UNIVERSITY OF
NORTHERN COLORADO

PCI DSS 3.1 Security Policy

Purpose

This document outlines all of the policy items required by PCI to be compliant with the current PCI DSS 3.1 standard and that it is the University of Northern Colorado's Policy to be compliant with all requirements set forth below.

Applies To

This Policy applies to all PCI environments within the University of Northern Colorado and to all staff, faculty, and students that operate within or in cooperation with a PCI environment.

Definitions

CDE – Cardholder data environment

DSS – Data Security Standards

PA-DSS – Payment Application Data Security Standards

PCI – Payment Card Industry

PAN – Primary Account Number

SAD – Sensitive Authentication Data, includes Full Track Data, PIN/PIN Block, CAV2/CVC2/CVV2/CID

Cardholder Data – PAN, Cardholder Name, Service Code, Expiration Date

Policy

UNC commits to the following actions in regard to each section of PCI-DSS version 3.1:

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

1.1

a. A formal process exists for approving and testing all external network connections and changes to the firewall and router configurations.
b. UNC will, at all times, maintain a current network diagram for PCI environments.
c. Configuration standards include requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.
d. The current network diagram is consistent with the firewall configuration standards.
e. Firewall and router configuration standards include a description of groups, roles, and responsibilities for logical management of network components.
f. Firewall and router configuration standards include a documented list of services, protocols and ports necessary for business (for example, hypertext transfer protocol (HTTP), Secure Sockets Layer (SSL), Secure Shell (SSH), and Virtual Private Network (VPN) protocols).
g. All allowed insecure services, protocols, and ports necessary, and are security features documented and implemented for each.
h. Firewall and router configuration standards require a review at least every six months.
i. Firewall and router rule sets reviewed at least every six months.
j. Maintain a current network PCI network diagram for each of the PCI environments.
k. Maintain a current dataflow diagram for PCI environments.

1.2

a. Inbound and outbound traffic is restricted to that which is necessary for the cardholder data environment, and the restrictions are documented.
b. All other inbound and outbound traffic specifically denied.
c. Router configuration files are secure and synchronized.
d. Perimeter firewalls are installed between any wireless networks and the cardholder data environment, and are these firewalls configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.

1.3

a. Direct connections are prohibited for inbound or outbound traffic between the Internet and the cardholder data environment.
b. Internal addresses are prohibited from passing from the Internet into the PCI environment.
c. Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized.

d. Stateful inspection, also known as dynamic packet filtering, is implemented (that is, only established connections are allowed into the network).
e. System components that store cardholder data (such as a database) are placed in an internal network zone, segregated from the DMZ and other untrusted networks.
f. Methods are in place to prevent the disclosure of private IP addresses and routing information to the Internet.
g. Any disclosure of private IP addresses and routing information to external entities requires authorization.

1.4

a. Personal firewall software is installed and active on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.
b. The personal firewall software is configured to specific standards, and not alterable by mobile and/or employee owned computer users.

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

2.1

a. Vendor-supplied defaults are always changed before installing a system on the network.
b. For the wireless environment encryption keys are changed from default at installation, and changed anytime anyone with knowledge of the keys leaves the company or changes positions.
c. Default SNMP community strings on wireless devices are changed.
d. Default passwords/passphrases on access points are changed.
e. Firmware on wireless devices is updated to support strong encryption for authentication and transmission over wireless networks.
f. All other security-related wireless vendor defaults are changed.

2.2

a. Configuration standards are developed for all system components and are they consistent with industry-accepted system hardening standards.
b. System configuration standards are updated as new vulnerability issues are identified, as defined in requirement 6.2.
c. System configuration standards are applied when new systems are configured.
d. Only one primary function is implemented per server, to prevent functions that require different security levels from co-existing on the same server.

e. Virtualization technologies are used, and only one primary function is implemented per virtual system component or device.
f. Only necessary services, protocols, daemons, etc. are enabled as required for the function of the system.
g. All enabled insecure services, daemons, or protocols are justified, and are security features documented and implemented.
h. System administrators and/or personnel that configure system components are knowledgeable about common security parameter settings for those system components.
i. Common system security parameters settings are included in the system configuration standards.
j. Security parameter settings are set appropriately on system components.
k. All unnecessary functionality - such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers – have been removed.
l. Enabled functions are documented and do support a secure configuration.
m. Only documented functionalities are present on system components.

2.3

a. All non-console administrative access is encrypted with strong cryptography, and a strong encryption method invoked before the administrator's password is requested.
b. System services and parameter files are configured to prevent the use of Telnet and other insecure remote login commands.
c. Administrator access to web-based management interfaces are encrypted with strong cryptography.
d. All non-console administrative access requires two factor authentication.

2.4

a. An inventory of all system components in the PCI is maintained by each environment owner and reported up to the CISO.

2.5

a. Security policies and operational procedures for managing vendor defaults and other security parameters are documented and used by all parties.

Requirement 3: Protect stored cardholder data.

3.1

a. Data retention and disposal policies and procedures are implemented and do they include specific requirements for retention of cardholder data as required for business, legal, and/or regulatory purposes.
b. Policies and procedures include provisions for the secure disposal of data when no longer needed for legal, regulatory, or business reasons, including disposal of cardholder data.

c. Policies and procedures include coverage for all storage of cardholder data.
d. Processes and procedures include:
A programmatic process (automatic or manual) to remove, at least quarterly, stored cardholder data that exceeds requirements defined in the data retention policy.
Requirements for a review, conducted at least quarterly, to verify that stored cardholder data does not exceed requirements defined in the data retention policy.
e. All stored cardholder data meets the requirements defined in the data retention policy.

3.2

a. When sensitive authentication data is received and deleted, processes in place to securely delete the data to verify that the data is unrecoverable. The university does not store SAD.
b. 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) are not stored under any circumstance.
c. The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance.
d. The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance.

3.3

a. The PAN is masked when displayed (the first six and last four digits are the maximum number of digits to be displayed).

3.4

a. PAN is rendered unreadable anywhere it is stored (including data repositories, portable digital media, backup media, and in audit 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.
b. Logical access to encrypted file systems is managed independently of native operating system access control mechanisms.
c. Cryptographic keys stored securely.
d. Cardholder data on removable media is encrypted wherever stored.

3.5

a. Access to cryptographic keys are restricted to the fewest number of custodians necessary.
b. Keys are stored in encrypted format and are key-encrypting keys stored separately from data-encrypting keys.
c. Cryptographic keys are stored in the fewest possible locations and forms.

3.6

a. Cryptographic key procedures include the generation of strong cryptographic keys.
b. Cryptographic key procedures include secure cryptographic key distribution.
c. Cryptographic key procedures include secure cryptographic key storage.
d. Cryptographic key procedures include cryptographic key changes for keys that have reached the end of their defined cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of ciphertext 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).
e. Cryptographic key procedures include retirement or replacement (for example, archiving, destruction, and/or revocation) of cryptographic keys when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key).
f. Cryptographic key procedures include replacement of known or suspected compromised keys.
g. If retired or replaced cryptographic keys are retained, are these keys only used for decryption/verification purposes (not used for encryption operations).
h. Cryptographic key procedures include split knowledge and dual control of cryptographic keys (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key), for manual clear-text key-management operations.
i. Cryptographic key procedures include the prevention of unauthorized substitution of cryptographic keys.
j. Cryptographic key custodians required to formally acknowledge (in writing or electronically) that they understand and accept their key-custodian responsibilities.

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

4.1

a. Strong cryptography and security protocols, such as later versions of TLS, SSH or IPSEC, are used to safeguard sensitive cardholder data during transmission over open, public networks.
b. Only trusted keys and/or certificates are accepted.
c. Security protocols implemented to use only secure configurations, and not to support insecure versions or configurations.
d. The proper encryption strength is implemented for the encryption methodology in use (check vendor recommendations/best practices).

e. For SSL/TLS implementations:
HTTPS appears as part of the browser Universal Record Locator.
Cardholder data is required only when HTTPS appears in the URL.

f. Industry best practices (for example, IEEE 802.11i) are used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment.

4.2

a. PANs are rendered unreadable or secured with strong cryptography whenever they are sent via end-user messaging technologies (for example, e-mail, instant messaging, or chat).

b. Policies are in place that state that unprotected PANs are not to be sent via end-user messaging technologies.

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

5.1

a. Anti-virus software is deployed on all systems commonly affected by malicious software.

b. All anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software (for example, viruses, Trojans, worms, spyware, adware, and rootkits).

5.2

a. The anti-virus policy requires updating of anti-virus software and definitions.

b. The master installation of the software is enabled for automatic updates and scans.

c. Automatic updates and periodic scans is enabled.

d. All anti-virus mechanisms will generate audit logs, and logs are retained in accordance with PCI DSS Requirement 10.7.

5.3

a. Anti-virus configurations are actively running on systems required by PCI and have been configured to prevent removal.

5.4

a. Security policies and operational procedures for protecting system against malware are documented and known to all affected parties.

Requirement 6: Develop and maintain secure systems and applications.

6.1

a. All system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.
b. Critical security patches are installed within one month of release.

6.2

a. A process exists to identify newly discovered security vulnerabilities, including a risk ranking that are assigned to such vulnerabilities.
b. A process exists to identify new security vulnerabilities include using outside sources for security vulnerability information.

6.3

a. The software development processes are based on industry standards and/or best practices.
b. Information security is included throughout the software development life cycle.
c. Software applications are developed in accordance with PCI DSS (for example, secure authentication and logging).
d. Custom application accounts, user IDs, and/or passwords are removed before applications become active or are released to customers.
e. All custom application code changes are reviewed (either using manual or automated processes) prior to release to production or customers in order to identify any potential coding vulnerability as follows:
Code changes are reviewed by individuals other than the originating code author, and by individuals who are knowledgeable in code review techniques and secure coding practices. Code reviews ensure code is developed according to secure coding guidelines (per PCI DSS Requirement 6.5). Appropriate corrections are implemented prior to release. Code review results are reviewed and approved by management prior to release.
Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle. Code reviews can be conducted by knowledgeable internal personnel or third parties.
Web applications are also subject to additional controls, if they are public-facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.

6.4

a. Development/test environments are separate from the production environment, and access control is in place to enforce the separation.

b. There are separation of duties between personnel assigned to the development/test environments and those assigned to the production environment.
c. Production data (live PANs) is not used for testing or development.
d. Test data and accounts are removed before production systems become active.
e. Change control procedures for implementing security patches and software modifications are documented and require items 6.4.5.1 – 6.4.5.4.
f. All changes have a documentation of impact.
g. All changes are approved by authorized parties.
h. All changes are functionality tested to verify that the change does not adversely impact the security of the system.
i. Custom code changes, are updates are tested for compliance with PCI DSS Requirement 6.5 before being deployed into production.
j. There is a back out procedure for each change.

6.5

a. All applications developed is based on secure coding guidelines.
b. Developers are knowledgeable in secure coding techniques.
c. Prevention of common coding vulnerabilities are covered in software development processes to ensure that applications are not vulnerable to, at a minimum the following:
Injection flaws, particularly SQL injection.
Buffer overflow.
Insecure cryptographic storage.
Insecure communications.
Improper error handling.
All ""High"" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).
Cross-site scripting (XSS).
Improper Access Control such as insecure direct object references, failure to restrict URL access, and directory traversal.
Cross-site request forgery (CSRF).
Broken authentication and session management.

6.6

a. For public-facing web applications, new threats and vulnerabilities are addressed on an ongoing basis, these applications are protected against known attacks by applying either of the following methods:
Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, as follows: At least annually. After any changes by an organization that specializes in application security. That all vulnerabilities are corrected. That the application is re-evaluated after the corrections- or

- Installing a web-application layer firewall in front of public-facing web applications to detect and prevent web-based attacks.

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

7.1

a. Access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows:
Access rights for privileged user IDs are restricted to least privileges necessary to perform job responsibilities.
Privileges are assigned to individuals based on job classification and function (also called "role-based access control" or RBAC).
Documented approval by authorized parties required (in writing or electronically) that specifies required privileges.
Access controls implemented via an automated access control system.

7.2

a. An access control system is in place for systems with multiple users to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:
Access control systems is in place on all system components.
Access control systems is configured to enforce privileges assigned to individuals based on job classification and function.
Access control systems have a default "deny-all" setting.

7.3

a. Ensure that security policies and operational procedures for restricting access to cardholder data are documented, in use, and known by all parties.

Requirement 8: Identify and authenticate access to system components.

8.1

a. All users are assigned a unique ID before allowing them to access system components or cardholder data.

8.2

a. In addition to assigning a unique ID, is one or more of the following methods employed to authenticate all users:
Something you know, such as a password or passphrase.
Something you have, such as a token device or smart card.
Placing servers containing cardholder data behind proxy servers/firewalls or content caches.
Something you are, such as a biometric.

8.3

a. Two-factor authentication is incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties.

8.4

a. All passwords are rendered unreadable during transmission and storage on all system components using strong cryptography.

8.5

a. Proper user identification and authentication management controls are in place for non-consumer users and administrators on all system components, as follows:
Additions, deletions, and modifications of user IDs, credentials, and other identifier objects controlled, such that user IDs are implemented only as authorized (including with specified privileges).
User identity is verified before performing password resets for user requests made via a non-face-to-face method (for example, phone, e-mail, or web).
First-time and reset passwords will set to a unique value for each user, and each user must change their password immediately after the first use.
Access for any terminated users is immediately deactivated or removed.
Inactive user accounts over 90 days old will either be removed or disabled.
Accounts used by vendors for remote access, maintenance or support is enabled only during the time period needed.
Vendor remote access accounts is monitored when in use.
Authentication procedures and policies is communicated to all users who have access to cardholder data.

b. Group, shared, or generic accounts and passwords, or other authentication methods, are prohibited as follows:
Generic user IDs and accounts are disabled or removed.
Shared user IDs for system administration activities and other critical functions do not exist.
Shared and generic user IDs are not used to administer any system components.

c. User passwords are changed at least every 90 days.

d. A minimum password length of at least seven characters is required.

e. Passwords will contain both numeric and alphabetic characters.

f. An individual must submit a new password that is different from any of the last four passwords he or she has used.
g. Repeated access attempts is limited by locking out the user ID after no more than six attempts.
h. Once a user account is locked out, the lockout duration is set to a minimum of 30 minutes or until administrator enables the user ID.
i. A session that has been idle for more than 15 minutes, users are required to re-authenticate (for example, re-enter the password) to re-activate the terminal or session.
j. All access to any database containing cardholder data is authenticated.
k. All user access to, user queries of, and user actions on (for example, move, copy, delete), the database through programmatic methods only (for example, through stored procedures).
l. User direct access or queries to databases is restricted to database administrators.
m. Application IDs with database access will only be able to be used by the applications (and not by individual users or other processes).

8.6

a. Where other authentication mechanisms are used the following mechanisms must be used: Authentication mechanisms must be assigned to an individual account and not shared across multiple accounts. Physical and/or logical controls must be in place to ensure only the intended account can use that mechanism to gain access.

8.7

a. Access to any database containing cardholder data is restricted as per PCI DSS 3.1 requirements.

Requirement 9: Restrict physical access to cardholder data.

9.1

a. Appropriate facility entry controls is in place to limit and monitor physical access to systems in the cardholder data environment.
b. Video cameras and/or access-control mechanisms are in place to monitor individual physical access to sensitive areas.
c. Video cameras and/or access-control mechanisms are protected from tampering or disabling.
d. Data collected from video cameras and/or access control mechanisms are reviewed and correlated with other entries, and data is stored for at least three months, unless otherwise restricted by law.
e. Physical access to publicly accessible network jacks is restricted.
f. Physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunication lines is restricted.

9.2

a. Procedures are developed to easily distinguish between onsite personnel and visitors, as follows:

Processes and procedures for assigning badges to onsite personnel and visitors include the following:
Granting new badges.
Changing access requirements.
Revoking terminated onsite personnel and expired visitor badges.

Access to the badge system is limited to authorized personnel.
Badges will clearly identify visitors and easily distinguish between onsite personnel and visitors.

9.3

a. Visitors is authorized before entering areas where cardholder data is processed or maintained.
b. Visitors are given a physical token (for example, a badge or access device) that identifies the visitors as not onsite personnel.
c. Visitor badges will expire.
d. Visitors are asked to surrender the physical token before leaving the facility or upon expiration.

9.4

a. A visitor log is in use to record physical access to the facility as well as for computer rooms and data centers where cardholder data is stored or transmitted.
b. The visitor log contain the visitor's name, the firm represented, and the onsite personnel authorizing physical access, and is the visitor log retained for at least three months.

9.5

a. Media back-ups are stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility.
b. This location's security is reviewed at least annually.

9.6

a. All media is physically secured (including but not limited to computers, removable electronic media, paper receipts, paper reports, and faxes).

9.7

a. Strict control is maintained over the internal or external distribution of any kind of media.
b. Controls include the following:

Media is classified so the sensitivity of the data can be determined.
Media that is sent by secured courier or other delivery method that can be accurately tracked.

9.8

a. Logs are maintained to track all media that is moved from a secured area, and management approval obtained prior to moving the media (especially when media is distributed to individuals).

9.9

a. Strict control is maintained over the storage and accessibility of media.
b. Inventory logs of all media properly are maintained and periodic media inventories are conducted at least annually.

9.10

a. Hardcopy materials are cross-cut shredded, incinerated, or pulped so that cardholder data cannot be reconstructed.
b. Containers that store information to be destroyed are secured to prevent access to the contents.
c. Cardholder data on electronic media are rendered unrecoverable via a secure wipe program in accordance with industry-accepted standards for secure deletion, or otherwise by physically destroying the media (for example, degaussing), so that cardholder data cannot be reconstructed.

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

10.1

a. A process is in place to link all access to system components (especially access done with administrative privileges such as root) to each individual user.

10.2

a. Automated audit trails implemented for all system components to reconstruct the following 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 object.

10.3

a. Are the following audit trail entries recorded for all system components for each event:
User identification.
Type of event.
Date and time.
Success or failure indication.
Origination of event.
Identity or name of affected data, system component, or resource.

10.4

a. All critical system clocks and times are synchronized through use of time synchronization technology, and is the technology kept current.

b. The following controls implemented for acquiring, distributing, and storing time:
Only designated central time servers receive time signals from external sources, and all critical systems have the correct and consistent time, based on International Atomic Time or UTC.
Designated central time servers peer with each other to keep accurate time, and other internal servers only receive time from the central time servers.

c. Time and date are protected as follows:
Access to time data is restricted to only personnel with a business need to access time data.
Changes to time settings on critical systems are logged, monitored, and reviewed.

d. Time settings received from specific, industry-accepted time sources.

10.5

a. Audit trails secured so they cannot be altered, as follows:
Viewing of audit trails is limited to those with a job-related need.
Audit trail files are protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation.
Audit trail files are promptly backed up to a centralized log server or media that is difficult to alter.
Logs for external-facing technologies (for example, wireless, firewalls, DNS, mail) offloaded or copied onto a secure, centralized log server or media on the internal LAN.
File-integrity monitoring or change-detection software are used 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

a. Logs for all system components reviewed at least daily, and follow-ups to exceptions are required.

10.7

a. Audit log retention policies and procedures are in place and do require that audit trail history is retained for at least one year.
b. Audit logs are available for at least one year and processes are in place to immediately restore at least the last three months' logs for analysis.

Requirement 11: Regularly test security systems and processes.

11.1

a. A documented process implemented to detect and identify wireless access points on a quarterly basis.
b. The methodology to detect and identify any unauthorized wireless access points, including at least the following:
WLAN cards inserted into system components.
Portable wireless devices connected to system components (for example, by USB, etc.).
Wireless devices attached to a network port or network device.
c. The process to identify unauthorized wireless access points is performed at least quarterly for all system components and facilities.
d. Automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.), monitoring is configured to generate alerts to personnel.
e. The Incident Response Plan (Requirement 12.9) includes a response in the event unauthorized wireless devices are detected.

11.2

a. Internal and external network vulnerability scans run 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), as follows:
Quarterly internal vulnerability scans are performed.
The quarterly internal scan process include rescans until passing results are obtained, or until all "High" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
Internal quarterly scans are performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV).
b. Quarterly external vulnerability scans are performed.
c. External quarterly scan results do satisfy the ASV Program Guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures).
d. Quarterly external vulnerability scans performed by an Approved Scanning Vendor (ASV), are approved by the Payment Card Industry Security Standards Council (PCI SSC).

e. Internal and external scans are performed after any significant change (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).
f. The scan process include rescans until:
For external scans, no vulnerabilities exist that are scored greater than a 4.0 by the CVSS
For internal scans, a passing result is obtained or all ""High"" vulnerabilities as defined in PCI DSS Requirement 6.2 are resolved.
g. Scans are performed by a qualified internal resource(s) or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV).

11.3

a. External and internal penetration testing is performed at least once a year and after any significant infrastructure or application changes (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment).
b. Noted exploitable vulnerabilities are corrected and testing repeated.
c. Tests are performed by a qualified internal resource or qualified external third party, and if applicable, does organizational independence of the tester exist (not required to be a QSA or ASV). These penetration tests include the following:
Network-layer penetration tests.
Application-layer penetration tests.

11.4

a. Intrusion-detection systems and/or intrusion-prevention systems are used to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment.
b. IDS and/or IPS are configured to alert personnel of suspected compromises.
c. All intrusion-detection and prevention engines, baselines, and signatures are kept up-to-date.

11.5

a. File-integrity monitoring tools are deployed within the cardholder data environment.
b. The tools are configured to alert personnel to unauthorized modification of critical system files, configuration files or content files, and the tools perform critical file comparisons at least weekly.

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

12.1

a. A security policy is established, published, maintained, and disseminated to all relevant personnel.

b. The policy addresses all PCI DSS requirements.
c. An annual risk assessment process is documented that identifies threats and vulnerabilities, and results in a formal risk assessment.
d. The risk assessment process is performed at least annually.
e. The information security policy is reviewed at least once a year and updated as needed to reflect changes to business objectives or the risk environment.

12.2

a. Daily operational security procedures are developed that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures), and do they include administrative and technical procedures for each of the requirements.

12.3

a. Usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage) are developed to define proper use of these technologies for all employees and contractors.

b. Explicit approval by authorized parties to use the technologies is required.
c. Authentication for use of the technology is required.
d. A list of all such devices and personnel with access is kept.
e. Labeling of devices to determine owner, contact information, and purpose is required.
f. Acceptable uses of the technologies is required.
g. Acceptable network locations for the technologies is required.
h. List of company-approved products is required.
i. Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity is required.
j. Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use is required.
k. Personnel accessing cardholder data via remote-access technologies, the prohibition of copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need, all require policies.
l. For personnel with proper authorization, policy requires the protection of cardholder data in accordance with PCI DSS Requirements.

12.4

a. The security policy and procedures clearly define information security responsibilities for all personnel.

12.5

a. Responsibility for information security is formally assigned to a Chief Information Security Officer.

b. The following information security management responsibilities are formally assigned to an individual or team:
Establishing, documenting, and distributing security policies and procedures.
Monitoring and analyzing security alerts and information, and distributing to appropriate personnel.
Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations.
Administering user accounts, including additions, deletions, and modifications.
Monitoring and controlling all access to data.

12.6

a. A formal security awareness program is in place to make all personnel aware of the importance of cardholder data security.

b. A formal security awareness program is in place to make all employees aware of the importance of cardholder data security.

c. The security awareness program provides multiple methods of communicating awareness and educating personnel.

d. Personnel are educated upon hire and at least annually.

e. Personnel are required to acknowledge, at least annually, that they have read and understood the security policy and procedures.

12.7

a. Potential personnel (see definition of ""personnel"" at Requirement 12.1, above) are screened prior to hire to minimize the risk of attacks from internal sources.

12.8

a. If cardholder data is shared with service providers, are policies and procedures maintained and implemented to manage service providers, as follows:
A list of service providers is maintained.
A written agreement is maintained that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.
There is an established process for engaging service providers, including proper due diligence prior to engagement.
A program is maintained to monitor service providers' PCI DSS compliance status at least annually.

12.9

a. An incident response plan has been implemented in preparation to respond immediately to a system breach, as follows:
   An incident response plan been created to be implemented in the event of system breach.
   The plan address, at a minimum:
      Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands.
      Specific incident response procedures.
      Business recovery and continuity procedures.
      Data back-up 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.
b. The plan tested at least annually.
c. Specific personnel designated to be available on a 24/7 basis to respond to alerts.
d. Appropriate training is provided to staff with security breach response responsibilities.
e. Alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems are included in the incident response plan.
f. A process developed and placed to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

Revision History

Version	Published	Author	Description
1.0	2014/06/18	Matt Langford	Original publication.
1.1	2014/06/19	Matt Langford	Minor revisions
1.2	2015/07/21	Matt Langford	Update to DSS 3.1