develop usage policies for critical technologies to define their proper use by all personnel. These include remote access, wireless, removable electronic media, laptops, tablets, handheld devices, email and Internet

12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel

12.5 Assign to an individual or team information security responsibilities defined by 12.5 subsections

12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data securit

12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Example screening includes previous employment history, criminal record, credit history, and reference checks.

12.8 If cardholder data is shared with service providers, maintain policies and procedures to formally 24 identify service provider responsibilities for securing cardholder data, and monitor service providers' PCI DSS compliance status at least annually

12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.