1. Build and maintain a Secure network and System
   1. Install and maintain a firewall configuration to protect cardholder data
      1. Establish and implement firewall and router configuration standards
      2. Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.
      3. Prohibit direct public access between the Internet and any system component in the cardholder data environment.
      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
      5. Ensure that security policies and operational procedures for managing firewalls are documented, in use, and known to all affected parties.
   2. Do not use vendor-supplied defaults for system passwords and other security parameters
2. Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network
3. 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.
4. Encrypt all non-console administrative access using strong cryptography.
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
6. Shared hosting providers must protect each entity’s hosted environment and cardholder data
7. Protect Cardholder data
   1. Protect stored cardholder data
      1. Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes
      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.
      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 the first six/last four digits of the PAN
      4. Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs)
      5. Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse
      6. Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data
   2. Encrypt transmission of cardholder data across open, public networks
      1. Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission over open, public networks
      2. Never send unprotected PAN by end-user messaging technologies
8. Maintain a vulnerability Management System Program
   1. Protect all systems against malware and regularly update anti-virus software or programs
      1. Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
      2. Ensure that all anti-virus mechanisms are maintained
      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
      4. Ensure that security policies and operational procedures for protecting systems against malware are documented, in use, and known to all affected parties.
   2. Develop and maintain secure systems and applications
      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.
      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.
      3. Develop internal and external software applications (including web-based administrative access to applications) securely
      4. Follow change control processes and procedures for all changes to system components
      5. Address common coding vulnerabilities in software-development processes
      6. For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks
      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.
9. Regularly Monitor and Test networks
   1. Track and monitor all access to network resources and cardholder data
      1. Implement audit trails to link all access to system components to each individual user.
      2. Implement automated audit trails for all system components
      3. Record at least the following audit trail entries for all system components
      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.
      5. Secure audit trails so they cannot be altered
      6. Review logs and security events for all system components to identify anomalies or suspicious activity.
      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).
      8. Additional requirement for service providers only: Implement a process for the timely detection and reporting of failures of critical security control systems
   2. Regularly test security systems and processes
      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.
      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).
      3. Implement a methodology for penetration testing
      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
      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
      6. Ensure that security policies and operational procedures for security monitoring and testing are documented, in use, and known to all affected parties.