RESOLUTION

REGARDING SECURITY OF SENSITIVE AND CONFIDENTIAL INFORMATION AND BREACH RESPONSE PLAN

WHEREAS, the City of Marion, in its normal course of business collects identifying information from customers, employees, vendors, and other individuals, and

WHEREAS, this information is confidential, and failing to secure such information could be detrimental to such persons, and

WHEREAS, G.S 132-1 states the governing body has an obligation to secure and limit access to information involving customers and employees, and

WHEREAS, in accordance with the Federal Trade Commission's Fair and Accurate Credit Transaction Act of 2003, the Identity Protection Act of 2005, NCGS 75-60 of the Identity Theft Protection Act, NCGS 14-113.20 Identity Theft and NCGS 132-1.10 of the Public Records Act, the City is required to safeguard certain information of customers, employees, vendors, and other individuals who provide information to the City that is covered by the Act, and

WHEREAS, the Federal Trade Commission requires the adoption of identity theft programs in place by November 1, 2008

NOW, THEREFORE, BE IT RESOLVED, that the City Council of the City of Marion does hereby adopts this resolution and the attached Policy: Security of Sensitive and Confidential Information and Breach Response Plan the purpose of which is to communicate to employees and third parties their responsibility for protecting sensitive and confidential information pursuant to the Act and a response plan in the event that there is a breach of information subject to the Act.

ADOPTED this the 7th day of October, 2008.

Resolution Number: R-08-10-07-1

City of Marion
Administrative Policy

Policy: Security of Sensitive and Confidential Information and Breach Response Plan

SECTION 1. Purpose

In accordance with the Federal Trade Commission's Fair and Accurate Credit Transactions Act of 2003, the Identity Protection Act of 2005, North Carolina General Statutes (N.C.G.S) 75-60 of the Identity Theft Protection Act, N.C.G.S 14-113.20 Identity Theft, and N.C.G.S 132-1.10 of the Public Records Act (together, the "Act"), the City is required to safeguard certain information of customers, vendors, employees, and other individuals who provide information to the City that is covered by the Act. The purpose of this policy is to communicate to employees and third parties their responsibility for protecting sensitive and confidential information pursuant to the Act and a response plan in the event that there is a breach of information subject to the Act.

SECTION 2. Definitions

Sensitive Information – Information that is identifying information according to the Act and through contractual obligations related to merchant services (credit card acceptance). The following are specifically identified as sensitive information:

1. Social security and employer taxpayer identification numbers
2. National and international identification
3. Drivers license, State identification card, or passport numbers
4. Credit card and debit card numbers
5. Savings and checking account numbers
6. Personal Identification (PIN) Code
7. Passwords
8. Electronic identification numbers, electronic mail names or addresses, internet account numbers, or internet identification names
9. Customer credit information (credit history, pay arrangements, and financial transactions)
10. Parent's legal surname prior to marriage
11. Any other numbers or information that can be used to access a person's financial resources.
12. Digital signatures

13. Biometric data
14. Fingerprints
15. A persons first name or first initial and last name in combination with identifying information

Confidential information – Under State statute (N.C.G.S 132-1), the City also has an obligation to secure and limit access to other information involving customers and employees. The following are identified as confidential information, although this is not a complete listing:

1. Communication with legal counsel
2. State and local tax information that contain information about a taxpayer's income or receipts except as provided in G.S. 153A-148.1 and G.S. 160A-208.1.
3. Public enterprise billing information (utility customer data)
4. Records of criminal investigations conducted by public law enforcement agencies
5. Names, addresses, telephone numbers, or email addresses that are contained in the 911 database, emergency notification system, or reverse 911 system.
6. Emergency response plans
7. Economic development incentives

Security Breach – A breach is considered to have taken place if any sensitive or confidential information is suspected to have been stolen, viewed, copied, or otherwise compromised by an unauthorized individual or if it is suspected that information has been lost and could be accessed by unauthorized individual(s). A breach of information can occur physically or virtually via technology. Access and use of sensitive or confidential information by an employee or agent of the City for a legitimate purpose is not a security breach, provided that the sensitive or confidential information is not used for a purpose other than a lawful purpose and is not subject to further unauthorized disclosure.

SECTION 3. Responsibilities of Departments

3.1 Each department will develop and maintain a standard procedure to provide staff with specific guidance on the protection of sensitive and confidential information applicable to the department. Departmental procedures will supplement, but not supersede this policy or applicable laws.

3.2 Each department will ensure that service providers who are in contact with sensitive or confidential information are aware of security

requirements, as well as the need for confidentiality, through proper contractual agreements and arrangements.

3.3 Department heads are responsible for determining which employees are authorized to access and handle sensitive and confidential information and the department head must ensure that the authorized employees are trained to handle such information in accordance with this policy.

3.4 All employees who manage and work with sensitive and confidential information are required to read and sign the Sensitive Information User Agreement which will be maintained in the employees personnel file.

3.5 All third party contractors who may have access to sensitive and confidential information are required to read and sign the Sensitive Information Service Agreement which will be maintained with the contract.

SECTION 4. Managing, maintaining, and storing sensitive and confidential information

4.1 Employees who have access to sensitive and confidential information are required to create, handle, maintain, and dispose of such information with prudent care in order to ensure proper security. Access to sensitive and confidential information will be limited and only provided in order for authorized employees and contractual third parties to perform essential tasks for City business.

4.2 The following procedures should be followed while creating, handling, maintaining, storing, and disposing of sensitive information.

1. Enter information directly to a final destination (i.e. computer system) and refrain from documenting the information in other areas.
2. If sensitive information is written on paper for reference, shred immediately upon recording the information in the final destination.
3. Electronic payment data should be handled by authorized personnel and only the last 4 digits of the customer's credit or debit account number should be visible on reports.
4. Sensitive information should not be included on e-mails.

5. Sensitive information should not be included on printed reports except as needed for the performance of essential tasks.
6. Maintain documents that contain sensitive information in a secured room and limit access to the area.
7. If possible, utilize encryption to secure information in the database or storage system.
8. Do not leave a computer unattended if sensitive information could be accessed by unauthorized individuals. While away from the computer, log off or lock the workstation.
9. Do not store files with sensitive information on laptops or on flash drives unless the information and the device can be secured and not accessible to unauthorized individuals.
10. Take reasonable measures when destroying sensitive data that will prohibit the information from being read or reconstructed. Documents with sensitive data should be shredded by the individual who has authorized access to the data or by another employee while in the presence of the authorized employee. The City may enter into a written contract with a third party in the business of record destruction to destroy sensitive information in a manner consistent with this policy.

4.3 In order to protect sensitive and confidential information, the City will only release sensitive information to the account holder or individual(s) who own the information upon confirmation of personal identifying information or a valid picture ID. The confirmed account holder or individual may authorize the release of sensitive information to a third party. Confidential information will only be released in accordance with state statute. The only exception will be the release of specified information pursuant to a court order, warrant, subpoena or other requirement by law.

SECTION 5. Identify Theft Risk

5.1 The City has a responsibility to define high risk areas for identity theft and identify potential threats for identity theft known under the Act as red flags. The red flags are indicators that sensitive information is being fraudulently used. This policy in combination with department specific guidelines should help to detect a potential for identify theft and unauthorized use of information.

5.2 The following are red flags that have been identified as indicators that sensitive information is being used fraudulently. Red flags are most commonly associated with activity on customer accounts (utilities, taxes, activity registrations, vendors). Other red flags may exist that are unique to a department and should be included in departmental guidelines.

1. The customer or individual provides notice that they are a victim of identify theft
2. A consumer reporting agency or service provider has provided an alert, notification, or other warning
3. Unusual number of recent and significant inquiries
4. Unusual or significant change in recently established credit or financial relationships
5. Conflicting names on identification and other documentation
6. Documents provided appear to have been altered or forged
7. Picture identification is not consistent with the appearance of the individual presenting the identification or the physical description on the identification does not match
8. Shortly after establishing an account, there is a request to change a mailing address or to add authorized users to the account
9. Personal identifying information provided is not consistent with other external information sources
    a. Social security number does not match or is listed on the Social Security Administration's death master file
    b. Address does not match or is fictitious, a mail drop, or prison
    c. The phone number is invalid or associated with a pager or answering service
    d. Authenticating information (i.e. PIN, password) provided is incorrect
    e. Name on credit card or check does not match name on account or names associated with the account.

5.3 Upon identification of a red flag indicating a potential risk of identify theft; staff should notify their immediate supervisor in person or by telephone to determine the validity of the red flag. Once an identify theft risk is confirmed, staff should respond in accordance with the breach response plan (Section 6).

SECTION 6. Sensitive and Confidential Information Breach Response Plan

6.1 Step 1. Identify that a breach of sensitive or confidential information has occurred.

Physical Breach - The following are indications that there has been unauthorized access to sensitive and confidential information via a physical breach. Other activities may occur that are also physical breaches that are not included in the listing.

a. Evidence of lock tampering on file cabinets or office doors
b. Evidence of unauthorized entry in an area where sensitive and confidential information is stored
c. Missing files or documents that contain sensitive information

Technology Breach - The following are indications that there has been unauthorized access to sensitive and confidential information via a technology breach. Other activities may occur that are also technological breaches that are not included in the listing.

a. Unknown or unauthorized name in the computer logon window
b. Disconnected computer cables or power cables
c. Missing computer equipment (desktop, laptop)
d. Evidence that electronic files have been accessed by unknown or unauthorized individuals or are missing
e. Devices or media attached to the computer that are not known or authorized
f. Unusual programs running, icons, or windows that appear that are not known and are not part of the normal work process
g. Any other suspicious activity which indicates an attempt to use technology without approval

6.2 Step 2. Notify the appropriate internal and external contacts.

Internal notification – Any City employee who becomes aware of a suspected or actual security breach must notify their immediate supervisor. The immediate supervisor will notify department management who is responsible for further investigation and notification. If the breach involves electronic equipment, the Information Systems Manager should be notified by telephone or in person.

External notification – The City is required to notify affected individuals of actual security breaches. Each suspected breach will be reviewed by the city manager's office, the department where the

breach occurred, law enforcement, and Information Systems (if applicable) to determine the appropriate action that will include the following:

a. Notify the affected individuals without unreasonable delay providing information in general terms about the incident, the type of sensitive information that was subject to the unauthorized access, the actions that the City will take to protect the information from further access, a telephone number that the person may call for further information and assistance, and advice that directs the person to remain vigilant by reviewing account statements and monitoring free credit reports.
b. Providing affected individuals with information about how to alert credit agencies to potential fraud and identity theft.
c. Notice to affected individuals may be provided by one or more of the following methods:
    a. Written notice
    b. Electronic notice for those individuals for whom the City has a valid email address and who have agreed to receive communications electronically
    c. Telephonic notice provided the contact is made directly with the affected persons and appropriately documented by the City.
d. A substitute notice may be given if the cost of providing the notice exceeds $250,000, the number of affected persons is greater than 500,000, or the City does not have the necessary contact information to notify the individual in any of the aforementioned manners. A substitute notice will include posting a notice on the City's website and notifying major statewide media.
e. If a security breach involves more than 1,000 persons, the City will provide written notice of the timing, distribution, and content of the notice to the Consumer Protection Division of the North Carolina Attorney General's Office, as well as to all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S. C. 1681a(p).
f. Notice may be delayed if law enforcement informs the City that disclosure of the breach would impede a criminal investigation or jeopardize national security. Such request by law enforcement must be documented in writing.

6.3 Step 3. Implement Plan

The City Manager will designate a security breach response team to investigate and handle the breach until such time that the threat has ended and affected individuals and agencies are notified.

Technology Breach Response – The Information Technology employee or contracted provider is responsible for the following response upon being notified of a technology security breach by the Finance Director or City Manager.

a. The Information Technology employee, Finance Director or City Manager will notify computer users that a technology breach has occurred and the breach response plan is being implemented
b. The Information Technology employee or contracted provider will secure the computer infrastructure as deemed appropriate which may include but is not limited to disconnecting network connections to outside locations, disconnecting servers or any other device on the network until the breach is isolated.
c. Information Technology employee or contracted provider will preserve evidence that may be needed by law enforcement for investigative purposes

6.5 At least annually, the City will review all incidents of potential or actual security breaches and report findings and recommendations to the City Council.

SENSITIVE INFORMATION USER AGREEMENT

I have read the Security of Sensitive and Confidential Information and Breach Response Plan policy for the City of Marion, North Carolina and understand how to properly manage, maintain, store, and dispose of sensitive and confidential information at the City of Marion, North Carolina. I will abide by the policy and will handle sensitive and confidential information with prudent care in order to ensure proper security of the information.

In the event of a suspected or actual breach of sensitive and confidential information, I will notify my immediate supervisor without delay and follow the breach response plan.

I understand that negligent handling or inappropriate use of the City's sensitive and confidential information will be subject to disciplinary action up to and including dismissal and may be criminally and civilly prosecuted as allowed by law.

I have read, understand, and agree to the conditions above.

Printed Name of Employee: _____

Department: _____

Signature of Employee: _____

Date Signed: _____

SENSITIVE INFORMATION SERVICE AGREEMENT

I, _____, an authorized representative of _____ ("Company"), hereby acknowledge that I have read and will adhere to the requirements listed below as they apply to the services procured by the City of Marion, North Carolina ("City").

1. The appointed representative(s) of the Company have read the City of Marion, North Carolina administrative policy III.14 Security of Sensitive and Confidential Information and Breach Response Plan.

2. The Company accepts responsibility for the security of sensitive and confidential information in their possession.

3. Data can only be used to complete the service as described by the City for which the Company was engaged to perform.

4. If the Company is providing service that is related to a key function of the City, the Company must assure business continuity in the event of a major disruption, disaster, or failure as provided for by contract.

5. If a security intrusion has been detected, the Company will notify the City immediately. If the Company has placed sensitive data on their system and the system has been breached, the Company will allow their system to be thoroughly reviewed at the Company's expense. This review may be conducted by the City or an appointed representative. In the event the intrusion is related to credit card numbers, the review may be conducted by a Payment Card Industry representative and will validate compliance with Payment Card Industry Security Standards for protecting cardholder data.

Name of Company: _____
Address: _____
_____

Name of Representative: _____
Title: _____

Signature: _____
Date: _____