Emerald PUD Identity Theft Prevention Policy

Policy/Purpose

**Purpose:** The purpose of this policy is to protect personal information Emerald PUD receives, handles, and stores, and to comply with the Oregon Consumer Identity Theft Protection Act and all related federal regulations. Emerald PUD is entrusted with many varieties of sensitive and confidential information. This includes the personal information of a variety of consumers including clients, customers, licensees and employees. As owners and custodians of that information, Emerald PUD is responsible for protecting those assets from loss or misuse. The loss of personal information can result in substantial harm to individuals, including identity theft or other fraudulent use of the information.

**Personal Information is:**

A consumer’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or data elements are not encrypted or when the data elements are encrypted and the encryption key also has been acquired:

- Social Security Number
- Driver’s License number or state identification card number
- Identification number issued by a foreign nation
- Passport number or other United States issued identification number
- Account number, credit card number or debit card number, in combination with any required security code, access code or password that would permit access to a consumer’s financial account

**Policy:** Employees are responsible for protecting personal information from unauthorized access. Access to personal information shall be restricted to a “need-to-know” basis and available only to those individuals authorized to use such information as part of their duties and with the requirement that they keep the information confidential and use it only for authorized business purposes.

Employees must:

- Be knowledgeable of agency safeguards and follow all procedures and processes established to protect information assets and personal information
- Protect personal information from unauthorized viewing
- Properly secure personal information both when in use and when stored or filed electronically or in portable format (such as paper, discs, removable storage devices)
- Encrypt personal information when appropriate and feasible
- Have a valid business purpose to send personal information over the network and a secure way to transmit
• Have prior written approval to download personal information to any portable or removable device
• Immediately report any suspected breach of personal information to a supervisor

Authority: The Identity Theft Prevention Officer, with assistance from the Identity Theft Prevention committee, is responsible for developing appropriate written procedures and internal controls to assure compliance with the act. It is the responsibility of the Board of Directors to approve the initial plan before implementation and review an annual report.

Guidelines/Procedures:

1. Actions to be taken for each of the Red flags which relate to the opening of new accounts and the monitoring to existing accounts.
   
   a. In an effort to ensure proper detection of any Red Flags, all customers must provide at least the following information before any account will be opened:
      
      i. Full Name  
      ii. Date of birth  
      iii. Address  
      iv. Identification  

   1. US Citizen  
      a. Social Security Number and/or  
      b. State issued driver’s license number or state issued identification card (if SSN is refused, photo-bearing documentation will be required in the office)  
   2. Non US Citizen  
      a. Social Security Number and/or  
      b. State issued driver’s license or state issued identification card  
      c. Passport number and country of issuance  
      d. Alien identification number and country of issuance  
      e. Any other government issued document evidencing nationality or residence. (if SSN is refused, photo-bearing documentation will be required in the office)

   For any current account holder of an open account which the above information is not already on file at Emerald PUD, the customer will be contacted within a reasonable period of time after discovering the missing information to obtain the necessary information.

   To assist with the detection of Red Flags, Emerald PUD will implement the appropriate review process to help authenticate customers, monitor transactions, and change of address requests.

2. Preventing, Detecting and Mitigating Breaches in Security
a. Identity Theft Prevention committee will develop procedures designed to detect, prevent and mitigate breaches of security.

3. **Responding to Notices of Address Discrepancies**
   a. Emerald PUD will furnish a confirmed address to the consumer reporting agency under the following conditions:
      i. Emerald PUD can form a reasonable belief the customer report relates to the customer in Emerald PUD's records
      ii. The customer under review is a current customer with an active account
      iii. The request involves a customer opening a new account
      iv. CRA provides the request in writing
      v. Utility has established a relationship with the CRA
   b. Confirmation of address will be provided by Emerald PUD to CRA in writing within 14 days of request

4. **Providing Designated Employees with Identity Theft Prevention Training**
   a. Identity Theft Prevention committee will develop a training plan to train designated employees on a need to know basis according to job responsibilities. The committee will also develop ongoing training to ensure employees are aware of new issues and will document the training.

5. **Properly Handling Reports of Suspected Identity Theft**
   a. When a customer suspects identity theft, they must notify Emerald PUD in writing, completing the Federal Trade Commission Affidavit.
   b. Customer must submit a copy of affidavit with police report
   c. Customer service staff will make a copy of the customer's photo ID and record the receipt of the documents.
   d. Copies of the FTC affidavit, policy report and photo ID will be submitted to the Customer Service Manager to ensure reporting to proper organizations.

6. **Conducting Information Technology Audits to Monitor risk for Identity Theft**
   a. Identity Theft Prevention committee will develop a program checklist to audit and evaluate internal and external identity theft risk in information technology security.

7. **Ensuring Confidentiality of Medical Records**
   a. Emerald PUD will treat all medical information pertaining to the customer as confidential.
   b. Medical information is information or data, whether oral or recorded, in any form of medium, created by or derived from a health care provider or the customer that relates to:
      i. The past, present or future physical, mental or behavioral health care to an individual.
      ii. The provision of health care to an individual; or
      iii. The payment for the provision of health care to an individual.
   c. Medical information will not be used in the determination of a customer's eligibility for services.
d. Emerald PUD will not release medical information to third parties.
e. Rescue squads, government entities that require location of citizens on ventilators for planning purposes will be provided the information upon the written permission of the customer.

8. Disposal of records under protective procedures
   a. Emerald PUD will collect and protect documents and data until the time of destruction.
      i. Paper including faxes: The exposure of customer’s secured information in the office will be monitored by the Identity Theft Prevention committee. Examples are shredding any documents containing secured information before disposal and locking document in secured storage until disposal time.
      ii. Electronic records will be erased.
      iii. CD’s will be broken.
   b. Emerald PUD will maintain records of data destruction to include content, date and method of destruction.
   c. The destruction of records will be scheduled no longer than a monthly basis to minimize possible exposure of information as well as excess storage of records.