RESOLUTION # 09-04

RESOLUTION OF THE BOARD OF COMMISSIONERS OF THE IMMOKALEE WATER AND SEWER DISTRICT ADOPTING AN IDENTITY THEFT PREVENTION PROGRAM

WHEREAS, the Board of Commissioners of the IMMOKALEE WATER AND SEWER DISTRICT (hereinafter referred to as the "Board") is authorized and empowered to construct, operate and maintain a Water and Sewer System (the "System") within the boundaries of the lands described in Florida Statute Chapter 2005-298; and

WHEREAS, the Board is authorized and empowered to make rules and regulations for its own government and proceedings; and

WHEREAS, the Board met, reviewed, and adopted the Identity Theft Prevention Plan during a publicly advertised meeting on November 14, 2008;

NOW, THEREFORE, BE IT RESOLVED BY THE BOARD OF COMMISSIONERS OF THE IMMOKALEE WATER AND SEWER DISTRICT, in public meeting assembled that the following Identity Theft Prevention Program be adopted and recognized as Resolution 09-04:

Identity Theft Prevention Program

For

Immokalee Water & Sewer District

1020 Sanitation Road

Immokalee, FL 34142

Date 11/1/08

Immokalee Water & Sewer District Identity Theft Prevention Program

This Plan 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.

Contact Information:

The Senior Management Person responsible for this plan is:
Name: Eva J. Deyo
Title: Executive Director
Phone number: 239-658-3630

The Governing Body Members of the District are:
Board Members

1 .Patricia Anne Goodnight

2. Fred N. Thomas, Jr.

3. Pete Cade

4. Raymond Holland

5. Sandra Freeman

6. Everett Loukonen

7. Richard Rice

Risk Assessment

The Immokalee Water & Sewer District 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 Fax
- Account information accessed In Person

Detection (Red Flags):

The Immokalee Water & Sewer District adopts the following red flags to detect potential fraud. These are not intended to be all-inclusive and other suspicious activity may be investigated as necessary:

- Identification documents appear to be altered
- Photo and physical description do not match appearance of applicant
- Other information is inconsistent with information provided by applicant
- Other information provided by applicant is inconsistent with information on file.
- Information provided is associated with known fraudulent activity (e.g. address or phone number provided is same as that of a fraudulent application)
- Information commonly associated with fraudulent activity is provided by applicant (e.g. address that is a mail drop or prison, non-working phone number or associated with answering service/pager)
- SS#, address, or telephone # is the same as that of other customer at utility
- Customer fails to provide all information requested
- Personal information provided is inconsistent with information on file for a customer
- Applicant cannot provide information requested beyond what could commonly be found in a purse or wallet
- 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
- Notify internal manager: Any Immokalee Water & Sewer District employee who becomes aware of a suspected or actual fraudulent use of a customer or potential customers identity must notify the Director, or the Administrative Assistant.
- Notify law enforcement: The district will notify the Collier County Sheriff's Department at 657-6168 of any attempted or actual identity theft.
- Do not open the account
- Close the account

Personal Information Security Procedures:

The Immokalee Water & Sewer District adopts the following security procedures.

1. Paper documents, files, and electronic media containing secure information will be stored in file cabinets, in a locked room.
2. Only specially identified employees with a legitimate need will have keys to the room, or the cabinets.
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 log off their computers when leaving their work areas
6. Employees lock file cabinets when leaving their work areas
7. Employees lock file room doors when leaving their work areas
8. Access to offsite storage facilities is limited to employees with a legitimate business need.
9. Visitors who must enter areas where sensitive files are kept must be escorted by an employee of the District.
10. No visitor will be given any entry codes or allowed unescorted access the office.

11. Access to sensitive information will be controlled using “strong” passwords. Employees will choose passwords with a mix of letters, numbers, and characters. User names and passwords will be different. Passwords will be changed at least monthly.

12. Passwords will not be shared or posted near workstations.

13. Password-activated screen savers will be used to lock employee computers after a period of inactivity.

14. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.

15. Sensitive information that is sent to third parties over public networks will be encrypted

16. Sensitive information that is stored on computer network or portable storage devices used by your employees will be encrypted.

17. Email transmissions within your business will be encrypted if they contain personally identifying information.

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

19. When sensitive data is received or transmitted, secure connections will be used

20. Computer passwords will be required.

21. User names and passwords will be different.

22. The use of laptops is restricted to those employees who need them to perform their jobs.

23. Laptops are stored in secure place.

24. Laptop users will not store sensitive information on their laptops.

25. Laptops which contain sensitive data will be encrypted

26. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.

27. If a laptop must be left in a vehicle, it is locked in a trunk.

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

29. Any wireless network in use is secured.

30. Maintain central log files of security-related information to monitor activity on your network.
31. Monitor incoming traffic for signs of a data breach.
32. Monitor outgoing traffic for signs of a data breach.
33. Implement a breach response plan.
34. Check references or do background checks before hiring employees who will have access to sensitive data.
35. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
36. Access to customer's personal identify information is limited to employees with a "need to know."
37. Procedures exist for making sure that workers who leave your employ or transfer to another part of the company no longer have access to sensitive information.
38. Implement a regular schedule of employee training.
39. Employees will be alert to attempts at phone phishing.
40. Employees are required to notify the Director immediately if there is a potential security breach, such as a lost or stolen laptop.
41. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
42. 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.
43. Paper records will be shredded before being placed into the trash.
44. Paper shredders will be available at each desk in the office, next to the photocopier, and at the home of any employee doing work at home.
45. Any data storage media will be disposed of by shredding, punching holes in, or incineration.

Identity Theft Prevention Program Review and Approval

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

A report will be prepared annually and submitted to the above named senior management or governing body to include matter related to the program, the effectiveness of the policies and procedures, the oversight and effectiveness of any third party billing and account establishment entities, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

If any phase or portion of this Resolution is held invalid or unconstitutional by any court of competent jurisdiction, such portion shall be deemed a separate, distinct and independent provision and such holding shall not affect the validity of the remaining portion.

This resolution shall become effective on November 1, 2008.

PASSED AND DULY ADOPTED by the Board of Commissioners of the IMMOKALEE WATER AND SEWER DISTRICT, this 14th day of November 2008.

BOARD OF COMMISSIONERS
IMMOKALEE WATER AND SEWER DISTRICT

BY:_____

Anne Goodnight
Chairperson

BY:_____

Pete Cade
Secretary