Finance Committee Meeting

AGENDA

April 1, 2014

I. CALL TO ORDER

II. MATTERS BEFORE COMMITTEE

1. Approval - Vehicle Use Policy
2. Approval - Electronic Check Transfer Agreement
3. Approval - Incident Response Plan for PCI Compliance
4. Approval - IT Policy Addendum for PCI Compliance

III. ADJOURN

Finance Committee Meeting

AGENDA

April 1, 2014

Item:

Approval - Vehicle Use Policy

Department:

Additional Information:

Financial Impact:

Budgeted Item:

Recommendation / Request:

Viewing Attachments Requires Adobe Acrobat. Click here to download.

Attachments / click to download

Vehicle Use Policy

Cover Memo

Item # 1

CITY OF MONROE

VEHICLE POLICY AND PROCEDURES

Effective Date: April 09, 2014

GENERAL PROVISIONS

A. Municipal Vehicles

It is the policy of the City of Monroe to authorize the acquisition and utilization of vehicles for use by employees of the city, in the conduct of their employment responsibilities, either during the work shift or on a twenty-four (24) hour on-call basis. City vehicles are not personal vehicles and are not for personal use. City vehicles should be viewed as belonging to the citizens of Monroe and are assigned solely for purposes consistent with providing services to those citizens.

B. Expense Reimbursement

It is the policy of the City of Monroe to reimburse employees for reasonable expenses which they incur as a result of personal automobile use on city business. Receipts and the Expense Reimbursement Form must be submitted in order for an employee to be reimbursed for such expenses. Expense reimbursement is intended for travel outside the City of Monroe. Employees will not be reimbursed for personal automobile use within the city without advance approval of the department head or the City Administrator.

PROCEDURE

A. Garaging of Vehicles

All municipal vehicles, except those authorized for twenty-four (24) hour use, shall be garaged at the end of each day in assigned municipal parking lots. No vehicles, except those authorized for twenty-four (24) hour use, are to be taken home at the end of the workday.

B. Assignment of Vehicles

The assignment of municipal vehicles during work time use is based upon job responsibilities. Department Heads who have municipal vehicles available for this purpose may assign such vehicles in a manner consistent with departmental workload and employee function. Department Heads are responsible for the vehicle use, maintenance, including cleanliness, and storage. Department

Heads shall ensure that vehicles are routinely washed, the interior cleaned, and the preventative maintenance schedule is observed. Department Heads are responsible to the City Administrator for a full accounting of all municipal vehicles usage. The assignment of vehicles may be rescinded with reasonable notice by the City Administrator for work-related reasons.

C. Assignment of Municipal Vehicles for Twenty-Four (24) Hour Use (Vehicle Approved for Commuting Purposes)

1) The assignment of vehicles for twenty-four (24) hour use will be made in writing by the City Administrator (see Exhibit A), and will only be considered for employees who require a vehicle for the ordinary and necessary discharge of their job functions. Criteria, which will be used in the determination of eligibility for twenty-four (24) hour vehicle use, include:

   - officially designated on-call status
   - requirement for frequent emergency availability
   - issuance of a pager or other communication device
   - emergency or other equipment contained in the vehicle

   Such assignment may be rescinded with reasonable notice by the City Administrator for work-related reasons.

2) When commuting**,** vehicle use is limited to travel to and from the residence and place of work. The vehicle should be driven over the most direct route taking into account road and traffic conditions. The vehicle should not be utilized for travel outside a direct commuting route for personal reasons. All employees assigned a vehicle for twenty-four (24) hour use (see Exhibit A) will be allowed to utilize this privilege so as long as the employee's residence is in Walton County. The only exception to this policy is addressed in C.5.a.

3) Whenever a position becomes vacant, the authorization for twenty-four (24) hour use for commuting shall be reevaluated.

4) Employees that are assigned municipal vehicles on a twenty-four (24) hour basis will be given a copy of this policy and will be required to sign a confirmation of receipt.

5) Qualified Non-Personal Use of City Vehicles (Internal Revenue Service Regulations for Use of Municipal Vehicles)

   a) Employees who drive marked or unmarked police vehicles must be authorized to carry a weapon and have the power to arrest and, therefore, are not subject to imputed income taxation. Sworn officers will be allowed to utilize a twenty (20) mile radius when assigned a city-owned Police vehicle.

b) Vehicles which meet Internal Revenue Service guidelines as qualified non-personal use vehicles are not considered personal vehicles subject to taxation.

c) Other employees authorized to commute in a city vehicle may be subject to imputed income regulations as set forth by the Internal Revenue Service, which considers a certain portion of the vehicle use (namely the commute) to be income for the purposes of income taxation. The Finance Department shall be responsible for determining any tax liability and will be provided with the names of all employees authorized to use city vehicles for commuting purposes, and the normal, one-way commuting distance, each by December

d) Employees using city vehicles to commute will be subject to the Commuting Rule per Internal Revenue Service Publication 15-B. This would not be in force during weekends, holidays or vacations. Anytime an employee visits a work site on the way from home to the office, or from the office to home, it negates the tax liability. In this case, a log must be kept and submitted on a regular basis.

D. Operation and Maintenance of Vehicles

All employees are required to adhere to the following minimum rules of operation of city vehicles:

1. Speed Limits: Strictly observed, excepting emergency vehicles en route to an emergency.

2. Use of Safety Restraints: Seat belts, shoulder harness, and other restraints should be worn at all times vehicle is in motion, by driver and all passengers.

3. Rules of the Road: All traffic, driving and road regulations are to be strictly observed. Courtesy is to be extended to all entering and exiting traffic whenever vehicle is operated within the City of Monroe.

4. Use of Controlled Substances: Alcohol, illegal drugs, or prescription medication which may interfere with effective and safe operation are strictly prohibited.

5. Fuel is supplied exclusively through a city facility or through an issued or assigned fuel card for city-owned vehicles.

6. Maintenance responsibilities will be assigned to the Department of Streets and Transportation, Maintenance Division.

7. Tobacco Use: At no time will tobacco use be allowed in a city vehicle.

E. General Vehicle Use Regulations

City vehicles may only be used for legitimate city business.

City vehicles will not be used to transport any individual who is not directly or indirectly related to city business. Passengers shall be limited to city employees and individuals who are directly associated with city work activity (committee members, consultants, contractors, etc.) Family members shall not be transported in city vehicles.

Employees who operate city vehicles shall have a valid Georgia motor vehicle operator's license and of the class required for the specific vehicle being operated. Employees may be required to provide proof of valid operator's license upon request.

Vehicles should contain only those items for which the vehicle is designed. The city shall not be liable for the loss or damage of any personal property transported in the vehicle.

Employees are expected to keep city vehicles clean, and to report to their supervisor any malfunction or damage.

Employees who are assigned vehicles for commuting purposes are expected to park such vehicles in safe locations.

Employees who incur parking or other fines in city vehicles will generally be personally responsible for payment of such fine.

Employees who are issued citations for any offense while using a city vehicle must notify their supervisor immediately when practicable, but in no case later than twenty four (24) hours. Failure to provide such notice will be grounds for disciplinary action in accordance with Section K of this policy.

An employee who is assigned a city vehicle and who is arrested for or charged with a motor vehicle offense for which the punishment includes suspension or revocation of the motor vehicle license, whether in his/her personal vehicle or in a city vehicle, shall notify his/her supervisor immediately when practicable, but in no case later than twenty four (24) hours. Conviction for such an offense may be grounds for loss of city vehicle privileges and/or further disciplinary action.

No employee may use a city vehicle for out of state use without advance approval of the City Administrator.

F. Reporting of Accidents

Whenever a city vehicle is involved in an accident, or subject to damage, or in the event an employee's personal vehicle is damaged during an approved, work-related trip, the employee operating the vehicle is required to immediately notify his/her immediate supervisor, and contact the Georgia State Patrol. When the estimated damage exceeds $1000.00, an Accident/Incident Report shall be filed with the Finance Department.

G. Registering and Insuring a Vehicle

The Finance Department shall coordinate all vehicle registrations, renewals, and insuring

H. Withholding and Reporting Requirements:

City is required to withhold federal income tax and social security taxes, if applicable, on the value of the fringe benefit to be included in the employee's gross income per Internal Revenue Service Publication 15-B.

I. Expense Reimbursement – Personal Vehicles

1. Expense reimbursement is intended for travel outside the City of Monroe. Employees will not be reimbursed for the use of a personal automobile within the City of Monroe without advance approval of the department head.

2. When an employee is authorized to use a personal automobile for work-related travel, he/she shall be reimbursed at a rate based on the current standard mileage rate issued each year by the Internal Revenue Service.

    a. The mileage rate is intended to include the costs of fuel, repairs, insurance, and general wear and tear on the automobile.

    b. In addition to the mileage rate, the city will reimburse employees authorized to travel outside Monroe, driving personal or municipal vehicles, for tolls and reasonable parking expenses, when receipts are provided.

    c. The city retains the right to require employees who are reimbursed for work-related travel, to show proof of the following minimum levels of insurance coverage:

        1) Bodily Injury: $100,000/$300,000

        2) Property Damage: $25,000

d. An employee who uses his/her personal automobile to travel from home to a temporary assignment, rather than his/her regularly assigned work location, shall be allowed personal automobile expenses between home and the temporary assignment, or between the temporary assignment and the regular work location, whichever is less.

e. In order to be reimbursed for personal automobile use, employees shall complete the Personal Automobile Travel Expense Form. This form should be submitted to the Department Head for approval prior to submission to the Accounts Payable Division for payment.

J. Special Circumstances

This policy is intended to provide a basic framework governing the use of personal and municipal vehicles in the City of Monroe, and, as such, cannot contain procedures governing every situation that might arise. Employees seeking clarification of or exemption from the provisions of this policy should contact the City Administrator who will provide such clarification and may authorize exceptions to the policy under mitigating circumstances.

K. Sanctions

Failure to comply with any and all provisions of this policy may result in disciplinary action up to and including removal of city vehicle privileges, suspension, and/or termination from city service.

Exhibit A

Assignment of vehicles for twenty-four (24) hour use:

Position Title	Department	Destination
City Administrator	Administration	Walton County
Director of Code Enforcement	Code	Walton County
Director of Electric	Electric/Telecomm	Walton County
Assistant Director of Electric/Telecomm	Electric/Telecomm	Walton County
Cable TV Foreman	Cable	Walton County
Electric Foreman	Electric	Walton County
Locate Technician	Electric	Walton County
Fire Chief	Fire	Walton County
Director of Finance	Finance	Walton County
Police Chief	Police	Twenty (20) Mile Radius
Assistant Police Chief	Police	Twenty (20) Mile Radius
Sworn Police Officers	Police	Twenty (20) Mile Radius
Director of Streets and Transportation	Streets and Transportation	Walton County
Buildings and Grounds Foreman	Streets and Transportation	Walton County
Mechanic Foreman	Streets and Transportation	Walton County
Street Foreman	Streets and Transportation	Walton County
Director of Solid Waste	Solid Waste	Walton County
Director of Water/Gas	Water/Gas	Walton County
Assistant Director of Water/Gas	Water/Gas	Walton County
Gas Foreman	Gas	Walton County
Wastewater Foreman	Sewer	Walton County
Pump/Lift Station Serviceman	Sewer	Walton County
Water Foreman	Water	Walton County

Finance Committee Meeting

AGENDA

April 1, 2014

Item:

Approval - Electronic Check Transfer Agreement

Department:

Additional Information:

Financial Impact:

Budgeted Item:

Recommendation / Request:

Viewing Attachments Requires Adobe Acrobat. Click here to download.

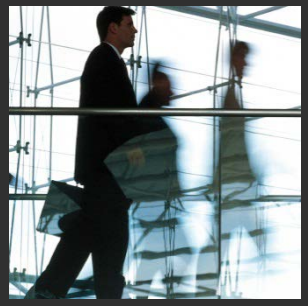
Attachments / click to download

Electronic Remittance ACH

Cover Memo

Item # 2

fiserv.


Electronic Remittance Overview

Beth Smith

Item # 2

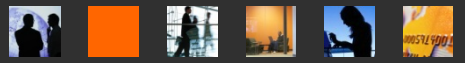
About Fiserv

- **Fiserv, Inc. (NASDAQ: FISV) is the leading global provider of information management and electronic commerce systems for the financial services industry. We are trusted by more than 16,000 clients worldwide including banks, credit unions and thrifts of all sizes; mortgage lenders and leasing companies; telecommunications and utility companies; brokerage and investment firms; healthcare and insurance providers; and retailers and municipalities.**

- **What we do**
  We help our clients solve complex business challenges. Maybe they want to grow deposits or do a better job of attracting and retaining customers. Maybe they are fighting fraud or need to get a handle on regulatory compliance. We provide the expertise and tools to help them deal with these types of issues.

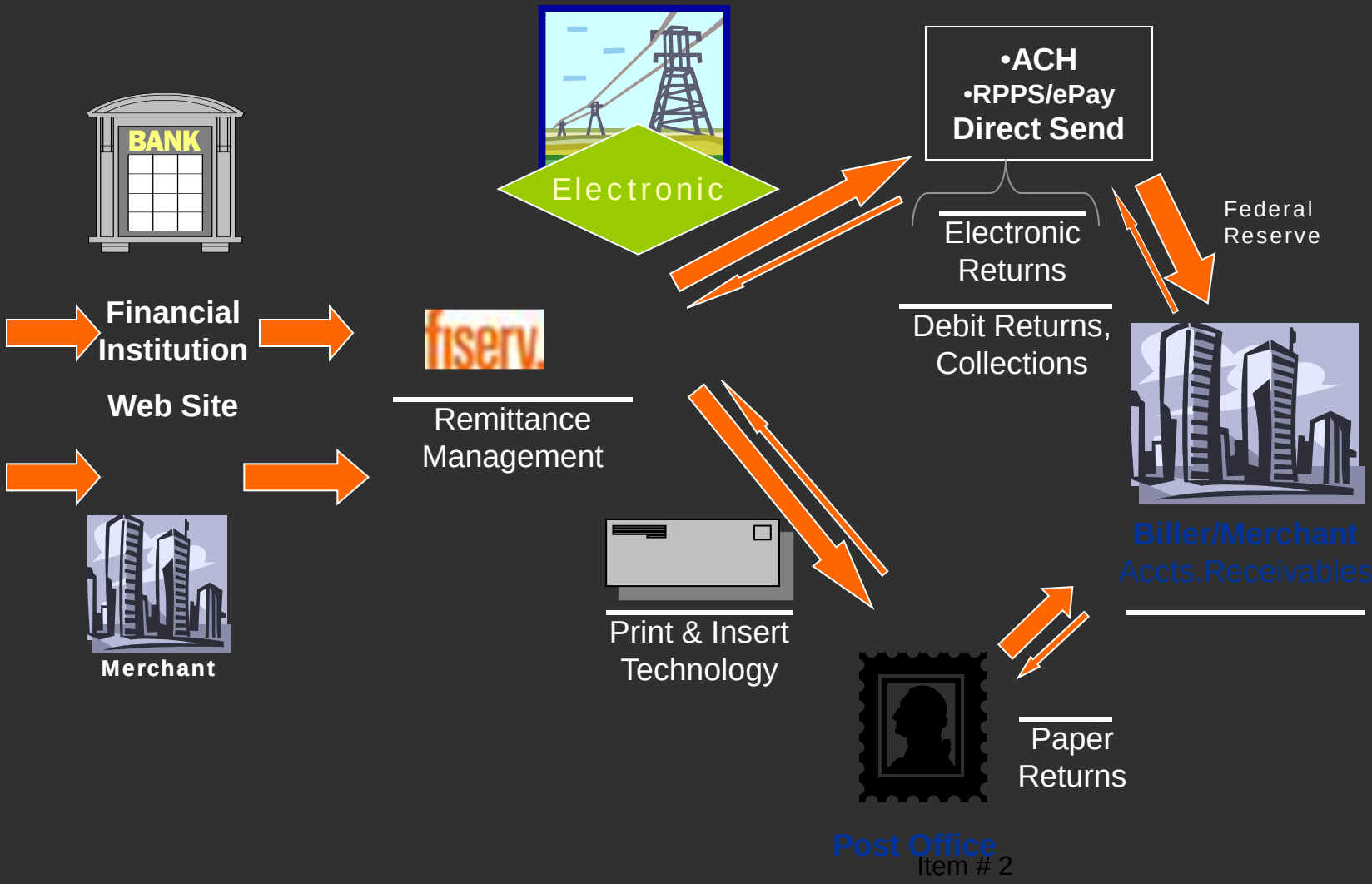
  - **Fiserv delivers financial services technology solutions in five areas of competence:**
  - **Payments – Solutions for optimizing all aspects of the payments mix to help create efficiency and drive growth**
  - **Processing Services – Solutions for reliably and securely managing account-based transactions**
  - **Risk & Compliance – Solutions for proactive risk prevention and mitigation**
  - **Customer & Channel Management – Solutions for attracting, retaining and growing customer relationships**
  - **Insights & Optimization – Solutions that help transform data from information to actionable business insights**

Item # 2



fiserv.

Payment Path—From Click to Pay

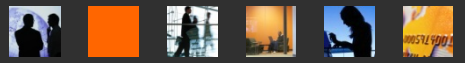


Item # 2

Value of Fiserv's Electronic Remittance Processing

- Fiserv consolidates payments from approximately 3,000 payment origination sites we support.
- Fiserv bears the cost of maintaining the infrastructure (database, ITO, connectivity to the Fed) to handle these payments.
- Fiserv maintains a merchant profile that contains remittance business rules, such as account schemes and remittance addresses in order to route transactions accurately.
- Fiserv has a department of associates responsible for corrections to data (bank or customer) that improve the electronic rate of payments (i.e., less paper, which is more expensive to process).

Item # 2

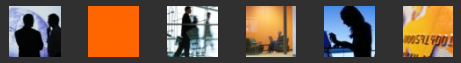


fiserv.

Benefits of Fiserv's Electronic Remittance Processing

- A merchant/biller does not need to manage individual remittance streams from each bank, brokerage and portal and saves the personnel, legal and infrastructure costs of processing paper transactions.
- A merchant/biller has the ability to receive funding for payment transactions at a faster rate then traditional paper payment processing would allow.
- A merchant/biller avoids costs by having Fiserv as a business partner, maintain the infrastructure (database, ITO, connectivity to the Fed) that enables processing of transactions
- A merchant/biller does not need to have relationships with all 3,000 payment origination sites to maintain their remittance profile for accurate routing of transactions from customers paying their bills online.
- A merchant/biller avoids the cost of supporting full time employees to process unpostable payments manually.

Item # 2



Fiserv Electronic Payment ACH Solution

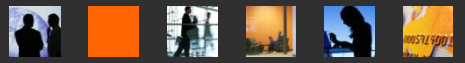
- **Fiserv will create a single deposit into a Checking account at the merchant/billers bank.**

- **Fiserv will send a fax or email remittance. The email is not a file that can be uploaded. The remittance containing the customer's name, account number, and amount paid is in the body of the email.**

- **The payment information will need to be manually posted to the customers account with your company. The email is sent non-secure via the internet.**

- **This is a free service. There are no set up fees, monthly or per transaction fees.**

Item # 2



Reversibility

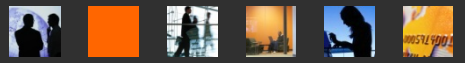
- **At the same time that Fiserv is depositing the funds for the payment into the account with the merchant/billers financial institution, we are debiting the customer that is sending the payment.**

- **The actual funds that Fiserv is depositing are from Fiserv's corporate bank account and Fiserv is processing the transaction in good faith with the belief that the person making the payment has the funds available in their bank account to reimburse Fiserv.**

- **A Reversibility agreement states that after we deposit the funds into the merchant/billers account, if we are unable to successfully debit the funds from the mutual customer, Fiserv will send the merchant/biller a reversal advice notification and retrieve the funds back from the merchant/biller.**

- **There are two reversibility options available:**
  - Auto debit - Fiserv retrieves the funds from an account at the merchant/biller's financial institution
  - Auto credit – The merchant/biller initiates a credit back to a designated bank account at Fiserv.

Item # 2



Contract process

To request the contract Fiserv would need the following information

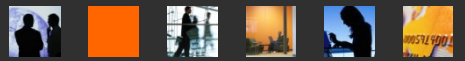
- **Corporate Name or Legal name**
- **Corporate Physical Address, City, State and Zip**
- **State of Incorporation**
- **Persons name that will be signing contracts**
- **Merchant/Biller Tax id #**
- **Fax number**
- **Which reversibility method the merchant/biller has chosen.**
- **Which method would the merchant/biller would like to use for reversed items, Fiserv to ACH Debit or ACH Credit?**

➢ **If the merchant/biller chooses debit reversibility they must supply the routing number and DDA number for the account that they would like debited.**

Next Steps:

- **Merchant/Biller returns signed completed and signed contract**
- **Merchant/Biller returns completed Needs Analysis document providing all information needed to create a merchant/biller profile as well as supplying merchant/biller contact information for implementation.**

Item # 2

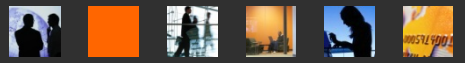


Implementation Process

- **Project manager and or Remittance Specialist is assigned once the contract is returned completed and signed.**
- **Project Manager/Remittance Specialist will contact merchant/biller to review set-up process and determine testing schedule if necessary.**
- **Project Manager will facilitate testing if needed.**
- **Merchant/Biller and Project Manager will agree upon a production date.**
- **Electronic Remittance processing will move into production for payments to be processed electronically.**

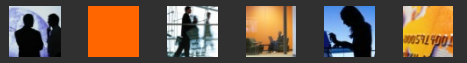
- ***Note: It is extremely important for the merchant/biller to maintain contact with Fiserv and respond quickly to the project manager with necessary information needed in order to meet production timelines for implementation.***

Item # 2



Questions

Item # 2



Finance Committee Meeting

AGENDA

April 1, 2014

Item:

Approval - Incident Response Plan for PCI Compliance

Department:

Additional Information:

Financial Impact:

Budgeted Item:

Recommendation / Request:

Viewing Attachments Requires Adobe Acrobat. Click here to download.

Attachments / click to download

Incident Response Plan

Cover Memo

Item # 3

Incident Response Plan
for PCI-DSS Compliance

City of Monroe, Georgia
Information Technology Division
Finance Department

I. Policy

The City of Monroe Information Technology Administrator is responsible for responding to reports of incidents, compromises, and breaches of City of Monroe computers, data, and network resources. The purpose of the Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements to address instances of unauthorized access to or disclosure of City information. The Incident Response Plan defines the policy, roles and responsibilities for the involved personnel when reacting to an information security threat.

The primary emphasis of activities described within this plan is the return to a secure state as quickly as possible, while minimizing the adverse impact to the City. Depending on the circumstances, the Information Technology Administrator (IT Administrator) may decide to modify or bypass one or more of the procedures outlined in this plan in response to a particular security incident, with the understanding that the IT Administrator will take all reasonable steps to investigate and resolve any security issues. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, as well as classification of the incident.

The City shall provide timely and appropriate notice to affected individuals and departments when there has been a security incident, a compromise, or a breach involving city data, computers, or networks. The IT Administrator, Finance Department Director, and the City Administrator shall be responsible for reviewing breaches to determine whether notification is required, and directing responsible departments in complying with the notification obligation. All known or suspected security incidents must be reported to the IT Administrator. Suspected incidents can be reported at administrator@monroega.gov or through the City of Monroe Call Center.

II. Definitions

Security Incident - A vulnerability which may compromise the security of city resources has been discovered and is underway. Generally, this means a weakness in intrusion prevention has been found, an attempted exploit has taken place, or reconnaissance by a hacker has been thwarted. Examples include systematic unsuccessful attempts to gain entry, a PC or workstation infected with a virus, worm, Trojan, botnet, or other malware that has been discovered and removed.

Security Compromise – An escalation of a security incident where the attacker has gained control of a city account, system, or device, and is leveraging that position to control and utilize compromised resources for the purpose of unauthorized acquisitions. At this point, it has been determined that data has not been compromised or stolen.

Security Breach – A confirmed, unauthorized acquisition, modification or destruction of city or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.

Private data - Data about individuals that is classified by law as private or confidential and is maintained by the city in electronic format or medium. “Private data” means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

Unauthorized acquisition - For the purposes of this plan, this means that a person has obtained city data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-city purposes

Systematic unsuccessful attempts - continual probes, scans, or login attempts where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

City of Monroe Resources **or** ***Systems*** includes all city-owned computers, peripherals, networks, and related equipment and software, and the voice and data communications infrastructure.

III. General Incident Response Procedures

1) Intrusion attempts, security breaches, or other technical security incidents perpetrated against city-owned computing or networked resources must be reported to the IT Administrator. Functional unit managers and/or supervisory personnel must:

a) Report any security incidents in order to obtain assistance, advice, or to file the incident.
b) Report any systematic unsuccessful attempts (e.g., login attempts, probes, or scans).
c) Where feasible given the circumstances, reports should be sent as soon as the situation is detected; minimally the report should be sent as soon as possible thereafter.

2) Upon receiving a report of a security incident, the IT Administrator will:

a) Ensure that appropriate information is collected and logged per applicable procedures.
b) Immediately assess actual or potential disclosure or inappropriate access to institutional or personal information.
c) Report the situation to the Finance Director and/or City Administrator.
d) Consult with and/or assign the incident to other personnel for further investigation as necessary.
e) Provide preliminary advice or comment to the functional unit as required.
f) Initiate steps to warn other City of Monroe systems personnel if it appears that the situation has the potential to affect other city systems as well.
g) Perform or assist in any subsequent investigation and/or perform computer forensics as required.
h) If circumstances dictate, report and/or consult with city Legal Counsel, city Police, Internal Auditors, city Public Relations, or other appropriate agencies.
i) Ensure that appropriate records are filed.
j) Confirm actual or probable disclosure or inappropriate access to institutional or personal information.
k) Invoke formal incident response procedures commensurate with the situation.

3) In order to protect city data and systems, as well as to protect threatened systems external to the city, the IT Administrator may block, or place restrictions on technology services provided using any city owned systems and networks. Specifically:

a) Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or use of certain applications known to cause security problems.
b) Restrictions may be permanently deployed based on a continuing threat or risk after appropriate consultation with affected constituents, or they may be temporarily deployed, without prior coordination, in response to an immediate and serious threat.
c) Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the affect on city functions caused by the restriction approaches or exceeds risk associated with the threat, as negotiated between the affected constituents and the IT Administrator.

4) In order to protect city data and systems, as well as to protect threatened systems external to the city, the IT Administrator may unilaterally choose to isolate a specific city system from other city or external networks, given:

a) Information in-hand reasonably points to the system as having been compromised.
b) There is ongoing activity associated with the system that is causing or will cause damage to other city systems and/or data, or the assets of other internal or external agencies, or where there is a medium-to-high risk of such damage occurring.
c) All reasonable attempts have been made to contact the responsible systems personnel or department management, or such contact has been made where the technician or department managers are unable to (or choose not to) resolve the problem in a reasonable time.
d) Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the IT Administrator.
e) Advance consultation with the appropriate security contractor, or Legal Counsel, where practical and where circumstances warrant.

5) The reaction to a reported security vulnerability directly corresponds to the potential for damage to the local system (or adjacent systems) or inappropriate disclosure or modification of data. The risk levels are characterized as:

a) Very High Risk, response is immediate:

1. Damage to the system or data is occurring, or
2. Attempts to exploit the vulnerability on that system are occurring, or
3. The vulnerability is currently being actively exploited against other similar technologies within the City; probable damage to systems and data is being experienced in those other incidents.

b) High Risk, response is within 1 hour:

1. The vulnerability is known to exist on the system;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. Damage to systems and data are being experienced in those other incidents.

c) Medium Risk, response should be within 4 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. There is some potential for damage to systems and data.

d) Low Risk, response should be within 8 hours:

1. The system is susceptible to the vulnerability given that the system is configured incorrectly;
2. The exposure is currently being actively exploited against other similar technologies external to the City;
3. Damage to systems and data is possible but is not considered likely.

6) In the event of a significant series of incidents, a compromise, or a breach, the entire episode and response are reviewed to determine which parts of the incident response plan worked correctly. The "lessons learned" will be part of an After Action Review to determine areas that need to be changed (policies, system configurations, etc.).

IV. Procedures for System Users and Administrators

1) **Don't panic.** Be as calm and methodical as you can, and think about your course of action. Involve a second person to assist and observe all actions you take.

2) **Do a quick assessment.** Do not immediately shut down the machine, as you may lose important information. If the machine is being used to attack others, or if the attacker is actively using or damaging the machine, you may need to disconnect it from the network. If this does not appear to be the case, leave the system intact for the moment.

3) **Report the problem.** Call the IT Administrator or the City of Monroe Call Center, and request an emergency system security check. Every effort will be made to

respond as quickly as possible, as well as, respect the confidentiality of incident information.

4) **Gather all the relevant information you can find.** This may include, but is not limited to, system logs, directory listings, electronic mail files, screen prints of error messages, and activity logs. Copy them to a safe location (that will not be deleted or over-written), so that we can study them later.

5) **Take notes.** Have your partner record all relevant information, including things you observed, actions you took, dates and times, and the like. It is best to log your activities as they occur. Over time, your actions and the order in which they were executed will not be easily remembered. The preservation of information is critical to any legal action that may take place at a later date.

6) **Change account passwords.** All system accounts that were involved with the incident should have new passwords requested. Exceptions to this rule are accounts which are authenticated with tokens or certificates, in which case the PIN or pass-phrase for them should be changed. **Never** share your password (pin, or pass-phrase) with anyone, for any reason.

7) **Change the status of accounts, if necessary.** In the event that a system administrator detects a problem with a system, or user activity on a system, a quick way to stop the unwanted activity is to "disable" an account, by restricting logins to it. This is *not* deleting the account, but is merely making the account temporarily unusable through Active Directory.

8) **Stop rogue service(s), if necessary.** In the event that a system compromise or denial-of-service attack is underway, and you are unable to stop or kill the service(s), you may need to disconnect the machine from the network to get them stopped.

Finance Committee Meeting

AGENDA

April 1, 2014

Item:

Approval - IT Policy Addendum for PCI Compliance

Department:

Additional Information:

Financial Impact:

Budgeted Item:

Recommendation / Request:

Viewing Attachments Requires Adobe Acrobat. Click here to download.

Attachments / click to download

IT Policy Addendum

Cover Memo

Item # 4

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.