

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

I. Introduction:

This standard provides requirements and guidance for all credit card processing activities for Purdue University. E-Commerce/Credit Card Operations (ECCO) must approve all credit card processing activities at the Purdue University prior to a unit entering into any contracts or purchasing equipment for such processing. This requirement applies regardless of the transaction method used (e.g. online processing, outsourced to a third party, or swipe terminals). Units that wish to engage in credit card processing must obtain approval for the processing and must meet the Payment Card Industry (PCI) Data Security Standard (DSS) requirements for processing credit card information

The PCI DSS is a set of information security standards designed by credit card companies to protect consumer credit card information and transactions. The PCI DSS applies to any entity, whether merchant or service provider, that store, processes or transmits cardholder account and/or transaction information. The PCI DSS offers a single approach to safeguarding sensitive cardholder data for all credit card issuers. The PCI Data Security Standard identifies twelve basic security requirements for cardholder transactions.

There are four levels of merchant compliance validation with the PCI DSS. Currently, Purdue University is classified as level 4. This level is subject to change based upon the volume of credit card transactions handled at the University, as well as the amount of potential risks to cardholder data, and any data exposures experienced by the University.

II. Credit Card Acceptance Guidelines

This policy governs the acceptance of credit cards (e.g. Visa, MasterCard, American Express, and Discover) by the University. Being able to provide this payment option to students, staff, parents, alumni, donors and the general public does however, come with significant responsibility to maintain cardholders' security and to mitigate the risk of fraud. The University, as a merchant, must adhere to strict security guidelines established by the Payment Card Industry or face significant financial penalties. In addition to such penalties, any compromise of cardholder information undermines public confidence in the University's ability to maintain appropriate stewardship over confidential information entrusted to it. Lack of compliance in a single area of the University could jeopardize the University's ability to accept credit cards in any area. Hence, all departments and units accepting payment cards must abide by this policy.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- a. Merchant Approval – University departments and units must receive approval prior to accepting credit and debit cards. Approval is granted by the University Comptroller through the Ecommerce and Credit Card Operations office (ECCO). Once approved, ECCO works with the University’s Treasury Operations Office and our contracted processor to establish the needed merchant accounts. ECCO also work with the department or unit to ensure user training takes place, and all other requirements are met before payment cards may be accepted.
- b. Merchant Card Acceptance – Once merchant accounts are established for an t area, the merchant has an ongoing responsibility to understand security requirements, comply with PCI DSS standards, and to maintain proper business practices. Merchants are responsible for paying all fees and other costs associated with accepting credit cards, including internal fees for administering the University’s compliance program.
- c. Compliance with PCI DSS Standards – The University is committed to protecting confidential cardholder information. Merchants accepting credit cards are expected to adhere to these standards, which are updated periodically, and to enforce the compliance of third party service providers. They are also required to attend training and periodic refresher training necessary to understand and stay current with these standards.
- d. The University Comptroller, through E-commerce and Credit Card Operations; and the Office of Information Technology at Purdue (ITAP) , through its ITaP IT Networks and Security (ITNS) group have been assigned responsibility for assessing, determining, and monitoring compliance with these standards. As a result, responsibility for determining how to apply these standards and for assessing deficiencies is shared among these areas.
- e. Sanctions for Non-Compliance – University departments or units that transact business using credit cards in a manner that deviates from this policy are subject to various financial and other sanctions. These may include termination of merchant accounts, financial penalties and costs associated with a security breach, penalties and costs associated with bringing a non-compliant application into compliance, and/or possible disciplinary action of the staff involved - up to and including termination of employment.
- f. Use of Third Party Software – The University has spent considerable time and resources partnering with Touchnet and evaluating various third party solutions to meet unique business needs. Departments and units whose needs cannot be met through these pre-approved applications must request prior approval from ECCO before considering or acquiring third party solutions. A written agreement acknowledging service provider’s responsibility for the security of cardholder

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

data that they maintain. Third party vendors must provide proof of PCI DSS/PA DSS compliance.

- g. Engagement of Service Providers - This process is coordinated by ECCO and the merchant area will work in conjunction with the manager and other areas of the University process as appropriate regarding engagement including University Contracting, Treasury Operations, and Internal Audit. An ongoing program to monitor service provider's compliancy status is performed by ECCO.
- h. Hosting Servers- Payment card related websites or software owned or managed by a university department or unit must be hosted on a server certified by a qualified security assessor as well as the ITNS team.
- i. Secure Transmissions – To ensure that proper business practices and security are maintained, only secure and approved processes are allowable for transmitting payment card information. Any unapproved processes, including email, are not allowed to transmit or store payment card information.
- j. Security Breaches – All known or suspected security breaches of cardholder information must be reported immediately to ITNS and ECCO. Please see Information Technology Incident Response (V.1.4) for additional reporting requirements. Departments and units must cooperate fully with any resulting investigation.

http://www.purdue.edu/policies/pages/information_technology/v_1_4.html

Forms and procedures for obtaining approval for credit card acceptance can be found on the ECCO web page at: <http://www.purdue.edu/ECCO/> Questions regarding this process can be emailed to the Manager of ECCO at ecco@purdue.edu or call 765-496-7873.

III. Compliance Validation:

Any unit that engages in any type of credit card processing is responsible for ensuring appropriate compliance with this standard on University IT Resources within that unit's area of responsibility. Units are also responsible for documenting appropriate compliance with this standard on University IT Resources within their areas of responsibility. Documentation should include how PCI DSS requirements are being met in a particular area or what types of compensating controls are in place. Documented processes should be periodically reviewed to ensure continued compliance with this standard.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

Documentation regarding compliance with this standard is required by ECCO and may be required by third party payment card industry assessors. Any unit accepting credit cards is also required to comply with ECCO or ITNS requests for information in order to respond to requests from external compliance validation requests from third party assessors.

Units processing credit card data must be able to document compliance by completing a self-assessment questionnaire that is appropriate for the manner in which they acquire, process, transmit and store credit card data. The appropriate validation type for each merchant is determined according to the following guidelines:

- SAQ A – Card-not-present merchants, all cardholder data functions outsourced
- SAQ B – Imprint-only or stand-alone dial-up terminal merchants with no electronic cardholder data storage
- SAQ C – Merchants with payment application systems connected to the Internet with no electronic cardholder data storage
- SAQ D – All other merchants not included in descriptions of SAQ A, B or C above

- IV. Purdue maintains an active security policy that addresses specific PCI DSS policy standards. All employees and contractors should become familiar with the University Standards.

Purdue's security policy pertaining to PCI DSS requirements may be located at:
http://www.purdue.edu/policies/pages/information_technology/info_tech.html .

The following individual policies are specific to the PCI DSS requirements:

- [Authentication and Authorization \(V.1.2\)](#)
- [Data Security and Access Policy \(C-34\)](#)
- [Delegation of Administrative Authority and Responsibility For Information Assurance, Security and Awareness \(V.1.1\)](#)
- [Incident Response \(V.1.4\)](#)
- [Privacy for Electronic Information \(V.1.3\)](#)
- [Proper Disposal of Electronic Media \(V.1.5\) Interim](#)
- [Remote Access to IT Resources \(V.1.6\) Interim](#)

- v. PCI Requirements and Purdue Processes:

The PCI DSS has very specific requirements that must be followed in order to protect cardholder data. The PCI DSS requirements apply only to the systems that process, store, or transmit credit card data. These requirements are grouped into specific themes of controls.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

Following the recitation of each PCI DSS requirement is language regarding Purdue specific procedures and processes that can be utilized in order to meet the PCI DSS requirement. The PCI DSS requirements are very detailed; and are referenced by via subheadings only in this standard. The complete list of PCI DSS requirements can be found at:

<https://www.pcisecuritystandards.org/index.htm>

Build and Maintain a Secure Network

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

- 1.1 Establish firewall and router configuration standards that include the following:
 - 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations
 - 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks
 - 1.1.3 Requirements for a firewall at each internet connection and between any demilitarized zone (DMZ) and the internal network zone
 - 1.1.4 Description of groups, roles and responsibilities for logical management of network components
 - 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure
 - 1.1.6 Requirements to review firewall and router rule sets at least every six months
- 1.2 Build a firewall configuration that restricts connections between untrusted networks and any systems components in the cardholder environment
 - 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment
 - 1.2.2 Secure and synchronize router configuration files.
 - 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment and configure these firewalls 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 Prohibit direct public access between the Internet and any system component in the cardholder data environment
 - 1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment
 - 1.3.2 Limit inbound Internet traffic to addresses within the DMZ
 - 1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ
- 1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ
- 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only "established" connections are allowed into the network.)
- 1.3.7 Place the database in an internal network zone, segregated from the DMZ
- 1.3.8 Implement IP masquerading to prevent internal addresses from being translated and revealed on the Internet, using RFC 1918 address space. Use network address translation (NAT) technologies—for example, port address translation (PAT).
- 1.4 Install personal firewall software 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.

Build and Maintain a Secure Network

Requirement 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—for example, include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.
 - 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. Ensure wireless device security settings are enabled for strong encryption technology for authentication and transmission.
- 2.2 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.
 - 2.2.1 Implement only one primary function per server.
 - 2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).
 - 2.2.3 Configure system security parameters to prevent misuse.
 - 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- 2.3 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
- 2.4 Shared hosting providers must protect each entity's hosted environment and cardholder data. These providers must meet specific requirements as detailed in Appendix A: Additional PCI DSS Requirements for Shared Hosting Providers.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

- 3.1 Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.
- 3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3:
 - 3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, contained in a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.
 - 3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions. Note: See PCI DSS Glossary of Terms, Abbreviations, and Acronyms for additional information.
 - 3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.
- 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed). Notes:

This requirement does not apply to employees and other parties with a legitimate business need to see the full PAN.

This requirement does not supersede stricter requirements in place for displays of cardholder data—for example, for point-of-sale (POS) receipts
- 3.4 Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs) by using any of the following approaches:
 - One-way hashes based on strong cryptography
 - Truncation
 - Index tokens and pads (pads must be securely stored)
 - Strong cryptography with associated key-management processes and procedures
- 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.
- 3.5 Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse:
 - 3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.
 - 3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.
- 3.6 Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following:

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 3.6.1 Generation of strong cryptographic keys
- 3.6.2 Secure cryptographic key distribution
- 3.6.3 Secure cryptographic key storage
- 3.6.4 Periodic cryptographic key changes, as deemed necessary and recommended by the associated application (for example, re-keying); preferably automatically; at least annually
- 3.6.5 Retirement or replacement of old or suspected compromised cryptographic keys
- 3.6.6 Split knowledge and establishment of dual control of cryptographic keys
- 3.6.7 Prevention of unauthorized substitution of cryptographic keys
- 3.6.8 Requirement for cryptographic key custodians to sign a form stating that they understand and accept their key-custodian responsibilities

Protect Cardholder Data

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

- 4.1 Use strong cryptography and security protocols such as SSL/TLS or IPSEC to safeguard sensitive cardholder data during transmission over open, public networks. Examples of open, public networks that are in scope of the PCI DSS are:
 - o The Internet,
 - o Wireless technologies,
 - o Global System for Mobile communications (GSM), and
 - o General Packet Radio Service (GPRS).
- 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (for example, IEEE 802.11i) to implement strong encryption for authentication and transmission.

For new wireless implementations, it is prohibited to implement WEP after March 31, 2009.
For current wireless implementations, it is prohibited to use WEP after June 30, 2010.
- 4.2 Never send unencrypted PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat).

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

- 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).
- 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 5.2 Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.

Maintain a Vulnerability Management Program

Requirement 6: Development and maintain secure systems and applications

- 6.1 Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release. Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less critical devices and systems within three months.
- 6.2 Establish a process to identify newly discovered security vulnerabilities (for example, subscribe to alert services freely available on the Internet). Update configuration standards as required by PCI DSS Requirement 2.2 to address new vulnerability issues.
- 6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle. These processes must include the following:
- 6.3.1 Testing of all security patches, and system and software configuration changes before deployment, including but not limited to the following:
- 6.3.1.1 Validation of all input (to prevent cross-site scripting, injection flaws, malicious file execution, etc.)
 - 6.3.1.2 Validation of proper error handling
 - 6.3.1.3 Validation of secure cryptographic storage
 - 6.3.1.4 Validation of secure communications
 - 6.3.1.5 Validation of proper role-based access control (RBAC)
- 6.3.2 Separate development/test and production environments
- 6.3.3 Separation of duties between development/test and production environments
- 6.3.4 Production data (live PANs) are not used for testing or development
- 6.3.5 Removal of test data and accounts before production systems become active
- 6.3.6 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers
- 6.3.7 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability

Note: This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development life cycle required by PCI DSS Requirement 6.3. 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

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

implementation, as defined at PCI DSS Requirement 6.6.

- 6.4 Follow change control procedures for all changes to system components. The procedures must include the following:
 - 6.4.1 Documentation of impact
 - 6.4.2 Management sign-off by appropriate parties
 - 6.4.3 Testing of operational functionality
 - 6.4.4 Back-out procedures
- 6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following: Note: The vulnerabilities listed at 6.5.1 through 6.5.10 were current in the OWASP guide when PCI DSS v1.2 was published. However, if and when the OWASP guide is updated, the current version must be used for these requirements.
 - 6.5.1 Cross-site scripting (XSS)
 - 6.5.10 Failure to restrict URL access
 - 6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.
 - 6.5.3 Malicious file execution
 - 6.5.4 Insecure direct object references
 - 6.5.5 Cross-site request forgery
 - 6.5.6 Information leakage and improper error handling
 - 6.5.7 Broken authentication and session management
 - 6.5.8 Insecure cryptographic storage
 - 6.5.9 Insecure communications
- 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:
 - Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes
 - Installing a web-application firewall in front of public-facing web applications

Implement Strong Access Control Measures

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

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:
 - 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
 - 7.1.2 Assignment of privileges is based on individual personnel's job classification and function
 - 7.1.3 Requirement for an authorization form signed by management that specifies required privileges
 - 7.1.4 Implementation of an automated access control system
- 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. This access control system must include the following:
 - 7.2.1 Coverage of all system components
 - 7.2.2 Assignment of privileges to individuals based on job classification and function
 - 7.2.3 Default — "deny-all" setting

Implement Strong Access Control Measures

Requirement 8: Assign a unique ID to each person with computer access

- 8.1 Assign all users a unique ID before allowing them to access system components or cardholder data.
- 8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:
 - Password or passphrase
 - Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)
- 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.
- 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography (defined in PCI DSS Glossary of Terms, Abbreviations, and Acronyms).
 - 8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.
 - 8.5.10 Require a minimum password length of at least seven characters.
 - 8.5.11 Use passwords containing both numeric and alphabetic characters.
 - 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.
 - 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.
- 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-enter the password to re-activate the terminal.
- 8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users.
- 8.5.2 Verify user identity before performing password resets.
- 8.5.3 Set first-time passwords to a unique value for each user and change immediately after the first use.
- 8.5.4 Immediately revoke access for any terminated users.
- 8.5.5 Remove/disable inactive user accounts at least every 90 days.
- 8.5.6 Enable accounts used by vendors for remote maintenance only during the time period needed.
- 8.5.7 Communicate password procedures and policies to all users who have access to cardholder data.
- 8.5.8 Do not use group, shared, or generic accounts and passwords.
- 8.5.9 Change user passwords at least every 90 days.

Implement Strong Access Control Measures

Requirement 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.
 - 9.1.1 Use video cameras or other access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law. Note: Sensitive areas refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.
 - 9.1.2 Restrict physical access to publicly accessible network jacks.
 - 9.1.3 Restrict physical access to wireless access points, gateways, and handheld devices.
- 9.10 Destroy media containing cardholder data when it is no longer needed for business or legal reasons as follows:
 - 9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.
 - 9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.
- 9.2 Develop procedures to help all personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. For purposes of this requirement:
 - Employee refers to full-time and part-time employees, temporary employees and personnel, and

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

contractors and consultants who are resident on the entity's site.

- Visitor is defined as a vendor, guest of an employee, service personnel, or anyone who needs to enter the facility for a short duration, usually not more than one day.

- 9.3.1 Authorized before entering areas where cardholder data is processed or maintained
- 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as non-employee
- 9.3.3 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 activity. Document the visitor's name, the firm represented, and the employee authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.
- 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or back-up site, or a commercial storage facility. Review the location's security at least annually.
- 9.6 Physically secure all paper and electronic media that contain cardholder data.
- 9.7 Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data, including the following:
 - 9.7.1 Classify the media so it can be identified as confidential.
 - 9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.
- 9.8 Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals).
- 9.9 Maintain strict control over the storage and accessibility of media that contains cardholder data.
 - 9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.

Regularly Monitor and Test Networks

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

- 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.
 - 10.2.1 All individual accesses to cardholder data
 - 10.2.2 All actions taken by any individual with root or administrative privileges
 - 10.2.3 Access to all audit trails
 - 10.2.4 Invalid logical access attempts
 - 10.2.5 Use of identification and authentication mechanisms
 - 10.2.6 Initialization of the audit logs

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 10.2.7 Creation and deletion of system-level objects
- 10.3.1 User identification
- 10.3.2 Type of event
- 10.3.3 Date and time
- 10.3.4 Success or failure indication
- 10.3.5 Origination of event
- 10.3.6 Identity or name of affected data, system component, or resource
- 10.4 Synchronize all critical system clocks and times.
- 10.5 Secure audit trails so they cannot be altered.
 - 10.5.1 Limit viewing of audit trails to those with a job-related need.
 - 10.5.2 Protect audit trail files from unauthorized modifications.
 - 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
 - 10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
 - 10.5.5 Use file-integrity monitoring or change-detection software 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 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion-detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). Note: Log harvesting, parsing, and alerting tools may be used to meet compliance with Requirement 10.6
- 10.7 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 back-up).

Regularly Monitor and Test Networks

Requirement 11: Regularly test security systems and processes

- 11.1 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.
- 11.2 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). Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.
- 11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

must include the following:

- 11.3.1 Network-layer penetration tests
- 11.3.2 Application-layer penetration tests
- 11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.
- 11.5 Deploy 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. Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise. File-integrity monitoring products usually come pre-configured with critical files for the related operating system. Other critical files, such as those for custom applications, must be evaluated and defined by the entity (that is, the merchant or service provider).

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

- 12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:
 - 12.1.1 Addresses all PCI DSS requirements.
 - 12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.
 - 12.1.3 Includes a review at least once a year and updates when the environment changes.
- 12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).
- 12.3 Develop 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 usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:
 - 12.3.1 Explicit management approval
 - 12.3.10 When accessing cardholder data via remote-access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media.
 - 12.3.2 Authentication for use of the technology
 - 12.3.3 A list of all such devices and personnel with access
 - 12.3.4 Labeling of devices with owner, contact information, and purpose
 - 12.3.5 Acceptable uses of the technology
 - 12.3.6 Acceptable network locations for the technologies

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

- 12.3.7 List of company-approved products
- 12.3.8 Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity
- 12.3.9 Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use
- 12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.
- 12.5.1 Establish, document, and distribute security policies and procedures.
- 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.
- 12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.
- 12.5.4 Administer user accounts, including additions, deletions, and modifications
- 12.5.5 Monitor and control all access to data.
- 12.6 Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.
- 12.6.1 Educate employees upon hire and at least annually.
- 12.6.2 Require employees to acknowledge at least annually that they have read and understood the company's security policy and procedures.
- 12.7 Screen potential employees (see definition of —employee at 9.2 above) prior to hire to minimize the risk of attacks from internal sources. For those employees such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.
- 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:
 - 12.8.1 Maintain a list of service providers.
 - 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.
 - 12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.
 - 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status.
- 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum; Specific incident response procedures; Business recovery and continuity procedures; Data back-up processes;

MERCHANT CARD ACCEPTANCE GUIDELINES AND SECURITY REQUIREMENTS

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

- 12.9.2 Test the plan at least annually.
- 12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.
- 12.9.4 Provide appropriate training to staff with security breach response responsibilities.
- 12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.
- 12.9.6 Develop process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.

DRAFT