KLAMATH COUNTY
Identity Theft Prevention
"Red Flag Policy"

OBJECTIVES

Klamath County adopts this policy to address the requirements of the Fair and Accurate Credit Transaction Act provisions of the Federal Fair Credit Reporting Act Rule 16, CFR § 681.2 (the FTC "Red Flag Rules") and the Oregon Consumer Identity Theft Protection Act ("OCITPA") set forth in ORS 646A.600, *etseq.* Under these laws Klamath County (County) must take appropriate measures to guard personal and confidential information. The purpose of this policy is to identify patterns, practices, or specific activities that indicate the possibility of identity Theft and to take all reasonable step to prevent and mitigate the theft of personal information. Under the Red Flag Rules, the County must adopt rules for Identifying and detecting "Red Flags" that raise concerns that personal information is potentially being misused or stolen, and under OCITPA, the County must implement safeguards for protecting the security, confidentially, and integrity of personal information entrusted to the county by its customers and employees, including the proper disposal of such information.

Klamath County previously adopted a " Red Flag Policy" on January 22, 2013.

DEFINITIONS

- Identity Theft- A fraud committed or attempted using the "Identifying Information" or "Personal Information" of another person without authority.

- Identifying Information- Any name or number that may be used, alone or in conjunction with any other information, to identify a specific person.
  - · Identifying Information includes, but is not limited to, a person's:
    - o Name
    - o Address
    - o Telephone
    - o Social Security Number (SSN)
    - o Date of Birth (DOB)
    - o Government issued Driver's License Number or Identification Number (DL/ID)
    - o Alien Registration Number
    - o Government Passport Number
    - o Employer or Taxpayer Identification Number
    - o Unique Electronic Identification Number
    - o Computer Internet Protocol Address
    - o Routing Code

- Personal Information - A consumer or employee's name in combination with: a SSN; a passport or any federal ID number; a DL or ID number; or a financial, credit, or debit card number along with a security code, access code, or password. It may also include the same types of information without the name if the information obtained would be sufficient to permit a person to commit Identity Theft against the person whose information was compromised.

- Private Information- A collective reference to Identifying Information and Personal formation.

- Red *Flag*- Any pattern, practice, or specific activity that indicates the possibility of Identity Theft Alert, notifications, or other warnings received from law enforcement or other governmental agencies can be regarded as Red Flags for Identity Theft. Such information may include a fraud alert or the United States Post Office providing a notice of address discrepancy.

POLICY

- In compliance with the Red Flag Rules, the County shall implement a program taking all reasonable steps to detect, prevent, and mitigate instances of Identity Theft and the misuse of Identifying Information. To carry out this policy, the County has adopted and will implement the rules set forth in this policy: to identify and detect Red Flags raising concerns that Identifying Information is potentially being misused or stolen; and to outline procedures for safeguarding Private Information.

- Any document marked "Confidential", "Sensitive", "Proprietary", or any document similarly labeled. The County will implement and maintain reasonable safeguards to protect the security and confidentiality of personal information, including proper custody and disposal.

- For the protection of SSN's the following activities are prohibited: printing SSN's on any mailed materials not requested by the employee unless redacted (meaning no more than the last four digits is readable or accessible); or printing SSN's on cards used to access products, services, buildings, and publicly posting or displaying of SSN's. Documents, forms, and processes that include or require personal information will be reviewed to determine if and when obtaining or retaining personal information is necessary. If the personal information is not necessary, the forms and process will be revised to eliminate that information. Personal information, if no longer needed, shall be redacted.

- This policy includes five primary compliance areas: 1) determining what Private Information the County holds; 2) being aware of potential Red Flags; 3) safeguarding Personal Information entrusted to the County by its employees; 4) providing notice of theft or misuse of Personal Information; and 5) implementing the policy.

HARD COPY DISTRIBUTION

- Access to Personal Information will be permitted in person at the County, only after verifying the person's identity through photo identification. Personal Information may also in the future be obtained over the internet with secure password protection. Access to information via telephone or internet (when available) shall require verification of his or her identification using-information that would only be known to the affected person. Information will not be given without first clearing any discrepancies in the information provided.

. • Except when required by law, SSN's shall not be printed on mailed materials unless redacted, shall not be printed on cards used to access products, services, or County buildings, and shall not be included on public postings or displays, including the County's website. Social Security Numbers may be used for internal verification or administrative processes, but should be redacted whenever possible.

- County buildings and all facilities used for record storage shall be locked at the end of each workday and alarm systems engaged where applicable.

- Desks, workstations, work areas, printers and fax machines will be cleared of all documents containing sensitive information when not in use. File cabinets, desk drawers, cabinets and other storage space containing documents with sensitive information will be locked when not in use. When documents containing sensitive information are discarded they will be immediately shredded using a mechanical cross cut shredder or stored in a secured space until transported to a commercial shredding site by authorized personnel. A certificate of shredding or other proof shall be required if the shredding is completed off-site.

- Notary journals that contain personal information should be kept in a secured area or a locked file cabinet or drawer. No identifying numbers shall be recorded in the notary journal. Type of identifying document and expiration date may be recorded in the notary journal only.

ELECTRONIC DISTRIBUTION

- Internally, sensitive information may be transmitted using approved County email.

- Any sensitive information sent externally must be encrypted and password protected and only to approved recipients.

CUSTOMER ACCOUNTS

- County employees will take reasonable care when accepting applications for service and be aware of any suspect activity.

NOTIFICATION

- The County shall provide notification of a security breach as soon as possible in writing, or electronically if it is the primary manner of communication with the customer or employee, or by telephone if the person is contacted directly. The exception is if the notification would impede a criminal investigation.

- A report will be prepared and submitted to the Klamath County Board of Commissioners of any identify theft incidents and the response to the incident along with recommendations for changes to the program, if any.

THIRD PARTY VENDORS

The County has various business relationships with third party contractors. Under these business relationships, the third-party contractor may have access to customers Private Information covered in this policy. The County shall ensure that the third-party contractors' work for the organization is consistent with this policy by:

- Amending County contract templates to incorporate these requirements; or

- By determining through written acknowledgement that the third-party contractor has reasonable alternative safeguards that provide the same or greater level of protection for Private Information as provided by the County.

EMPLOYEE TRAINING AND RESPONSIBILITIES

- The Human Resources Department is responsible to include this Identity Theft Prevention Program "Red Flag Policies" as part of the new employee orientation and documenting the review of the policy.

- Department Directors are responsible to be familiar with the "Identity Theft Prevention Program and Red Flag Policies". Department Directors are also responsible to include this policy in temporary employee orientation by documenting review of *this* policy.

- The County personnel are encouraged to use common sense judgment in securing the confidential information to the proper extent. If an employee is uncertain of the sensitivity of a particular piece of information, he/she should contact his/her supervisor and treat such information as confidential until a determination is made. The County shall only collect sensitive information that is necessary for each transaction or that is considered to be public information. Employees shall. adhere to this policy and any internal processes adopted by their department. Noncompliance may result in formal disciplinary action up to and including termination of employment.