

General Standards for Payment Card Environments at Miami University

1. Install and maintain a firewall configuration to protect cardholder data and its environment

Cardholder databases, applications, servers, and the networks and equipment that cardholder data traverses must be protected as follows:

- Networking must establish a formal process for approving and testing all external network connections and changes to the firewall and router configurations.
- Networking must maintain current network diagrams with all connections to cardholder data environment, including any wireless networks.
- Networking must create a network architecture that includes a firewall at each internet connection and a firewall between any demilitarized zone (DMZ) in the cardholder data environment and the internal network zone holding cardholder data.
- Networking must maintain a description of groups, roles, and responsibilities for logical management of network components.
- Networking together with Security Engineering must maintain 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.
- The ISO will engage Networking, together with Security Engineering to review firewall and router rule sets at least every six months.

The firewall configuration protecting the cardholder data environment must restrict connections between untrusted networks and any system in the cardholder data environment as follows:

- Inbound and outbound traffic shall be restricted to that which is necessary for the cardholder data environment.
- Router configuration files shall be secured and synchronized for consistency of parameters.
- Wireless networks shall be isolated from the cardholder data environment through firewall rules that deny all traffic between the two; an exception to this standard is that secure http (https) is permitted over wireless to web servers in the DMZ.

The firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- A DMZ shall be implemented to limit inbound and outbound traffic only to protocols that are necessary for the cardholder environment.
- Traffic inbound from the internet to the cardholder environment shall be limited to IP addresses within the DMZ.
- Direct routes for inbound or outbound traffic between the Internet and the cardholder data environment shall be prohibited; rather traffic shall be indirect through the DMZ.
- Internal addresses shall be prohibited from passing from the Internet into the DMZ.
- Traffic outbound from the cardholder data environment to the Internet shall be restricted such that outbound traffic can only access IP addresses within the DMZ.
- Stateful inspection (i.e. dynamic packet filtering) shall be implemented such that only established connections are allowed into the cardholder networks.
- Databases holding cardholder data shall be placed in an internal network zone, segregated from the DMZ.
- IP-masquerading using RFC 1918 address space must be implemented to prevent internal addresses from being translated and revealed on the Internet.

Personal firewall software must be installed on any mobile and/or employee-owned computers which have both direct connectivity to the Internet and connectivity to cardholder data of Miami's customers.

2. Vendor-supplied defaults for system passwords and other security parameters must be changed as follows:

Vendor-supplied defaults must be changed before installing a system on the network. Examples include passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

Except for retail access through web servers, wireless access is not permitted to the cardholder environment.

Configuration standards must be developed for all system components, these standards must address security vulnerabilities in a way that is consistent with industry-accepted system hardening standards such as SANS, NIST, and CIS. Controls must be in place to ensure the following:

- Only one primary function (eg database server, application server, web server) may be implemented per server.
- Services and protocols not directly needed to perform a device's specific function must be disabled. Insecure services and protocols must be disabled.
- System security parameters must be configured to prevent misuse.
- Functionality that is unnecessary (such as scripts, drivers, features, subsystems, file systems, and web servers) shall be removed

Administrative access not performed at the console must be encrypted using technologies such as SSH, VPN, or SSL/TLS.

3. Protect stored cardholder data

Storage of cardholder data must be kept to a minimum; storage amount and retention time must be limited to that which is required for business, legal, and/or regulatory purposes. Data-retention and disposal standards must be in place to specify the limitations of this minimum. Data retention is to be in accordance with our records retention policy.

Systems must adhere to the following requirements regarding storage of sensitive authentication data after authorization (even if encrypted).

- Do not store the full contents of any track from the magnetic strip located on the back of a card, contained in a chip, or elsewhere.
- Do not store the card-validation 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.
- Do not store the personal identification number (PIN) or the encrypted PIN block.

The PAN must be masked when displayed to persons who do not need to see it; unless there is a business need to know, the first six and the last four digits are the maximum number of digits that may be displayed.

The PAN must be rendered unreadable anywhere it is stored (including data on portable digital media, backup media, and in logs) by using any of the following approaches:

- If disk encryption (rather than file- or column-level database encryption) is used: logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases) and decryption keys must be independent of user accounts.

Cryptographic keys used for encryption of cardholder data must be protected against both disclosure and misuse.

- Access to cryptographic keys must be restricted to the fewest number of custodians necessary for business continuity.
- Cryptographic keys must be stored securely, and in the fewest possible locations and formats.

Key-management processes and procedures for cryptographic keys used for encryption of cardholder data must be fully documented and implemented. These key management processes must include the following:

- Generation of strong cryptographic keys
- Secure cryptographic key distribution
- Secure cryptographic key storage
- Periodic changing of cryptographic keys: As deemed necessary and recommended by the associated application (for example, re-keying), preferably automatically
- Retirement or replacement of old or suspected compromised cryptographic keys
- Split knowledge and establishment of dual control of cryptographic keys
- Prevention of unauthorized substitution of cryptographic keys
- Requirement for cryptographic-key custodians to sign a form stating that they understand and accept their key-custodian responsibilities

4. Transmission of cardholder data across open, public networks must be encrypted as follows:

Strong cryptography and security protocols, such as SSL/TLS or IPSEC, must be used to safeguard sensitive cardholder data during transmission over open, public networks. Open public networks include the internet, wireless technologies, Global System for Mobile Communication (GSM) and General Packet Radio Service (GPRS).

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission of cardholder data over open, public networks. Note: For new wireless implementation, it is prohibited to Implement WEP after March 31, 2009. For current wireless implementations, it is prohibited to use WEP after June 30, 2010.

Unencrypted PANs may not be sent over end-user messaging technologies such as e-mail, instant messaging, and chat unless that technology is specifically endorsed in writing by the ISO.

5. Anti-virus software must be used and updated in the cardholder data environment as follows:

Anti-virus software must be deployed on all systems in the cardholder data environment, particularly personal computers and servers that are commonly affected by malicious software. Anti-virus programs must be capable of detecting, removing, and protecting against all known types of malicious software. Anti-virus mechanisms must be current, actively running, and capable of generating audit logs.

6. Develop and maintain secure systems and applications for the cardholder environment

System components and software within the cardholder environment must have the latest vendor-supplied security patches installed within the following boundaries: a) security patches marked 'critical' by the vendor must be installed within one month of release. b) security patches not marked 'critical' by the vendor must be installed within three months of release. c) exceptions to these time frames may be granted in writing by the ISO following a risk based justification.

A process (such as subscription to alert services) must be in place to identify newly discovered security vulnerabilities. Configuration standards must be updated as required by PCI DSS Requirement 2.2 to address new vulnerability issues.

Development of applications that process cardholder data is not permitted. Creation of web pages that call cardholder sites through a secure link is not considered development.

For public-facing web applications involving cardholder data, new threats and vulnerabilities must be addressed on an ongoing basis and protected against known attacks by applying either of the following methods: a) Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or b) Installing a web-application layer firewall in front of public-facing web applications.

7. Restrict access to cardholder data by business need-to-know

Access to system components and cardholder data must be limited to those individuals whose jobs require such access. Access limitations must include the following:

- Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities.
- Assignment of privileges based on individual personnel's job classification and function.
- Requirement for an authorization form signed by management that specifies required privileges.
- Implementation of an automated access control system.

An access control system must be in place for systems with multiple users to restrict access based on a user's need to know, and it must be set to "deny all" unless specifically allowed. This access control system must include the following:

- Coverage of all system components.
- Assignment of privileges to individuals based on job classification and function.
- Default "deny-all" setting.

8. Assign a unique ID to each person with computer access to cardholder data

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

In addition to assigning a unique ID, one or more of the following methods must be employed to authenticate all users. Password or passphrase or two-factor authentication (for example: token devices, smart cards, biometrics, or public keys).

Two-factor authentication must be incorporated for network access originating from outside the cardholder data network to the cardholder data network by employees, administrators, and third parties. Technologies such as remote authentication and dial-in service (RADIUS) or terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates satisfy this requirement.

Passwords must be rendered unreadable using strong cryptography during transmission and storage on all cardholder system components. Strong cryptography is defined in PCI DSS and PA-DSS Glossary of Terms, Abbreviations, and Acronyms.

Proper user authentication and password management controls must be in place for non-consumer users and administrators on all cardholder system components as follow:

- Addition, deletion, and modification of user ID's credentials, and other identifier objects must be controlled.
- User identity must be verified before performing password resets.
- First-time passwords must be 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 must be immediately revoked.
- Inactive user accounts must be removed or disabled at least every 90 days.
- Accounts used by vendors for remote maintenance may be enabled only during the time period needed.
- Password procedures and policies must be communicated to all users who have access to cardholder data.
- Group, shared, or generic accounts and passwords are prohibited.
- User passwords must be changed at least every 90 days.
- A minimum password length of at least seven characters is required.
- Passwords must contain both numeric and alphabetic characters.
- Individual must submit a new password that is different from any of the last four passwords he or she has used.
- Repeated access attempts must be limited by locking out the user ID after no more than six failed attempts.
- The lockout duration above must be set to a minimum of 30 minutes or until an administrator enables the user ID.

- If a session has been idle for more than 15 minutes, the user must re-enter the password to re-activate the session.
- All access to any database containing cardholder data must be authenticated; this includes access by applications, administrators, and all other users.

9. Restrict physical access to cardholder data

Appropriate facility entry controls must be in place to limit and monitor physical access to systems in the cardholder data environment as follows:

- Access-control mechanisms such as video cameras must monitor individual physical access to sensitive areas. "Sensitive areas" refers to any data center, server room, or any area that houses system that store cardholder data. This excludes the areas where only point-of-sale terminals are present such as the cashier areas in a retail store.
- Data from access control mechanism must be collected (or be capable of being collected), reviewed, and correlated with other entries.
- Data from access control mechanisms must be stored for at least three months, unless otherwise restricted by law. Physical access to publically accessible network jacks leading to the cardholder environment must be restricted.
- Physical access to publically accessible network jacks in the card holder data environment must be restricted.
- Physical access to wireless access points, gateways, and handheld devices in the cardholder data environment must be restricted.

Procedures must be in place to help personnel easily distinguish between employees and visitors, especially in areas where cardholder data is accessible. For the purposes of this requirement, an "employee" refers to full-time and part-time employees, temporary employees and personnel and contractors and consultants who are "resident" on the entity's site. A "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. Visitors must be handled as follows:

- Authorized before entering areas where cardholder data is processed or maintained.
- Given a physical token for example, a badge or access device that expires and that identifies the visitor as non-employees.
- Asked to surrender the physical token before leaving the facility or at the date of expiration.

A visitor log must be in use to maintain a physical audit trail of visitor activity. The visitor's name, the firm represented, and the employee authorizing physical access must be documented on the log. The visitor log must be retained for a minimum of three months, unless otherwise restricted by law.

Media back-ups must be stored in a secure location, preferably in an off-site facility, such as an alternate or backup site, or a commercial storage facility. The security of the off-site facility must be reviewed at least annually.

All paper and electronic media that contain cardholder data must be physically secure.

Strict control must be maintained over the internal or external distribution of any kind of media that contains cardholder data. Controls must include the following: The media must be classified so that it can be identified as confidential. The media must be sent by secured courier or other delivery method that can be accurately tracked.

Processes and procedures must be in place to ensure that management approval is obtained prior to moving any and all media containing cardholder data from a secured area (especially when media is distributed to individuals).

Strict control must be maintained over the storage and accessibility of media that contains cardholder data as follows: Inventory logs of all media must be properly maintained. Media inventories must be conducted at least annually.

Media containing cardholder data must be destroyed when it is no longer needed for business or legal reasons. Destruction should be as follows: Hardcopy materials must be shredded, incinerated, or pulped so that cardholder data cannot be reconstructed. Electronic media with cardholder data must be rendered unrecoverable so that cardholder data cannot be reconstructed.

10. Track and monitor all access to cardholder data and network resources servicing it

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

Automated audit trails must be implemented for all system components to reconstruct the following events:

- All actions taken by any individual with root or administrative privileges.
- Access to all operating system audit trails.
- Invalid logical access attempts.
- Use of system level identification and authentication mechanisms.
- Initialization of system audit logs.
- Creation and deletion of system-level objects.

Automated audit trails must be implemented for all application components to reconstruct the following events:

- All individual access to cardholder data.
- Access to all application audit trails.
- Invalid logical access attempts.
- Use of application level identification and authentication mechanisms.
- Initialization of the application audit logs.

The following audit trail entries must be recorded for all system components (both operating system and application 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?

Critical system clocks and times must be synchronized.

Audit trails must be secured so they cannot be altered. Controls must ensure the following:

- Viewing of audit trails limited to those with a job-related need.
- Audit trail files protected from unauthorized modification.
- Audit trail files promptly backed up to a centralized log server or media that is difficult to alter.
- Logs for external-facing technologies written to a log server on the internal LAN.
- File-integrity monitoring or change-detection software must be 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.

Logs for all system components must be reviewed at least daily. Log reviews must include those servers that perform security functions like intrusion detection systems (IDS) and authentication, authorization, and

accounting protocol (AAA) servers, for example, RADIUS. Note: Log harvesting, parsing, and alerting tools may be used to achieve compliance with requirement 10.6. Audit trail history must be retained for at least one year, with a minimum of three months' history immediately available for analysis.

11. Regularly test security systems and processes related to cardholder data

The presence of wireless access points must be tested for by using a wireless analyzer at least quarterly or by deploying a wireless IDS/IPS to identify all wireless devices in use.

Internal and external network vulnerability scans must be 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. 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.

External and internal penetration testing must be performed 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 must include the following: network-layer penetration tests and application-layer penetration tests.

Intrusion-detection systems and/or intrusion-prevention systems must be used to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Intrusion-detection and prevention engines must be kept up-to-date.

File-integrity monitoring software must be deployed to alert personnel to unauthorized modification of critical system files, configuration files, or content files. This monitoring software must be configured to perform critical file comparisons at least weekly. For file-integrity monitoring purposes, critical files are 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 merchant or service provider.

12. Maintain a policy that addresses information security for employees and contractors who have a role in the cardholder environment

A security policy for the cardholder environment must be established, published, maintained, and disseminated appropriately. It must accomplish the following:

- Address all PCI DSS requirements.
- Include an annual process to identify threats and vulnerabilities, and which results in a formal risk assessment.
- Include a review at least once a year and be updated when the environment changes.

Daily operational security procedures must be developed that are consistent with requirements in this specification. Examples are user account maintenance procedures and log review procedures.

Usage policies for critical employee-facing technologies that could transmit card holder data must be developed to define proper use of these technologies for all employees and contractors. Examples of employee-facing technologies include remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants [PDAs], e-mail, and Internet usage. These usage policies must include the following:

- Explicit management approval.
- Authentication for the use of the technology.

- A list of all such devices and personnel with access.
- Labeling of devices with owner, contact information, and purpose.
- Acceptable use of the technologies.
- Acceptable network locations for the technologies.
- List of company-approved products.
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity.
- Activation of remote-access technologies for vendors only when needed by vendors, with immediate deactivation after use.
- When accessing cardholder data via remote-access technologies, copy, move, and storage of cardholder data onto local hard drives and removable electronic media is prohibited.

The security policy and procedures must clearly define information security responsibilities for all employees and contractors who support the cardholder environment.

The following information security management responsibilities must be assigned to an individual or team. They are assigned as follows:

- Establishing, documenting, and distributing security policies and procedures. ISO Office.
- Monitoring and analyzing security alerts and information, and distributing to appropriate personnel. Security Engineering.
- Establishing, documenting, and distributing security incident response and escalation procedures to ensure timely and effective handling of all situations. ISO Office.
- Administering user accounts, including additions, deletions, and modifications. Application Owners for both applications and servers.
- Monitoring and controlling all access to cardholder data. ISO Office and Treasury Services.

A formal security awareness program must be in place to make relevant employees aware of the importance of cardholder data security. Relevant employees must be educated upon hire and at least annually. Employees are required to acknowledge at least annually that they have read and understood Miami's security policy and procedures.

Potential employees with responsibility for the cardholder environment (see definition of "employee" in section 9 above) must be screened prior to hire to minimize the risk of attacks from internal sources. Screening is not required for those employees such as cashiers who have access to one card numbers only at a time when facilitating a transaction.

If cardholder data is shared with service providers, policies and procedures must be maintained and implemented to manage service providers. These policies and procedures must include the following.

- 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.

An incident response plan must be implemented to include the following in preparation to respond immediately to a system breach:

- The plan must address the following: (a) Roles, responsibilities, and communication and contact strategies in the event of a compromise including notification of the payment brands. (b) Specific incident response procedures. (c) Business recovery and continuity procedures. (d) Data back-up processes. (e) Analysis of legal requirements for reporting compromises. (f) Coverage and responses of all critical system components. (g) Reference or inclusion of incident response procedures from the payment brands."
- The plan must be tested annually

- Specific personnel must be designated to be available on a 24/7 bases to respond to alerts.
- Appropriate training must be provided to staff with security breach response responsibilities.
- Alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems must be included.
- A process must be in place to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.