City of Monroe

Information Technology Policy

PCI Compliance Addendum

PCI DSS stands for Payment Card Industry Data Security Standard, and is a worldwide security standard assembled by the Payment Card Industry Security Standards Council (PCI SSC).

Purpose: The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC). The PCI SSC is responsible for managing the security standards, while compliance with the PCI set of standards is enforced by the founding members of the Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc.

PCI DSS includes technical and operational requirements for security management, policies, procedures, network architecture, software design and other critical protective measures to prevent credit card fraud, hacking, and various other security vulnerabilities and threats. The standards apply to all organizations that store, process or transmit cardholder data.

The standards are designed to protect cardholder information of customers and any individual or entity that utilizes a credit card to transact business with the City. This policy is intended to be used in conjunction with the complete PCI-DSS requirements as established and revised by the PCI Security Standards Council.

Scope: All departments that collect, maintain, or have access to credit card information must comply with the PCI policy.

The City of Monroe currently has no third-party vendors that process and store credit card information using the City of Monroe's merchant accounts.

The City of Monroe does have a relationship with both Smith Data (QS/1) and Courtware Solutions who process utility bill payments and traffic fines by credit card. However, the City of Monroe's merchant accounts are not used and no credit card information is received from either vendor.

Who Should Read this Policy: All persons who have access to credit card information, including:

- Every employee that accesses handles or maintains credit card information. City of Monroe employees include full-time, part-time, salaried, and hourly staff members as well as intern workers who access, handle or maintain records.
- Employees who contract with service providers (third-party vendors) who process credit card payments on behalf of the City of Monroe
- IT staff responsible for scanning the City systems to insure no credit card numbers are stored electronically.

Definitions:

Merchant Account - A relationship set up by the Controller's office between the City and a bank in order to accept credit card transactions. The merchant account is tied to a general ledger account to distribute funds appropriately to the organization (owner) for which the account was set up.

Coordinator – The City official who has oversight responsibility for the regulation/standard. Regulation monitors stay abreast of updates to their respective regulations, ensure policies are up to date and notify the Information Security Officer and Data Managers about changes.

Credit Card Data - Full magnetic strip or the PAN (Primary Account Number) plus any of the following:

- Cardholder name
- Expiration date
- Service Code

PCI-DSS - Payment Card Industry Data Security Standard

PCI Security Standards Council - The security standards council defines credentials and qualifications for assessors and vendors as well as maintaining the PCI-DSS.

Self-Assessment - The PCI Self-Assessment Questionnaire (SAQ) is a validation tool that is primarily used by merchants to demonstrate compliance to the PCI DSS.

PAN - Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. It is also called Account Number.

Overview:

City of Monroe policy prohibits the storing of any credit card information in an electronic format on any computer, server, or database including Excel spreadsheets. It further prohibits the emailing of credit card information. Based on this policy, compliance with a number of the PCI Compliance requirements do not apply. The following list communicates the full scope of the compliance requirements but based on the City policy that prohibits storing of credit card information electronically and utilizing third-party vendors for web based credit card processing, some may not be relevant.

Requirements:

- Build and Maintain a Secure Network
- Maintain a Vulnerability Management Program
- Implement Strong Access Control Measures
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy
- Insure Third Party Compliance
- Training

Recommendations:

- Complete an annual self-assessment
- Perform a quarterly Network scan

Without adherence to the PCI-DSS standards, the City would be in a position of unnecessary reputational risk and financial liability. Merchant account holders who fail to comply are subject to:

- Any fines imposed by the payment card industry
- Any additional monetary costs associated with remediation, assessment, forensic analysis or legal fees
- Suspension of the merchant account.

Procedures:

The City of Monroe requires compliance with PCI standards. To achieve compliance, the following requirements must be met by departments accepting credit cards to process payments on behalf of the City.

General Requirements

- Credit card merchant accounts must be approved by the City.
- Management and employees must be familiar with and adhere to the PCI-DSS requirements of the PCI Security Standards Council.
- Management in departments accepting credit cards must conduct an annual self-assessment against the requirements. All employees involved in processing credit card payments must sign a statement that they have read, understood, and agree to adhere to Information Security policies of the City of Monroe and this policy.
- Any proposal for a new process (electronic or paper) related to the storage, transmission or processing of credit card data must be brought to the attention of and be approved by the City.

Storage and Disposal

- Credit card information must not be entered/stored on network servers, workstations, or laptops.
- Credit card information must not be transmitted via email.
- Web payments must be processed using a PCI-compliant service provider approved by the City.
- Although electronic storage of credit card data is prohibited by this policy, the City will perform a quarterly Network scan to insure that the policy has not been violated.
- Any paper documents containing credit card information should be limited to only information required to transact business, only those individuals who have a business need to have access, should be in a secure location, and must be destroyed via approved methods once business needs no longer require retention.
- All credit card processing machines must be programmed to print-out only the last four or first six characters of a credit card number.

- Securely dispose of sensitive cardholder data when no longer needed for reconciliation, business or legal purposes. In no instance shall this exceed 45 days and should be limited whenever possible to only 3 business days. Secured destruction must be via shredding either in house or with a third-party provider with certificate of disposal
- Neither the full contents of any track for the magnetic strip nor the three-digit card validation code may be stored in a database, log file, or point of sale product.

Third Party Vendors (Processors, Software Providers, Payment Gateways, or Other Service Providers)

- The City must approve each merchant bank or processing contact of any third-party vendor that is engaged in, or propose to engage in, the processing or storage of transaction data on behalf of the City of Monroe—regardless of the manner or duration of such activities.
- Insure that all third-party vendors adhere to all rules and regulations governing cardholder information security.
- Contractually require that all third parties involved in credit card transactions meet all PCI security standards.

Self-Assessment

- The PCI-DSS Self-Assessment Questionnaire must be completed by the merchant account owner annually and anytime a credit card related system or process changes. This assessment is the responsibility of the Finance Department.

Training

- Ongoing training and awareness programs will be offered to train employees on PCI DSS and importance of compliance.

Responsible Organization / Party: The Finance Utility Billing Administration Division Manager shall serve as the Coordinator of the policy which includes responsibility for notifying the City Administrator, Department Heads, and other Managers about changes to the policy. S/he will be assisted by the Director and Assistant Director of the Finance Department, and other employees as needed.

Enforcement: The IT Administrator will oversee enforcement of the policy. Additionally, this individual will investigate any reported violations of this policy, lead investigations about credit card security breaches, and may terminate access to protected information of any users who fail to comply with the policy. S/he will be assisted by the City Administrator, Department Heads, Managers, Supervisors, and other employees as needed.