Model Identity Theft Policy and Resolution: Sections 1-4

Dear Reader:

The following document was created from the MTAS website (mtas.tennessee.edu). This website is maintained daily by MTAS staff and seeks to represent the most current information regarding issues relative to Tennessee municipal government.

We hope this information will be useful to you; reference to it will assist you with many of the questions that will arise in your tenure with municipal government. However, the *Tennessee Code Annotated* and other relevant laws or regulations should always be consulted before any action is taken based upon the contents of this document.

Please feel free to contact us if you have questions or comments regarding this information or any other MTAS website material.

Sincerely,

The University of Tennessee
Municipal Technical Advisory Service
1610 University Avenue
Knoxville, TN 37921-6741
865-974-0411 phone
865-974-0423 fax
www.mtas.tennessee.edu

Table of Contents

Model Identity Theft Policy and Resolution: Sections 1-4

Reference Number: MTAS-1257

Model Identity Theft Policy and Adopting Resolution

_____, Tennessee
RESOLUTION NO. _____

A RESOLUTION ADOPTING AN IDENTITY THEFT POLICY

WHEREAS, The Fair and Accurate Credit Transactions Act of 2003, an amendment to the Fair Credit Reporting Act, requires rules regarding identity theft protection to be promulgated; and

WHEREAS, Those rules became effective November 1, 2008, and require municipal utilities and other departments to implement an identity theft program and policy, and

WHEREAS, The _____ (insert governing body's name) has determined that the following policy is in the best interest of the municipality and its citizens.NOW, THEREFORE,

BE IT RESOLVED by the _____ (insert governing body's name) that the following is hereby approved:

IDENTITY THEFT 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. Paychecks
2. Pay stubs
4.A.1.d: Cafeteria plan check requests and associated paperwork
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. Address
3. Phone numbers
4. Maiden name
5. Names
6. Customer 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 Tennessee Public Records Act 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. In the event that the municipality cannot resolve a conflict between this policy and the Tennessee Public Records Act, the municipality will contact the Tennessee Office of Open Records.

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, 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.
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 placed inside a locked shred bin or immediately shredded using a mechanical cross cut or Department of Defense (DOD)-approved shredding device. Locked shred bins are labeled "Confidential paper shredding and recycling." 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.
2. Any sensitive information sent externally must be encrypted and password protected and only to approved recipients. Additionally, a statement such as this should be included in the e-mail:
"This message may contain confidential and/or proprietary information and is intended for the person/entity to whom it was originally addressed. Any use by others is strictly prohibited."

MTAS