KNAPPA
WATER ASSOCIATION
EST 1966

92755 Allen Road
Astoria, OR 97103
P (503) 458-6461
F (503) 458-0993
kknappa@centurytel.net

Policy # 08-1
Identity Theft Prevention Program

Adopted or Effective: November 1, 2008
Reviewed or Revised: October 13, 2008

This program is intended to identify red flags that will alert our employees when new or existing accounts are opened using false information, protect against the establishment of false accounts, methods to ensure existing accounts were not opened using false information, and measures to respond to such events.

Risk Assessment
Knappa Water Association has conducted an internal risk assessment to evaluate how at risk the current procedures are at allowing customers to create a fraudulent account and evaluate if current (existing) accounts are being manipulated. This risk assessment evaluated how new accounts were opened and the methods used to access the account information. Using this information, the utility was able to identify red flags that were appropriate to prevent identity theft.

- New accounts opened In Person
- New accounts opened via Telephone
- New accounts opened via Fax
- Account information accessed In Person
- Account information accessed via Telephone (Person)

Detection (Red Flags)
Knappa Water Association adopts the following red flags to detect potential fraud.

- Notice of address discrepancy
- Other information provided by applicant is inconsistent with information on file.
- Application appears altered
- Personal information provided by applicant does not match other sources of information
- Address or telephone # is the same as that of another customer
- Customer fails to provide all information requested
- Personal information provided is inconsistent with information on file for a customer
- Identity theft is reported or discovered

Response
Any employee that may suspect fraud or detect a red flag will implement the following response as applicable. All detections or suspicious red flags shall be reported to the senior management official.

- Ask applicant for additional documentation
- Any employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customer's identity must notify office manager
- KWA will notify Clatsop County Sheriff at 503-458-7054 of any attempted or actual identity theft.
- Do not accept the application for membership/account
- Close the membership/account

Personal Information Security Procedures

Knappa Water Association adopts the following security procedures.

1. Paper documents, files, and electronic media containing secure information will be stored in locked file cabinets.

2. Only specially identified employees with a legitimate need will have keys to the room and cabinet.

3. Files containing personally identifiable information are kept in locked file cabinets except when an employee is working on the file.

4. Employees store files when leaving their work areas.

5. Employees lock file cabinets when leaving the office.

6. Employees lock doors when leaving the office.

7. Any sensitive information shipped will be shipped using a shipping service that allows tracking of the delivery of this information.

8. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the utility.

9. No visitor will be given any entry key or allowed unescorted access to the office.

10. Access to sensitive information will be controlled using password(s).

11. Sensitive information that is stored on computer network or portable storage devices used by your employees will be stored in locked cabinet.

12. Anti-virus and anti-spyware programs will be run on individual computers and on servers daily.

13. Computer passwords will be required.

14. When installing new software, vendor-supplied default passwords are changed.

15. The computer network will have a firewall where your network connects to the Internet.

16. Check references or do background checks before hiring employees who will have access to sensitive data.

17. Access to customer's personal identity information is limited to employees with a "need to know."

18. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.

19. Service providers notify you of any security incidents they experience, even if the incidents may not have led to an actual compromise of our data.

20. Paper records will be shredded or burned.

21. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Program Review and Approval

This plan has been reviewed and adopted by the Knappa Water Association Board of Directors. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

SIGNATURE ON FILE

Board President