

Mayor
John Murray
Mayor Pro Tem
Mary Hornsby
Council Members
John Plourde
Willard Rodarmel
William Siegel



Office of the
City Manager

119 Fox Street
Lemoore ♦ CA 93245
Phone ♦ (559) 924-6700
FAX ♦ (559) 924-9003

Administrative Policy 2009-02

IDENTITY THEFT PREVENTION PROGRAM

PURPOSE:

The purpose of this Administrative Policy is to develop and implement a written identity theft prevention program in accordance with State and Federal regulations, specifically the Fair and Accurate Credit Transaction Act of 2003. This policy provides internal policies and procedures with regard to the access, storage, and protection of sensitive information which could be used in identity theft.

DEFINITIONS:

Red Flags: A pattern, practice or specific activity that indicates the possible risk of identity theft.

Sensitive Information: As described in the Fair and Accurate Credit Transaction Act of 2003, information that is considered sensitive and personal in nature includes, but is not limited to, the following: name or maiden name, date of birth, social security number, driver's license number, alien registration number, passport number, taxpayer identification number, fingerprints, bank account numbers or routing codes, credit card account numbers, investment account number, insurance coverage membership identity or other unique electronic identification number, address or routing code.

When any of the above listed examples of sensitive information are released to an unauthorized party, it results in a breach of the security of sensitive information and a potential risk of identity theft.

SCOPE:

This policy applies to all employees of the City of Lemoore, contractors, vendors, consultants, volunteers, and other temporary workers of the City, including all personnel affiliated with third party contractors, vendors or consultants of the City.

GENERAL:

Over the course of time, various employees, particularly those in Finance and Human Resources, will carry out duties that deal with sensitive information of utility customers and/or City employees. In an effort to ensure that this information is handled with the utmost responsibility and security, all such information must be treated and dealt with in a specific and deliberate manner. The Federal Trade Commission has specific guidelines and responsibilities for employers and utility providers, such as the City of Lemoore, which must be followed. The following guidelines have been taken directly from the Federal Trade Commission's guide for "Protecting Personal Information" and other Commission guidelines.

ACCESS TO INFORMATION:

All employees having access to sensitive information must sign an agreement to follow the City of Lemoore's policies and procedures set forth in this policy regarding the confidentiality and security standards for handling sensitive information. Compliance with these standards is necessary to abide by both State and Federal laws dealing with the security of sensitive data. The City and its employees are responsible for ensuring that current and future practices prevent and discourage the theft of sensitive information for any purpose. This includes any references to, or the use of, Social Security numbers for identifying Utility Customers.

All rooms and filing cabinets containing sensitive information shall be locked when not being used by employees. All persons having keys and combinations to applicable locations holding sensitive information should be accounted for and known to the Finance Director and Human Resource Administrator(s). All employees must put away all files, lock applicable file cabinets and office doors, and log off their computers at the end of each work day, so long as said files, file cabinets, offices, or computers/log-ins contain sensitive information.

Keys to file cabinets containing sensitive information must be maintained by a designated person in each department. Personnel requiring access to these file cabinets should seek out the designated person, request use of the key or request the designated person open the cabinet, then return the key upon obtaining the necessary information. This process shall be repeated when personnel re-file the materials that were accessed.

Sensitive information should not be stored on any computer other than the server, via the user's assigned network drive, unless it is essential for conducting City business. These computers must be serviced with a 'wipe utility software' before the computer is released to another employee or is destroyed. Personnel are prohibited from sharing their passwords with co-workers.

When employees, having knowledge of combinations to secured areas and/or have keys to filing cabinets which store sensitive information, are terminated or conclude employment with the City of Lemoore, all network logins/passwords shall be terminated, all applicable combinations will be changed, the employee's key(s) will be returned to the department head, and a notation shall be required acknowledging receipt of said key(s).

When sensitive information is sent via inter-office envelopes with "confidential" stamping, only the employee to whom the envelope is addressed shall open such confidential inter-office information. When envelopes sent through U.S. mail are addressed to Directors or Managers, these envelopes shall not be opened by other personnel without the Director's or Manager's express consent.

The activities of all outside service providers are to be conducted in accordance with this policy designed to detect, prevent, and mitigate the risk of identity theft. All outside service providers who come in contact with or provide sensitive information to the City are required to sign an Outside Service Provider Agreement, in the form of the Outside Service Provider Agreement attached to this policy.

RED FLAGS

There are a number of indicators of potential identity theft that are referred to as "red flags." It is the responsibility of every City employee to monitor their own daily activities in an effort to recognize and detect "red flags." It is also each employee's responsibility to verify the identity of individuals and entities they assist and associate with during the course and scope of their daily activities.

Examples of “red flags” include, but are not limited to, the following:

- A fraud alert, active duty alert, credit freeze, or address discrepancy is included in a response to a request for a credit/consumer report.
- Documents, photographs, or other identification appears to have been altered, forged, or appears to have been destroyed and reassembled.
- Information contained on the identification is not consistent with information provided by the person or with information already on file.
- Information provided is not consistent with information found in a credit/consumer report or financial institution document or file.
- Information provided is associated with known fraudulent activity as reported by a financial institution or other source.
- The address provided does not exist, is a mail drop, or a prison.
- The social security number is the same as that submitted by another individual.
- An individual fails to provide all the required personal identifying information on an application.
- When challenge questions are used to verify identity (such as; mother’s maiden name) the individual cannot provide authenticating information beyond that which generally would be available from a wallet or consumer report.
- Shortly after providing a change of address, the individual requests a duplicate copy of records, invoices, or other documents containing personal identifying information.
- After an account is opened for services, the customer fails to make the first payment or initial payments, or payment is made with a check that fails to clear the bank.
- Mail sent to an address provided by the individual is returned undeliverable.
- A customer provides notice that they have not received their paper account statement in the mail.
- A customer provides notice that their statement for services includes unauthorized charges or transactions.
- Computer viruses on programs that contain personal identifying information.
- A City laptop has been lost or stolen.
- Personnel have found their account has been “locked” due to several failed log-in attempts.

RESPONDING TO RED FLAGS

If a red flag or other potentially fraudulent activity is detected, it is essential to act quickly, because a rapid appropriate response can protect customers and the City from damages and loss.

If a red flag or other potentially fraudulent activity is detected, gather all related documentation and take this information and present it to a supervisor or the City Finance Director immediately. If an employee presents the information to a supervisor, the supervisor shall present it immediately to the City Finance Director. The City Finance Director will complete additional authentication to determine whether a security breach has occurred and/or whether the attempted transaction was fraudulent. If a breach is discovered or a transaction is determined to be fraudulent, appropriate actions shall be taken as quickly as possible. Appropriate actions may include, but are not limited to:

- Cancel the transaction;
- Disconnect the server or computer;
- Implement appropriate access controls;
- Notify and cooperate with appropriate law enforcement;
- Determine extent of liability to the City; or
- Notify actual individual/customer that fraud has been attempted.

INFORMATION DISPOSAL:

Sensitive information maintained by the City or authorized third parties shall be appropriately destroyed when the information is no longer needed. Examples of the types of sensitive information retained by the City of Lemoore include, but are not limited to, the following:

1. Employee Social Security Numbers
2. Employee Checking/Savings Account numbers for Direct Deposit
3. Personnel Records
4. County Assessor's Information
5. Census information specific to persons

The City of Lemoore's Record Retention Schedule dictates how long sensitive information shall be retained. Upon conclusion of the allotted time, these records shall be destroyed to prevent access by unauthorized individuals.

Paper records shall be disposed of by means of shredding. When disposing of old computers and portable storage devices, a 'wipe utility program' shall be used to sufficiently delete sensitive data.

UPDATING THE POLICY

Annually, or more often as required, this policy shall be re-evaluated by City management to determine whether all aspects of the Policy are up-to-date and in compliance with current State and Federal law, and applicable in the current business environment. Based on such re-evaluation, appropriate changes will be made to the policy and presented to the City Council for adoption.

POLICY ADMINISTRATION AND ENFORCEMENT

This policy is the responsibility of the City Finance Director. This policy shall be administered by the City Finance Director with the support of all employees who have access to sensitive information. Operational responsibility for the policy may be delegated to a designated employee by the City Finance Director.

The City Finance Director and other City management will have the responsibility to implement this policy and ensure that it is followed by employees, contractors, vendors, consultants, volunteers, and other temporary workers of the City, including all personnel affiliated with third party contractors, vendors and consultants. Any employee found to have violated the policy or who knowingly causes a breach of sensitive information may be subject to disciplinary action.

EMPLOYEE TRAINING

Employee training shall be conducted for all employees for whom it is reasonably foreseeable that they may come into contact with accounts or sensitive information which may constitute a risk to the City or its customers. The training for existing employees shall be done upon adoption of this policy by the City Council; the training for new employees shall be done at the time of hiring. The training will address the standards set forth in this policy, including how to identify potential “red flags” and how to assess, protect, detect, reduce, and destroy possible breaches in the security of sensitive information.

All employees are required to sign an acknowledgment, in the form of the Acknowledgment of Confidential and Security Standards for Handling Sensitive Data attached to this policy. The attached acknowledgment bearing an employee signature is required for all employees whose duties involve the access, receipt, handling, or review of sensitive information as defined by this policy. The acknowledgement certifies that this policy has been read and understood by the employee.

CITY OF LEMOORE

“In God We Trust”

**ACKNOWLEDGEMENT OF CONFIDENTIALITY AND SECURITY STANDARDS
FOR HANDLING SENSITIVE DATA**

I, _____, as an Employee of City of Lemoore, do hereby acknowledge that I must comply with a number of State and Federal laws which regulate the handling of confidential and personal information regarding both customers of this City and its other employees.

I understand that I must maintain the confidentiality of ALL documents, credit card information, and personal information of any type and that such information may only be used for the intended business purpose. Any other use of said information is strictly prohibited. Additionally, should I misuse or breach any personal information of said customers/or employees, I understand I may be subject to discipline by the City and may be held fully accountable both civilly and criminally, which may include, but not limited to, Federal and State fines, criminal terms, real or implied financial damages incurred by the customers, employees, or the City.

I have received a copy of the City's Administrative Policy regarding the City's Identity Theft Prevention Program. I understand and will fully comply with its provisions along with all other rules and regulations the City has in place regarding the handling of confidential information so as to protect the privacy of all parties involved.

By my signature below, I acknowledge that I have read and understand the City of Lemoore's policy regarding its Identity Theft Prevention Program and its other policies regarding the handling and storage of sensitive information. I hereby consent to be governed by the terms of usage and the policies and procedures set forth by this policy and agree to abide by these terms. I also acknowledge that I have participated in a City sponsored Identity Theft Program Training. I understand that a copy of this signed form will be filed in my Personnel File.

Employee: _____
Signature Date

CITY OF LEMOORE
OUTSIDE SERVICE PROVIDER AGREEMENT

The City of Lemoore's Identity Theft Prevention Program requires every entity with which the City engages in the practice of business, whether for the provision of services or the provision of a product, must be informed of the City's Identity Theft Prevention Program and must agree to abide by the rules set forth in the policy.

Name, Address, Telephone Number of the Entity:

Name of the Responsible Contact Person(s):

We have read the City of Lemoore's Identity Theft Prevention Program requirements, including how to watch for "red flags" to potential identity theft, and we agree to abide by the provisions set forth in the policy.

We agree to take the utmost precautions to secure any and all sensitive identifying information we come in contact with pertaining to our business relationship with the City of Lemoore.

We agree to take prompt action in the event we notice a "red flag" or suspect that identity theft has occurred by notifying the City Finance Director immediately at (559) 924-6707.

Signature

PRINT NAME

DATE