

## **IDENTITY THEFT PREVENTION POLICY**

### **SECTION 1: BACKGROUND**

The risk to the municipality, its employees and customers from data loss and identity theft is of significant concern to the municipality and can be reduced only through the combined efforts of every employee and contractor.

### **SECTION 2: PURPOSE**

The municipality adopts this sensitive information policy to help protect employees, customers, contractors and the municipality from damages related to the loss or misuse of sensitive information.

This policy will:

1. Define sensitive information;
2. Describe the physical security of data when it is printed on paper;
3. Describe the electronic security of data when stored and distributed; and
4. Place the municipality in compliance with state and federal law regarding identity theft protection.

This policy enables the municipality to protect existing customers, reducing risk from identity fraud, and minimize potential damage to the municipality from fraudulent new accounts. The program will help the municipality:

1. Identify risks that signify potentially fraudulent activity within new or existing covered accounts;
2. Detect risks when they occur in covered accounts;
3. Respond to risks to determine if fraudulent activity has occurred and act if fraud has been attempted or committed; and
4. Update the program periodically, including reviewing the accounts that are covered and the identified risks that are part of the program.

### **SECTION 3: SCOPE**

This policy and protection program applies to employees, contractors, consultants, temporary workers, and other workers at the municipality, including all personnel affiliated with third parties.

### **SECTION 4: POLICY**

#### **4.A: Sensitive Information Policy**

##### **4.A.1: Definition of Sensitive Information**

Sensitive information includes the following items whether stored in electronic or printed format:

##### **4.A.1.a: Credit card information, including any of the following:**

1. Credit card number (in part or whole)
2. Credit card expiration date
3. Cardholder name
4. Cardholder address

##### **4.A.1.b: Tax identification numbers, including:**

1. Social Security number
2. Business identification number
3. Employer identification numbers

##### **4.A.1.c: Payroll information, including, among other information:**

1. W-2 forms
2. W-4 forms

##### **4.A.1.d: Bank account information, including:**

1. Bank account name
2. Bank account number

3. Bank routing number

4.A.1.e: Medical information for any employee or customer, including but not limited to:

1. Doctor names and claims
2. Insurance claims
3. Prescriptions
4. Any related personal medical information

4.A.1.f: Other personal information belonging to any customer, employee or contractor, examples of which include:

1. Date of birth
2. Service location & mailing address
3. Phone numbers
4. Maiden name
5. First, middle & last names
6. Customer & account numbers
7. Nearest relative's first & last name, address and phone number

4.A.1.g: Municipal personnel are encouraged to use common sense judgment in securing confidential information to the proper extent. Furthermore, this section should be read in conjunction with the Ohio Open Records Law and the municipality's open records policy. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact their supervisor.

**4.A.2: Hard Copy Distribution**

Each employee and contractor performing work for the municipality will comply with the following policies:

1. File cabinets, desk drawers, overhead cabinets, safes and any other storage space containing documents with sensitive information will be locked when not in use.

2. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised. The Utilities Business Office, Information Technology and Income Tax work areas will be secured by an alarm system at the end of each workday.
3. Desks, workstations, work areas, printers and fax machines, and common shared work areas will be cleared of all documents containing sensitive information when not in use.
4. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
5. When documents containing sensitive information are discarded they will be immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Municipal records, however, may only be destroyed in accordance with the city's records retention policy.

#### **4.A.3: Electronic Distribution**

Each employee and contractor performing work for the municipality will comply with the following policies:

1. Internally, sensitive information may be transmitted using approved municipal e-mail. All sensitive information must be encrypted when stored in an electronic format and, if received or transmitted, only secure connections will be used.
2. A statement such as this should be included in the e-mail:

*Portions of this message may be confidential under an exemption to Ohio's public records law or under a legal privilege. If you have received this message in error or due to an unauthorized transmission or interception, please delete all copies from your system without disclosing, copying, or transmitting this message.*

#### **4.A.4: Information Technology Security**

The municipality will complete ongoing monitoring of its information systems in order to prevent the possibility of identity theft through access to/through its computer software and hardware. This monitoring will include, but not be limited to the following:

1. Testing and installation of critical systems patches to remove software defects which would create weaknesses in the security of either software or hardware which if left unresolved would allow access to "identifying information".
2. The computer network will have a firewall and wireless networks will be secured. Anti-virus and anti-spyware programs will be run on network servers daily. Maintenance of central log files of security-related information to monitor activity on the network will occur daily as well as the monitoring of incoming and outgoing traffic for signs of a data breach.

3. All computers will have the appropriate password protocol and software and/or hardware to allow the machine to be locked down. All laptops must be encrypted.
4. An annual audit of the computer systems security will be performed by the Auditor of the State of Ohio.

## **SECTION 5: ADDITIONAL IDENTITY THEFT PREVENTION PROGRAM**

**If the municipality maintains certain covered accounts pursuant to federal legislation, the municipality may include the additional program details.**

### **5.A: Covered Accounts**

A covered account includes any account that involves or is designed to permit multiple payments or transactions. Every new and existing customer account that meets the following criteria is covered by this program:

1. Business, personal and household accounts that involve multiple payments or transactions for which there is a reasonably foreseeable risk of identity theft; or
2. Business, personal and household accounts for which there is a reasonably foreseeable risk to the safety or soundness of the municipality from identity theft, including financial, operational, compliance, reputation, or litigation risks.

### **5.B: Red Flags - Suspicious Documents**

**5.B.1:** Documents provided for identification that appear to have been altered, forged or inauthentic.

**5.B.2:** The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.

**5.B.3:** Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.

**5.B.4:** Other information on the identification is not consistent with readily accessible information that is on file with the municipality.

**5.B.5:** An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.

### **5.C: Red Flags - Suspicious Personal Identifying Information**

**5.C.1:** Personal identifying information provided is associated with known fraudulent activity as indicated by internal or third-party sources used by the municipality. For example, the address on an application is the same as the address provided on a fraudulent application

**5.C.2:** Personal identifying information provided is of a type commonly associated with fraudulent activity as indicated by internal or third-party sources used by the municipality. For example:

- The address on an application is fictitious, a mail drop, or a prison; or
- The phone number is invalid or is associated with a pager or answering service.

**5.C.3:** The social security number provided is the same as that submitted by other persons opening an account or other customers.

**5.C.4:** The address or telephone number provided is the same as or similar to the address or telephone number submitted by an unusually large number of other customers or other persons opening accounts.

**5.C.5:** The customer or the person opening the covered account fails to provide all required personal identifying information.

**5.C.6:** Personal identifying information provided is not consistent with personal identifying information that is on file with the municipality.

**5.C.7:** When using security questions (mother's maiden name, pet's name, etc.), the person opening the covered account or the customer cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.

#### **5.D: Red Flags - Unusual Use Of, Or Suspicious Activity Related To, The Covered Account**

**5.D.1:** Shortly following the notice of a change of address for a covered account, the municipality receives a request for new, additional, or replacement goods or services, or for the addition of authorized users on the account.

**5.D.2:** A new revolving credit account is used in a manner commonly associated with known patterns of fraud patterns. For example, the customer fails to make the first payment or makes an initial payment but no subsequent payments

**5.D.3:** A covered account is used in a manner that is not consistent with established patterns of activity on the account. There is, for example:

- Nonpayment when there is no history of late or missed payments;
- A material change in purchasing or usage patterns

**5.D.4:** A covered account that has been inactive for a reasonably lengthy period of time is used (taking into consideration the type of account, the expected pattern of usage and other relevant factors).

**5.D.5:** Mail sent to the customer is returned repeatedly as undeliverable although transactions continue to be conducted in connection with the customer's covered account.

**5.D.6:** The municipality is notified that the customer is not receiving paper account statements.

**5.D.7:** The municipality is notified of unauthorized charges or transactions in connection with a customer's covered account.

**5.D.8:** The municipality receives notice from customers, victims of identity theft, law enforcement authorities, or other persons regarding possible identity theft in connection with covered accounts held by the municipality

**5.D.9:** The municipality is notified by a customer, a victim of identity theft, a law enforcement authority, or any other person that it has opened a fraudulent account for a person engaged in identity theft.

## **SECTION 6: DETECTING RED FLAGS**

### **6.A: New Accounts**

In order to detect any of the Red Flags identified above associated with the opening of a new account, personnel will require identifying information such as first, middle and last name, service location and mailing address, phone number, social security number and nearest relative's name, address and phone number.

### **6.B: Existing Accounts**

In order to detect any of the Red Flags identified about for an existing account, personnel will take the following steps to monitor transactions with an account:

**6.B.1:** Verify the identification of customers if they request information (in person, via telephone, facsimile or e-mail).

**6.B.2:** Verify the validity of requests to change billing addresses.

**6.B.3:** Verify changes in banking information given for billing and payment purposes.

## **SECTION 7: RESPONDING TO RED FLAGS**

**7.A:** Once potentially fraudulent activity is detected, an employee must act quickly as a rapid appropriate response can protect customers and the municipality from damages and loss.

**7.A.1:** Once potentially fraudulent activity is detected, gather all related documentation and write a description of the situation. Present this information to the designated authority for determination.

**7.A.2:** The designated authority will complete additional authentication to determine whether the attempted transaction was fraudulent or authentic.

**7.B:** If a transaction is determined to be fraudulent, appropriate actions must be taken immediately. Actions may include:

1. Canceling the transaction, refusing to open an account, closing the account or reopen account with new customer number;
2. Notifying and cooperating with appropriate law enforcement;
3. Determining the extent of liability of the municipality; and
4. Notifying the actual customer that fraud has been attempted.

## **SECTION 8: PERIODIC UPDATES TO PLAN**

**8.A:** At periodic intervals established in the program, or as required, the program will be re-evaluated to determine whether all aspects of the program are up to date and applicable in the current business environment.

**8.B:** Periodic reviews will include an assessment of which accounts are covered by the program.

**8.C:** As part of the review, red flags may be revised, replaced or eliminated. Defining new red flags may also be appropriate.

**8.D:** Actions to take in the event that fraudulent activity is discovered may also require revision to reduce damage to the municipality and its customers.

## **SECTION 9: PROGRAM ADMINISTRATION**

### **9.A: Involvement Of Management**

1. The Identity Theft Prevention Program shall not be operated as an extension to existing fraud prevention programs, and its importance warrants the highest level of attention.
2. The Identity Theft Prevention Program is the responsibility of the governing body. Approval of the initial plan must be appropriately documented and maintained.

3. Operational responsibility of the program is delegated to the Assistant Municipal Administrator.

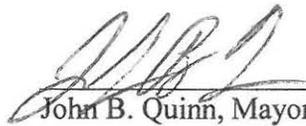
#### **9.B: Staff Training**

1. Staff training shall be conducted for all employees, officials and contractors for whom it is reasonably foreseeable that they may come into contact with accounts or personally identifiable information that may constitute a risk to the municipality or its customers.
2. The Assistant Municipal Administrator is responsible for ensuring identity theft training for all requisite employees and contractors.
3. Employees will receive on-going training in all elements of this policy.
4. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

#### **9.C: Oversight Of Service Provider Arrangements**

1. It is the responsibility of the municipality to ensure that the activities of all service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft.
2. A service provider that maintains its own identity theft prevention program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
3. Any specific requirements should be specifically addressed in the appropriate contract arrangements.

This resolution will take effect immediately upon its passage, the public welfare requiring it.

  
John B. Quinn, Mayor

5/1/09  
Date