CITY OF OAKWOOD
ADMINISTRATIVE POLICIES AND PROCEDURES

POLICY NO. 15
SUBJECT: Sensitive Information Policy
DATE: June 8, 2009

PREPARED BY: _____
CINDY STAFFORD, FINANCE DIRECTOR

APPROVED AS TO FORM: _____
DALMA GRANDJEAN, CITY ATTORNEY

APPROVED BY: _____
NORBERT S. KLOPSCH, CITY MANAGER

POLICY: This policy addresses the sensitive information of the municipality, its employees, customers and vendors.

PURPOSE: To establish guidelines designed to detect, prevent, mitigate and protect employees, customers and contractors from identity theft in connection with 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.

DEFINITIONS

Identify theft means fraud committed or attempted using the identifying information of another person without authority.

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

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
b. Tax identification numbers, including:
    1. Social Security number
    2. Business identification number
    3. Employer identification numbers
c. Payroll information, including, among other information:
    1. Paychecks

2. Pay stubs

d. 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
e. 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
f. 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 city of Oakwood's public records requests policy number seven and the identity theft "red flags" policy number fourteen. 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 Open Meetings and Public Records acts, collectively known as the "Sunshine Laws.", the municipality will contact the Ohio Attorney General's office (email Sunshine@OhioAttorneyGeneral.gov).

PROCEDURE

Hard Copy Distribution. Each employee and contractor performing work for the municipality will comply with the following policies:

a. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with sensitive information will be locked when not in use.
b. Storage rooms containing documents with sensitive information and record retention areas will be locked at the end of each workday or when unsupervised.
c. 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.
d. Whiteboards, dry-erase boards, writing tablets, etc. in common shared work areas will be erased, removed, or shredded when not in use.
e. When documents containing sensitive information are discarded they will be placed inside a locked shred bin or immediately shredded using a mechanical shredding device. Municipal records, however, may only be destroyed in accordance with the city's records retention policy.

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

a. Internally, sensitive information may be transmitted using approved municipal e-mail. All sensitive information must be encrypted when stored in an electronic format.
b. Any sensitive information sent externally must be encrypted and password protected and only sent to approved recipients. Additionally, a statement such as this should be included in the e-mail: *"This message (including any attachments) may contain privileged and confidential information intended for use only by a specific individual and purpose. If you are not the intended recipient or the person responsible for delivering the e-mail to the intended recipient, you should delete this message from your system without copying or forwarding it. Any use, disclosure, printing, copying, or distribution of this message, or the taking of any action based on it, is strictly prohibited. If you have received this message in error, please notify the sender by return e-mail. Thank you."*

ADMINISTRATION

A. Staff Training
   a. 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.
   b. The Finance Director is responsible for ensuring identity theft training for all requisite employees and contractors.
   c. Employees must receive annual training in all elements of this policy.
   d. To ensure maximum effectiveness, employees may continue to receive additional training as changes to the program are made.

B. Oversight of service provider arrangements
   a. 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.
   b. A service provider that maintains its own identity theft program, consistent with the guidance of the red flag rules and validated by appropriate due diligence, may be considered to be meeting these requirements.
   c. Any specific requirements should be specifically addressed in the appropriate contract arrangements.