POLICY:

Periodically, sensitive customer information is handled by the Department. The Citrus County Board of County Commissioners approved this policy to comply with the Federal Trade Commission's Identity Theft Red Flags Rule, originally adopted at 16 C.F.R. 681.1 (the "Red Flags Rule") to help protect all persons residing and doing business with the County from damages related to the loss or misuse of Sensitive Personal Information.

The purpose of this administrative regulation is to prevent, detect, and mitigate identity theft that may occur in connection with opening new covered accounts and managing existing accounts, by: setting forth the scope of the Red Flags Policy; establishing means of identifying red flags; establishing means of detecting red flags; establishing a process for addressing red flags if detected, and providing a process for administering this Policy including provisions for employee training and updating of the Policy.

PROCEDURE:

The Red Flags Rule applies to "creditors". For purposes of the rule, a "creditor" includes any entity, including a governmental entity, regularly providing services for which customers are billed, as well as one who collects payment for services over time. Whereas the County provides services that may fall within the scope of the Red Flags Rule, including provision of water, reclaimed water, wastewater, and solid waste services, to residents and businesses within Citrus County, the Board of County Commissioners wishes to implement the Red Flags Rule in order to ensure that all customer information is protected from identity theft.

The types of accounts that will be covered by this policy include those involving multiple payments or transactions. This will include any account for which services are provided and billed on a continuous basis, and those accounts for which the County allows payment over time. It shall also apply to any account for services provided by the County which includes confidential account information that may be accessed remotely due to the potential risk of identity theft. It shall not apply to accounts established for the one-time payment of a one-time fee, unless such account is accessible remotely.

This Policy applies to all County contractors, subcontractors, consultants, and their employees to the extent of their involvement with covered accounts.

Notwithstanding the provisions of this Policy, all County records subject to Florida's broad public records law shall remain so. This Policy is not intended to circumvent any attempt to obtain public records and should be read in conjunction with Florida's public records laws and in the event of a conflict, the County shall provide information in a manner that is consistent with Florida Statutes. If an employee is uncertain as to whether information should be provided pursuant to a public records request, the employee should contact a supervisor or the County's Records Manager for assistance.

DEFINITIONS:

The Red Flags Rule applies to "creditors". For purposes of the rule, a "creditor" includes any entity, including a governmental entity, regularly providing services for which customers are billed, as well as one who collects payment for services over time. Whereas the County provides services that may fall within the scope of the Red Flags Rule, including provision of water, reclaimed water, wastewater, and solid waste services, to residents and businesses within Citrus County, the Board of County Commissioners wishes to implement the Red Flags Rule in order to ensure that all customer information is protected from identity theft.

"Sensitive Personal Information" means the following items whether stored in electronic or printed format: credit card information, tax identification numbers, social security numbers, payroll information, medical information, other personal information belonging to customers including date of birth, phone numbers, address, maiden name, corporate information, or Proprietary or Confidential Information.

"Proprietary or Confidential Information" includes, but is not limited to: business methods, customer utilization information, retention information, sales information, marketing and other Company strategy, computer codes, screens, forms, information about, or received from, Company's current, former and prospective customers, sales associates or suppliers or any other non-public information. Proprietary or Confidential Information also includes the name and identity of any customer or vendor and the specifics of any relationship between and among them and the company.

IDENTIFYING RED FLAGS:

The first step in protecting against identity theft is identifying red flags that indicate someone is attempting to commit identity theft. A "red flag" is any potential pattern, practice, or activity which could create an opening or possibility for identity theft. For the purposes of this Policy, the following red flags have been identified:

A. Suspicious documents, including, but not limited to:

1. Identification that appears to be altered or forged.

2. A photo or description on a method of identification not matching the person presenting it.

3 Information on an identification card not matching other information documents provided to verify identification or statements from person providing the information.

4. An application that appears to be altered, forged, or torn and reassembled.

B. Suspicious personal identifying information, including, but not limited to:

1. Inconsistencies in information provided by customer or discovered in processing the information.

2. An address, phone number, or other personal information used on the account which is known or determined to be fraudulent or invalid, or information associated with a pager or answering service.

3. A social security number that is associated with another account.

4. An address or telephone number that is associated with another account.

5. Omission of required information on an application that is not provided after notice to the applicant.

6. A failure to provide authenticating information beyond what is generally available from a credit report or wallet.

C. Notice of fraud or identity theft from other sources associated with the name on the customer account.

DETECTING RED FLAGS:

Once red flags have been identified, the County must ensure that those red flags are detected during the day-to-day operations of the County and its contractors.

A. New Accounts.

When verifying the identity of a person opening a new account, customers must provide the following information: name, address, photo identification if opened in person or an identification number if not opened in person. If the customer is a corporate customer, the person opening the account, if not a principal of the corporation, must also provide proof of authorization to open the account from a principal of the corporation. County personnel will be responsible for reviewing the above information and photo to ensure that all information is consistent and matches the person presenting the information and photo identification.

B. Existing Accounts.

When verifying the identity of a customer contacting the County or an County contractor providing services on behalf of the County, County or contractor employees shall require that the customer provide his or her name, address, and account number or telephone number.

ACTIONS TAKEN UPON DETECTION OF RED FLAGS:

If a red flag is detected, the County shall respond in the following manner, depending on the severity of the flag:

A. Monitor a covered account for evidence of identity theft.

B. Contact the customer if account activity suggests identity theft.

C. Request additional forms of identification.

D. Close the account and no longer providing service.

E. Reopen closed accounts with new account numbers.

F. Not open a new account.

G. Notify law enforcement.

H. Determine that no response is warranted based on the circumstances.

In the event activity appears to have exposed a customer's social security number or bank account information to identity theft, the County or contractor shall immediately notify the customer and the appropriate law enforcement agency.

ADMINISTRATION OF POLICY:

In general this Policy will be administered by the County Administrator or an appropriate designee. Senior staff, along with the County Administrator, shall be responsible for ensuring that subordinate employees with employment functions involving covered accounts are properly trained and informed of the content of this Policy.

A. Updating Policy

Identity theft methods may change rapidly as technologies change and identity thieves become more sophisticated. The County will review and consider updates to this Policy at least once each year or upon the occurrence of any of the following:

1. Receipt of notice of new identity theft tactics.

2. Receipt of notice of new methods to detect, prevent, and mitigate identity theft.

3. Changes in the covered accounts offered by the County.

4. Changes in County processes relating to covered accounts.

If updates are necessitated, staff will present proposed changes to the Board of County Commissioners for review and approval.

B. Informing and Training Staff

Every employee and contractor performing work for the County that involves covered accounts shall receive a copy of this Policy and will comply with the following requirements:

1. File cabinets, desk drawers, overhead cabinets, and any other storage space containing documents with Sensitive Personal Information will be locked when not in use.

2. Storage rooms containing documents with Sensitive Personal Information and record retention areas will be locked 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 Personal Information when not in use.

4. When documents containing Sensitive Personal 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 shall be labeled “confidential paper shredding.”

5. Sensitive Personal Information may only be transmitted by email if necessary, and must include the following statement: "This message may contain confidential or proprietary `information and is intended for the person/entity to which it was originally addressed. Any use by others is strictly prohibited.”

In addition to receiving a copy of the most up to date version of the Policy, the County Administrator shall be responsible for reviewing all updates to the Policy upon approval by the Board of County Commissioners. Employees of the County shall review the Policy and contact supervisors if any questions regarding the Policy or its implementation. Supervisory staff shall have responsibility for ensuring that their subordinates understand and properly implement the Policy.

Subcontractors with responsibilities for covered accounts shall enforce this Policy in the event the subcontracting company has not adopted its own Red Flags Policy to help prevent and detect identity theft. The County shall also provide a copy of the Policy to subcontractors.

FOOTNOTES & REFERENCES TO RELATED AR's: