

City of Minneapolis
PCI Information Security Procedures

Governing Policy: PCI Information Security

Synopsis: Establishes roles, responsibilities, and procedures for maintaining compliance with PCI DSS inside of each department or agency cardholder data environment.

Procedure History: Department Approval: 12-19-2013; **City Council Approval (Received & Filed):** DATE

Last Revision Date: 12-19-2013

Links to Related Standard: [PCI DSS v2.0](#)

Administering Department: Finance/Treasury

Contact: Larry Parker Phone: (612) 673-5397

Table of Contents

Roles and Responsibilities.....	2
Scope.....	3
Risk Assessment.....	3
Logical Access Control.....	4
Physical Access Control.....	5
Security Training and Awareness.....	7
Employee Technologies.....	7
Data Retention and Disposal.....	8
Transmission of Data.....	9
Malicious Software Protection.....	9
Patch Management.....	9
Change Control.....	10
Network Security.....	10
Security Incident Response.....	11
Logging and Auditing.....	11
Software Application Development and Management.....	12
Information System Configuration.....	12
Information Security Testing.....	13
Service Provider Management.....	13
Procedure Distribution and Review.....	14

City of Minneapolis
PCI Information Security Procedures

Roles and Responsibilities

Role	Responsibility
CFO or delegate(s) of the CFO	<ol style="list-style-type: none"> 1. Develop, maintain, and annually review procedures for the implementation and ongoing maintenance of the PCI Information Security Policy. 2. Ensure the Finance Staff are carrying out their responsibilities. 3. Ensure that the City is complying with PCI DSS. 4. Determine the appropriate means of communicating the PCI Information Security Policy and Procedures to all relevant departments. 5. Sign and submit Attestation of Compliance documents annually.
Finance Staff	<ol style="list-style-type: none"> 1. Inform department heads of PCI DSS requirements and associated dates for annual submission of their Attestation of Compliance. 2. Provide department heads with compliance documents as needed (AOC, SAQ, etc.). 3. Perform or contract audits to assist with compliance and remediation of non-compliance with PCI DSS. 4. Maintain documentation/evidence of compliance with PCI DSS (see documentation section). 5. Coordinate quarterly ASV scans of all applicable external IP addresses. 6. Coordinate annual internal and external penetration testing of all applicable systems.
Department Heads	<ol style="list-style-type: none"> 1. Develop, maintain, and update (annually and after changes) network diagrams of the cardholder data environment, data flow diagrams of the cardholder data environment, list of all system components of the cardholder data environment, list of all payment applications used, and a list of service providers with

City of Minneapolis
PCI Information Security Procedures

	<p>access to the cardholder data environment.</p> <ol style="list-style-type: none"> 2. Establish, document and distribute department level information security policies, procedures, standards, and/or guidelines to ensure compliance with all applicable requirements of the PCI DSS for their cardholder data environment. 3. Establish, document, and distribute security incident response and escalation procedures. 4. Monitor and control all access to sensitive cardholder data. 5. Submit evidence/documentation of compliance with PCI DSS to the Finance Department (see documentation section)
Department Staff	<ol style="list-style-type: none"> 1. Maintain compliance with department level policies, procedures, standards, and guidelines developed in support of this policy.
Third Party Vendors/Service Providers (with access to any cardholder data environment)	<ol style="list-style-type: none"> 1. Maintain compliance with department level policies, procedures, standards, and guidelines developed in support of this policy or demonstrate independent compliance with PCI DSS.

Reference: PCI DSS v2.0 requirement 12.5 (12.5.1 – 12.5.5)

Scope

Departments must establish which PCI DSS requirements are applicable to their PCI Cardholder Data Environment. Departments must comply with the following requirements if they are applicable to their department. As an example, if a department does not process, transmit, or store cardholder data in their environment a formal change management process does not need to be developed. The Finance Department will assist the other departments in establishing which PCI DSS requirements are applicable.

Risk Assessment

Departments must regularly identify, define, and prioritize risks to the confidentiality, integrity, and availability of its information systems, network resources and data. Departments must conduct an annual formal, documented risk assessment of its information systems, data and network resources. The assessment must identify and prioritize the threats and vulnerabilities to department’s information systems, data and network resources and define the likelihood and impact of risks.

City of Minneapolis
PCI Information Security Procedures

The risk assessment must be used in conjunction with departments' risk management process to identify, select, and implement appropriate and reasonable controls to protect the confidentiality, integrity, and availability of departmental information systems, network resources, and data. The risk assessment will follow established methodologies such as OCTAVE, ISO 27005 or NIST SP 800-30.

Departments must conduct risk management on a regular basis and select & implement reasonable, appropriate, and cost-effective controls to manage, mitigate, or accept identified risks. All such controls must be commensurate with identified risks.

Annually, department heads must submit an information security risk management report to appropriate City of Minneapolis Finance Department. The report must identify the significant risks to information systems, data and network resources that have been identified during the past year, the risks that have been accepted and which risks have been mitigated.

Reference: PCI DSS v2.0 requirement 12.1.2, 12.1.3

Logical Access Control

Department employees, contractors, service providers and vendors must not attempt to gain logical access to information systems, data or network resources for which they have not been given proper authorization.

Logical access to information systems and media containing sensitive data must be denied until specifically authorized by department heads.

Direct access and queries to databases containing cardholder data must be restricted to database administrators, databases, and/or stored procedures.

Appropriate information system owners and/or data custodians or their designated delegates must define and approve logical access to information systems and media containing sensitive data.

Logical access to information systems and media must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege.

Departments must have a formal, documented user management process which enables the controlled addition, change, and termination of logical access rights on information systems, data and network resources. The process must be capable of granting different levels of access to information systems, data and network resources. An automated access control system will be implemented to control access to information systems.

A unique user name must be used by all persons accessing information systems and media containing sensitive data. Along with the unique user name, one of the following authentication methods must be used:

- Password
- Token devices or smart cards
- Biometrics

Two factor authentication must be used by employees, contractors, service providers and vendors for remote access to information systems and media containing sensitive data. Employees who

City of Minneapolis
PCI Information Security Procedures

telecommute must take all precautions necessary to secure any and all sensitive Departments data in their homes and prevent unauthorized access to any City of Minneapolis cardholder data environment.

Vendor maintenance accounts and ports on information systems that contain sensitive data must be disabled until the specific time they are needed by the vendor. After appropriate use by the vendor, they must again be disabled. All vendor access shall be monitored while in use.

Group, shared or generic accounts or passwords must not be used on Departments information systems that store, process or transmit sensitive data. The following requirements must be met for passwords on such systems:

- User passwords must be changed at least every 90 days.
- Passwords must be at least 7 characters long and include both numeric and alphabetic characters.
- First time passwords must be unique for each user and must be changed upon first use.
- Password history must be enabled to restrict the reuse of the last 24 passwords.
- Via the use of strong cryptography, all passwords must be unreadable during transmission and storage on all information systems that store, process or transmit sensitive data.
- User accounts must be locked after six failed login attempts. The lockout must be for at least 30 minutes or until an authorized system administrator unlocks the account.
- City of Minneapolis employees must not use passwords that are also used for non-City of Minneapolis accounts.

Activation of information system locking software or log off must occur when a user session on an information system is inactive for more than 15 minutes.

User identity must be appropriately verified before any password, which enables access to an information system or network resource, is reset.

User accounts that are inactive for more than 90 days on information systems that store, process or transmit sensitive data must be disabled or removed.

At least every 6 months, appropriate information system owners and/or data custodians or their designated delegates must review and verify logical access rights to information systems and media containing sensitive data. Such rights must be revised as necessary. Inactive accounts over 90 days old must be either removed or disabled.

Employees and contractors experiencing a change in status (e.g. termination, position change) must have their logical access rights promptly reviewed, and if necessary, modified or revoked.

Reference: PCI DSS v2.0 requirements 7.1 (7.1.1 – 7.1.4), 7.2 (7.2.1 – 7.2.3), 8.1, 8.2, 8.3, 8.4, 8.5 (8.5.1 - .16)

Physical Access Control

At least annually, departments must identify all of their physical areas that must be protected from unauthorized physical access. The assessment must take into consideration areas where sensitive data is stored, processed, or transmitted as well as the location of any supporting assets or critical infrastructure.

City of Minneapolis
PCI Information Security Procedures

Information systems and electronic & non-electronic media containing sensitive data must be located in physically secure areas (“limited access area”). Typically, such areas have a defined security perimeter such as a card controlled entry door. Information systems located in unrestricted, public access areas must be physically secured to prevent theft.

Access to limited access areas must be denied until specifically authorized by department heads. Such access must be provided only to those having a need for specific access in order to accomplish a legitimate task and must be based on the principles of need to know and least possible privilege. Access privileges to limited access areas must be reviewed at least annually.

Cameras or other access control mechanisms must monitor the entry and exit points of physical areas containing information systems that store, process or transmit sensitive data or electronic & non-electronic media containing sensitive data and must be protected from tampering or disabling and must be monitored. Camera data must be stored for at least three (3) months unless otherwise restricted by law.

Departments must control and restrict physical access to publicly accessible network jacks; they must also restrict physical access to wireless access points (WAPs), gateways and handheld devices, networking/communications hardware and telecommunications lines located at department facilities.

Backup media, both paper and electronic, that contains sensitive data must be stored in a secure location. The location’s security must be reviewed at least annually. An inventory of all such media must be conducted at least annually. Where appropriate, shred bins will be maintained with a lock preventing access to its contents. All such media, when no longer needed for business or legal reasons, must be destroyed in such a way that there is reasonable assurance that the media cannot be reconstructed (i.e. crosscut shredding, pulping or incinerating of hardcopy materials and degaussing, securely overwriting or physically destroying electronic media).

Departments’ electronic and non-electronic media containing sensitive data must be classified so that it can be identified as “Security Data.” Distribution of such media outside the department must be tracked and logged. Such media must only be distributed outside departments via a delivery method that can be tracked (such as secure courier).

Appropriate departmental management must approve the movement of any media containing sensitive data from a limited access area. This approval must also be logged.

Departments must have a formal, documented process in place that clearly identifies and distinguishes between employees, contractors, and visitors. Employee and contractors must be given a physical token (i.e., a badge or access device) that can be revoked upon termination of the employees and contractors.

Visitors to limited access areas must be formally authorized by an appropriate employee to access such areas. Visitors to limited access areas must be given a physical token (i.e., a badge or access device) that has an expiration date and that identifies a visitor as a non-employee. Visitors must be asked to return their physical token upon leaving a limited access area or at the expiration date.

Visitors must sign a visitor’s log prior to being granted physical access to limited access areas. The log must document the visitor's name, the company represented, the authorizing employee, and the date &

City of Minneapolis
PCI Information Security Procedures

time of entrance and departure. Unless otherwise restricted by law, visitor logs must be retained for at least three (3) months.

Reference: PCI DSS v2.0 requirements 9.1 (9.1.1 – 9.1.3), 9.2, 9.3 (9.3.1 – 9.3.3), 9.4, 9.5, 9.6, 9.7 (9.7.1 – 9.7.2), 9.8, 9.9 and 9.10

Security Training and Awareness

Departments must ensure that all personnel are provided with sufficient training and supporting reference materials to enable them to appropriately protect information systems, network resources, and data. Departments must provide information security awareness training to its employees and contractors upon hire and then at least annually.

Departments must provide regular security information and awareness to its employees and contractors via methods such as log-in banners, posters, web-based training, memos and periodic meetings. Such information and awareness must include, but is not limited to:

- Any significant revisions to Departments information security policies
- Significant new Departments information security controls or processes
- Significant changes to Departments information security controls or processes
- Significant new security threats to Departments information systems, network resources, or data
- Information security best practices

Employees must acknowledge, in writing or electronically, at least annually, that they have read and understood department level PCI Security Policies and Procedures.

Reference: PCI DSS v2.0 requirements 12.6 (12.6.1 – 12.6.2)

Employee Technologies

Employee technologies (i.e., remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, PDAs, email and internet usage) that access sensitive data must only be used by all personnel if the following controls are in place:

- Appropriate management approval for the use of the technologies

Appropriate authentication is used (i.e., a unique user name and one of the following authentication methods must be used: (1) password; (2) token devices or smart cards; or (3) biometrics)

- A regularly updated inventory of devices, approved network locations for their use, and list of the persons authorized to access the devices
- Inventory contains owner name, contact information, and a description of the device's purpose
- Devices are appropriately used and placed in appropriate network locations
- Departments maintains a regularly updated list of approved devices

When payment card data on information systems is remotely accessed, the data must not be copied, moved, or stored onto local hard drives or removable electronic media unless explicitly authorized for a defined business need. If users are authorized to copy, move, or store the data, policies must be created to assure the protection of the cardholder data complies with all PCI DSS requirements.

City of Minneapolis
PCI Information Security Procedures

Remote access sessions to information systems containing sensitive data must be disconnected after twenty (20) minutes of inactivity. Remote access technologies used by vendors or business partners to access information systems containing sensitive data must be turned off when not in use.

Reference: PCI DSS v2.0 requirements 12.3 (12.3.1 – 12.3.10)

Data Retention and Disposal

Departments must keep the storage of sensitive data to the minimum necessary required for business, legal and/or regulatory purposes. When no longer required for such purposes, sensitive data on information systems or on electronic and non-electronic media must be appropriately disposed. The following disposal methods must be used:

- Non-electronic media must be cross-cut shredded, incinerated or pulped, so that the data cannot be reconstructed.
- Electronic media must be securely overwritten, degaussed, shredded or otherwise physically destroyed so that sensitive data cannot be reconstructed.

Sensitive data on Departments electronic media and information systems must be securely and thoroughly erased before such items can be re-used.

Information systems and electronic & non-electronic media that contain sensitive data must be inventoried and audited on a quarterly basis to ensure that the stored data does not exceed the departments' data retention requirements.

After a payment card transaction is authorized, the following types of data must never be stored in electronic or non-electronic form at a department facility:

- Magnetic stripe data
- CVC2/CVV2/CID/CAV2
- PIN/PIN Block

Unless otherwise authorized, credit card primary account numbers (PANs) on information systems must be masked; the first six (6) and the last four (4) digits of the PAN are the maximum that can be displayed.

PANs stored electronically on information systems or portable storage devices must be made unreadable. One of the following methods must be used:

- Strong one-way hash functions
- Truncation
- Index tokens and pads, with the pads being securely stored
- Strong cryptography with associated key-management processes and procedures

Cryptographic keys must be securely stored and comply with the following key management procedures:

- Keys must be maintained separately from the operating system and not tied to user accounts
- Restrict access to the fewest number of custodians possible
- Generation of strong keys

City of Minneapolis
PCI Information Security Procedures

- Maintenance of an inventory of encryption keys
- Secure key storage in the fewest number of locations possible Secure key distribution
- Periodic key changes
- Destruction of old keys
- Split knowledge and dual control of keys
- Prevention of unauthorized substitution of keys
- Replacement of known or suspected compromised keys
- Definition of a cryptoperiod and change of keys before the cryptoperiod expires
- Revocation of old or invalid keys
- Revocation of key when integrity of key weakened

Key custodians must sign a form specifying that they understand and accept their key-custodian responsibilities.

Reference: PCI DSS v2.0 requirements 3.1, 3.2 (3.2.1 – 3.2.3), 3.3, 3.4, 3.5, 3.6, 9.10

Transmission of Data

If sensitive data must be sent over an open, public network (e.g., the Internet, wireless technologies, GSM, GPRS), strong cryptography such as SSL, TLS, SSH, or IPSEC must be used to encrypt the data.

If a wireless network is used to transmit sensitive data, strong encryption (i.e. WPA2, IPSEC or SSL) must be used.

Strong cryptography must be used whenever sensitive data is sent via end-user messaging technologies (e.g., email, instant messaging, chat).

Reference: PCI DSS v2.0 requirements 4.1, 4.2

Malicious Software Protection

All systems must have anti-virus software on their information systems commonly affected by malicious software. Such software must be capable of detecting, removing and protecting against all known types of malicious software including spyware and adware.

Anti-virus software must be kept actively running and capable of generating audit logs. Anti-virus software must be enabled for automatic updates and conduct periodic scans.

Reference: PCI DSS v2.0 requirements 5.1, 5.2.

Patch Management

A formal, documented process for regularly identifying and prioritizing relevant and necessary security and functional patches for information systems and applications that process, transmit or store sensitive data must be in place. A risk based approach for prioritizing security patch installations may be used. All critical new security patches must be applied within one (1) month of release. A process will be developed to identify and assign a risk ranking (based on security best practices such as CVSS) to newly discovered security vulnerabilities.

Reference: PCI DSS v2.0 requirements 6.1, 6.2.

Change Control

A formal, documented change control process for information system and software configuration changes must be used. The process must include:

- Identification and documentation of significant changes
- Assessment of the potential impact, including security implications, of significant changes
- Appropriate approval of all changes by authorized parties
- Ability to terminate and recover from unsuccessful changes
- Testing procedures to ensure the change is functioning as intended and does not adversely impact security
- Communication of completed change details to appropriate persons
- The updating of appropriate information system or software documentation upon the completion of a significant change

Only properly authorized persons may make an emergency change to information systems, data or network resources. Such emergency changes must be appropriately documented and promptly submitted, after the change, to the department's normal change management process.

Reference: PCI DSS v2.0 requirements 6.4.5 (6.4.5.1-6.4.5.4)

Network Security

All firewalls and routers must have formal, documented standards. Such standards must include:

- A formal process for approving and testing all network connections and changes to firewall and router configurations.
- A current diagram(s) of the department's cardholder data environment. The diagram must show all connections to information systems that process, transmit or store sensitive data. Changes to the network or cardholder data environment must be appropriately updated in the network diagram(s). The diagram must be reviewed and updated no less than annually.
- Requirements for a firewall at each logical point where the network connects to the Internet and between any demilitarized zone (DMZ) and internal network(s).
- A description of groups, roles, and responsibilities for logical management of network components.
- Documentation and business justification of all services, protocols, and ports allowed by the firewalls and routers, including documentation of security features implemented for insecure protocols (e.g. Telnet, FTP). Confirm that each insecure service, protocol and port are necessary.
- A requirement to review Departments firewall and router rule sets at least every six (6) months.

Firewalls must perform stateful inspection and must restrict connections between untrusted networks (i.e. the Internet) and information systems that process, transmit or store sensitive data. The firewalls must prohibit direct access between the Internet to such information systems, must restrict inbound and outbound traffic to that which is documented as necessary for organizational purposes and explicitly deny all other traffic.

Configuration files on routers must be secured and regularly synchronized.

City of Minneapolis
PCI Information Security Procedures

A firewall(s) must be installed between any wireless networks and information systems that process, transmit or store sensitive data. Such firewalls must deny or control traffic from any wireless networks to these information systems.

All inbound traffic from public addresses on untrusted networks must terminate in a DMZ. Inbound Internet traffic to the trusted cardholder data segment must be limited to IP addresses inside the DMZ. All databases that store sensitive data must be placed in the internal network(s) and be segregated from any DMZ and other untrusted networks.

Personal firewall software must be installed and active on any mobile and/or employee-owned computers with direct connectivity to the Internet that are used to access the cardholder data environment. The personal firewall software must be configured to specific standards and prevent unauthorized users from altering or disabling it.

IP masquerading (e.g., port address translation [PAT] or network address translation [NAT]) must be used for information systems on internal network(s).

Reference: PCI DSS 2.0 requirements 1.1 (1.1.1 – 1.1.6), 1.2 (1.2.1 – 1.2.3), 1.3 (1.3.1 – 1.3.8), 1.4.

Security Incident Response

Departments must have a formal, documented security incident response plan. The plan must include:

- Roles, responsibilities, and communication and contact strategies in the event of a security incident including notification of appropriate parties
- Specific incident response procedures
- Business recovery and continuity procedures
- Data back-up processes
- Legal requirements for reporting security incidents and compromises
- Coverage and responses for all critical information systems
- Reference or inclusion of payment card brand incident response procedures
- Procedures for responding to alerts from intrusion detection (IDS), intrusion prevention (IPS) and/or file integrity monitoring systems

The security incident response plan must be tested annually and must designate specific personnel to be available on a 24/7/365 basis in order to respond promptly to information security alerts. The plan must be reviewed regularly and modified as necessary, including modifications to include industry development. Lessons learned will be documented.

Employees who are responsible for responding to security incidents must receive regular and appropriate training in security incident response processes.

Reference: PCI DSS v2.0 requirements 12.9 (12.9.1 – 12.9.6)

Logging and Auditing

Appropriate logging and monitoring controls must be implemented on information systems, data and network resources.

Automated audit trails on information systems that store, process or transmit sensitive data must be implemented. The audit trails must be able to reconstruct the following events:

City of Minneapolis
PCI Information Security Procedures

- Individual accesses to sensitive data
- 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 audit logs
- Creation and deletion of system-level objects

For each of the above events, the following must be recorded:

- 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

Logs and audit trails on information systems that store, process or transmit sensitive data must be reviewed daily. Such logs and audit trails must be monitored by file integrity or change detection software. Log reviews must include intrusion detection and authentication, authorization and accounting (AAA) servers.

Information generated by logging and monitoring controls implemented on information systems, data and network resources must be protected from unauthorized access. Access to such information must be limited to only those individuals with a need-to-know. Such information must be promptly backed up to a centralized log server and/or media that is difficult to alter. Logs for external-facing technologies (i.e., firewalls, DNS, email) must be promptly copied onto a log server on the internal network. Unless otherwise restricted by law, audit and log file information must be retained for at least one year.

Department information systems must have their system clocks and times synchronized with a master time source (e.g. network time protocol [NTP]). Specific industry-accepted Internet time servers must be designated from which time updates will be accepted.

Reference: PCI DSS v2.0 requirements 10.1, 10.2 (10.2.1 – 10.2.7), 10.3 (10.3.1 – 10.3.6), 10.4, 10.5 (10.5.1 – 10.5.5), 10.6, 10.7.

Software Application Development and Management

City of Minneapolis departments must not internally develop software applications to store, process, or transmit sensitive data. Instead, PCI PA-DSS validated applications, PCI DSS validated service providers, and/or stand-alone payment terminals must be used for all payment processing, storage, and transmission activities.

Information System Configuration

All system components of the cardholder data environment must have implemented, formal, and documented configuration standards. Such standards must be consistent with system hardening best

City of Minneapolis
PCI Information Security Procedures

practices as defined by organizations such as ISO, SANS, NIST and CIS. At a minimum, the standards must require the following:

- Limiting to one primary function for servers that process, transmit or store sensitive data
- Disabling of unnecessary and/or insecure services and protocols
- Appropriate configuration of system security settings
- Removal of unnecessary functionality (e.g., scripts, Web servers, subsystems)
- Changing or removing vendor-supplied defaults (i.e., passwords, accounts, SNMP community strings)

All non-console logins that enable administrator access to system components of the cardholder data environment must be encrypted.

Additionally, a formal, documented process to identify newly discovered security vulnerabilities and update configuration standards to address new vulnerabilities must be in place. Configuration standards must be updated to reflect any newly discovered vulnerabilities.

Reference: PCI DSS v2.0 requirements 2.1, 2.2 (2.2.1 – 2.2.4), 2.3, 6.2

Information Security Testing

Department cardholder data environments must annually, or after any significant changes to the information technology environment, have internal and external penetration tests of information systems that process, transmit or store sensitive data. The penetration tests must include both network and application layer tests.

At least quarterly, an audit must be conducted at department facilities to identify all wireless devices in use or a wireless IDS/IPS must be deployed which is capable of identifying all wireless devices in use at department facilities and alerting appropriate personnel upon discovery of devices.

External vulnerability scans against all information systems that are Internet reachable must be performed at least quarterly and after any significant change in the network. Internal vulnerability scans must be run against all cardholder data environment information systems that process, transmit or store sensitive data at least quarterly and after any significant change in the network. All internal and external scans must be run until passing results are obtained, or all “High” vulnerabilities are resolved (identified during patch management risk ranking process).

Per its risk assessment, departments must implement and maintain network IDS, host based IDS and/or IPS to monitor all traffic to Departments information systems that process, transmit or store sensitive data. IDS/IPS signatures must be kept up-to-date at all times and configured to alert personnel of suspected compromise.

File integrity monitoring software must be deployed on all information systems that process, transmit or store sensitive data. The software must perform critical file comparisons at least weekly.

Reference: PCI DSS v2.0 requirements 11.1, 11.2, 11.3 (11.3.1 – 11.3.2), 11.4, 11.5.

Service Provider Management

If departments share sensitive data with service providers, then departments must develop and maintain a service provider management program that meets, at minimum, the following requirements:

City of Minneapolis
PCI Information Security Procedures

- Maintenance of a list of service providers.
- Written acknowledgement from each service provider that they are responsible for the security of the sensitive data the service provider possesses or has access to.
- An established process for engaging service providers that includes proper due diligence prior to engagement.
- Development and maintenance of a program to monitor service providers' PCI DSS compliance at least annually.

Reference: PCI DSS v2.0 requirement 12.8 (12.8.1 – 12.8.4)

Procedure Distribution and Review

Department level policies, procedures, standards, and guidelines that meet the requirements of this document must be created, published and distributed to all appropriate departments parties (employees, contractors, vendors, service providers and business partners).

These documents must be reviewed at least annually and revised as necessary.

Reference: PCI DSS v2.0 requirements 12.1, 12.1.3, 12.2