GENERAL MANAGER CONSENT #080449
OCTOBER 16, 2008

Identity Theft Detection and Prevention Program

in compliance with the Federal FACTAct (2003)

Identity Theft Red Flag Ruling

Statement of Policy

Summary of Law and Regulation

Policy:

It is the policy of Gainesville Regional Utilities (GRU) to:

- Respond to fraud and activity duty alerts
- Properly dispose of consumer report information
- Properly handle notice of identity theft
- Provide information to victims of identity theft
- Respond to any notification received from identity theft, to prevent refurbishing blocked information
- Comply with the rules regarding sharing information with affiliates
- Provide an oral, written, or electronic notice to those who receive less favorable terms for deposit
- Take appropriate action when the utility receives a notice of discrepancy in the consumer's address
- Comply with red flag guidelines
- Protect medical information in the utility system
- Protect Social Security Numbers
- Protect Banking information

The Privacy Officer, with assistance from the privacy committee members, is responsible for developing appropriate written procedures and internal controls to assure compliance with the act.

The management of each department is responsible for implementing and complying with these procedures and internal controls.

Identity Theft Detection and Prevention Program

Table of Contents

Purpose

The goal of this policy is to prevent identity theft. GRU recognizes the responsibility to safeguard customer's personal information during its collection, recording and handling within all departments of GRU. The purpose of this policy is to create an Identity Theft Detection and Prevention Program utilizing guides set forth in the FACT Act (2003).

Scope

This policy applies to management and all personnel of GRU. The following represents a policy for the development of the identity theft detection and prevention program. Any part or the whole of policies and procedures written and developed will be incorporated into the program where appropriate. This does not replace, but rather supplements, any of GRU's standing policies.

Responsibility

GRU must protect its customer data and implement policies and procedures that meet standards established by the Federal Trade Commission by November 1, 2008. Thereafter, GRU will continually report and monitor the program's integrity, completeness, and deficiencies. Any revisions to the program will be conducted at least annually.

Definitions

Identity Theft - Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting 1 or more transactions to commit fraud that results in substantial harm or inconvenience to the victim or GRU. This fraudulent activity may include opening new utility accounts, gaining access to existing accounts or providing unauthorized payments.

Red Flag – A pattern, particular specific activity that indicates the possible risk of identity theft.

Privacy Committee

GRU's Privacy Committee is established to create, drive and monitor the program. A Privacy Officer functions as the head of committee reports to a member of Senior Management regarding the outcomes and needs of "The Identity Theft Detection and Prevention Program."

Members:

Department	Name	Role
Customer Operations	Cindy Andrade	Privacy Officer – coordinates committee activities, reports and incident review.
Customer Service	Mary Alice Brown	Day-to-day processes in opening new accounts and monitoring existing accounts.
Security	David Thompson	Reviews security procedures and makes external law enforcement contact.
IT	Dianne Hope	Customer Care System application & internal security oversight.
	Scott Sheridan	Website and external application security oversight.
Utilities Attorney	Skip Manasco (advisor)	Provides interpretations of applicable state and federal law.
Human Resources	Keisha Jones (advisor)	Personnel policies and training.
Compliance	Kevin Crawford	Overall compliance oversight.

Policies & Procedures

A. Red Flags Identification and Mitigation Policies

Flag	Next Step	Mitigation
Alerts		
Consumer report indicates fraud or active duty alert.	Tell the customer about the alert and ask them to contact the appropriate agency to resolve the issue.	Do not open the account
Credit Freeze	Tell the customer about the alert.	If the customer is able to authorize the account, open it otherwise, do not open the account.
Notice of address discrepancy	Ask the customer to verify their previous and current addresses with supporting documentation if necessary.	If customer is able to verify addresses, open the account and notify agency of new verified address.
Presentation of Suspicious Documents		
Identification documents appear altered or forged.	Ask the customer to visit the issuing agency and get an acceptable copy of the suspicious document.	Do not open the account.
Photo/physical description does not match applicant.	Ask the customer to visit the issuing agency and get an updated copy of the identification document	Do not open the account.
Other information on identification is inconsistent information given from applicant	Ask the customer to verify the inconsistent information with supporting documentation such as marriage certificate or social security card.	If customer is able to verify information, no further action is necessary.
Application looks altered or forged or destroyed and reassembled.	Ask the customer to fill out another application in the office and verify all suspicious information.	Do not open the account unless you are able to verify the information on the application.
Information in utility files is inconsistent with information provided.	Inform the customer of the discrepancy and ask the customer to verify the information with supporting documentation.	Advise the customer to contact law enforcement should they believe identify theft has occurred.
Notice of Theft		
Utility is notified by law officials or others, that it has opened a fraudulent account for a person engaged in identity theft.	Follow the instructions of law enforcement.	Depending upon what law enforcement asks you to do, you may close the account or closely monitor the account.

Flag	Next Step	Mitigation
Suspicious Personal Identifying Information		
Identification is inconsistent with external source such as: 1.Address vs. Address on Consumer Report 2. Social security number not issued. 3. Social security number on Death Master File. 4. Inconsistent information, such as lack of correlation between date of birth and social security number.	1. Ask the customer to verify addresses and provide documentation if necessary. 2. Tell customer about discrepancy & ask them to contact SSA. 3. same as 2 4. Ask the customer to verify the information with documentation such as SSN card or DL	1. If customer is able to verify address, open account and notify CRA if necessary regarding new address. 2. Do not open account 3. Do not open account 4. If customer is able to verify information, no further action is necessary.
Applicant fails to provide all personal ID requested.	Inform the customer of the requirements to open an account and direct them to where they can obtain proper documentation.	Do not open the account unless you are able to verify the identity with other types of acceptable documentation.
Change of billing address is followed by request for adding additional properties to the account (or shortly following the notification of a change in address, the utility receives a request for the addition of authorized users on the account).	Verify identity of all persons requesting address changes, adding properties, or changing authorized users.	If you are able to verify the identity of the person making the request, then no further action should be necessary.
Payments are made in a manner associates with fraud. For example, deposit or initial payment is made and no payments are made thereafter.	Contact the customer.	Close inactive accounts after a reasonable period of time.
Mail sent to customer is repeatedly returned.	Contact the customer to verify the correct billing address.	Correct the address on file.
Customer notifies utility that they are not receiving their bill.	Verify the identity of the customer then verify the correct address.	Correct the address on file.
The utility is notified of unauthorized charges or transactions in connection with a customer's account.	Ask the customer to supply documentation regarding the possible identity theft such as an Affidavit or police report.	Notify security officer and law enforcement.

B. Handling a Breach in Security

To prevent identity theft by employees, GRU will:

- Limit exposure of secured information by review of application and data security
- Train management to recognize signs of employee theft including sifting through waste receptacles, downloading excessive amounts of consumer information, using secured terminals without authorization, etc.

In the event of a breech of security, the following policies and administrative guidelines are in place to educate employees and to mitigate damages:

- Policy 1, section II C: The Public employee is governed by high ideals in his/her public and private activities in order that he/she may merit the respect and confidence of people with whom he works and the public which he/she serves. He/she is careful to conduct himself/herself, both on duty and off, so as to reflect credit upon the City.

- GRU Administrative Guideline 2.6, Internet Policy, Specifically Unacceptable Use, (5) Any purposes which violate a federal or state law or City or GRU policy. ‘ intentionally seeking out information on, obtaining copies of, or modifying files and other data, which is private, confidential or not open to the public inspection or release. Users should seek the advice of the GRU legal staff if they are concerned about confidentiality issues.

- Negligent breach in security by personnel may result in violation of Policy 19, Rule 25 which states, “Wanton or willful violation of statutory authority, rules, regulations or policies”,

C. Handling an Address Discrepancy

Should any address discrepancies be brought to GRU’s attention, GRU will notify the customer or appropriate agency of the discrepancy.

D. GRU Disposal & Destruction of Sensitive Data

GRU is obligated to maintain and ensure that confidential employee and customer information remains confidential. Therefore, GRU will follow the proper outlined methods for the destruction of all data contained on the following media that's business need has expired.

1 OVERVIEW OF DATA MEDIA TYPES

The following table (Table One) is not an exhaustive list of all possible media types but instead offers a representative sample of the most common forms of media currently in use. These media types also demonstrate the characteristics that determine the appropriate deletion of destruction methods required to assure data is non-retrievable.

Media Type	Data Storage Mechanism	Suggested Removal Methods
Hard Disk Drives	Non volatile magnetic	Pattern wiping, Incineration, physical destruction
CDROM/DVD-R	Write once optical	Abrasion, Incineration, physical destruction
CD-RW/DVD-RW	Write many optical	Abrasion, Incineration, physical destruction
Magnetic Tape	Non volatile magnetic	Degaussing, Incineration, physical destruction
Flash Disk Drives	Solid State	Pattern wiping, Physical destruction
Paper Based		Shredding, Incineration

2. MEDIA DESTUCTION TECHNIQUES

Media, which is no longer required (or has passed its effective reuse period), should be destroyed. Destruction of the media should be witnessed to ensure that it is destroyed beyond recovery.

2.1 HARD DISK DESTRUCTION

The most permanent method of destruction is the complete physical destruction of the drive and its platters. Due to the component makeup of disk drives, only a specialist in IT will be assigned to remove and destroy the drive. The preferred method utilized by GRU is to drill into the drive making holes and destroying the ability to recover data.

2.2 CD-ROM AND DVD DESTRUCTION

Destruction of this media is accomplished by shredding by a confetti shredder to ensure that the media can not be recovered that was contained on the CD or DVD.

2.3 SOLID STATE DEVICES

Solid state devices normally consist of Flash USB drives or memory storage cards for PDAs and other handheld devices. Due to the compact nature of their internal makeup, the complete physical destruction of the device is required to

ensure that any recover of data is impossible. All electronic circuitry and storage devices must be broken into small pieces.

2.4 MAGNETIC TAPE BACKUP

The most effective method for the destruction of magnetic tape is the disintegration or shredding of the tape media.

2.5 PAPER BASED

Paper based media will be destroyed by shredding preferably with confetti producing shredders to ensure that data contained in the paper media is not recoverable. Sensitive customer information on paper is to be shredded prior to recycling.

3. DATA DESTRUCTION MANAGEMENT

GRU will utilize and maintain a Destruction of Data/Media Log for all media containing sensitive business records. This log will provide the Date, Time, Name of Person, and the type of Media destroyed. Any media removed from the immediate area of use will be destroyed by the assigned IT specialist who will provide a Certificate of Removal and Destruction.

The Log will be maintained by the Privacy Officer and will be reviewed annually by the Privacy Committee.

E. Training and Screening

- ✓ Run background checks, thorough screening, and ask specific scenario questions at hiring.
- ✓ Train employees to identify Red Flags.
- ✓ Supervisory training will involve additional information including managerial responsibilities in identity theft prevention.

Training

- The need to attend training will be determined by job duties, with priority registration given to the supervisors and employees with the greatest exposure or risk.

- All new employees will be expected to receive an introductory session prior to working in an area where there is risk of a breach occurring. This introductory session may be conducted by a manager, supervisor, or designated lead worker. At the next available classroom session, the new employee should be enrolled in the full session.

- Enrollment and completion of the training will be documented through the Learning & Development Division in the learning management system (Pathlore). A signed roster will be used to document all who attended the training and acknowledge participants having received any handouts given during the training.

- Annual refresher training can he be held at department staff meetings for all affected areas, with a signed roster acknowledging attendance and discussion of any updated information. When there are significant changes to law or practice, a classroom session or alternate learning method (on-line or computer based) will take place.

- All new employees will be expected to receive an introductory session prior to working in an area where there is risk of a breach occurring. This introductory session may be conducted by a manager, supervisor, or designated lead worker. At the next available classroom session, the new employee should be enrolled in the full session.

F. Handling Reports of Suspected Identity Theft

When a customer suspects Identity Theft, they must notify GRU in writing, filling out the Notice of Identity Theft form and make copy of their photo ID and attach it to the police report along with the completed form and send all to the Privacy Officer.

Actions to be taken:

- ✓ Close or block breached account and open new account if warranted.
- ✓ Place an alert on the account and notify appropriate personnel.
- ✓ Documents will be reviewed to determine validity of report and results reported to appropriate agency or individual.

G. Victim Record Request

Under the FACTAct, identity theft victims are entitled to a copy of the application or other business transaction records relating to their identity theft free of charge. GRU shall provide these records within 30 days or sooner of receipt of the victim's request. GRU will also provide these records to any party which the victim authorizes. GRU shall also follow any obligations under Florida Statues related to public records.

H. IT Security

The network administrator and IT management will conduct audits on a quarterly basis using the Identity Theft Prevention Program Checklist for Information Technology. All system administrators and IT professionals shall sign agreements to not disclose private information unless complying with a lawful order.

Comment [MSS1]: Checklist has been started but not completed.

I. Medical Confidentiality

Company shall not obtain or use medical information pertaining to a consumer in connection with any determination of the consumer's eligibility, or continued eligibility, for services. All medical information will be treated as confidential and rules of protection against identity theft apply as to all other private information.

J. Reports, Reviews and Updates for Policy Enforcement

Periodically, staff will review practices to ensure compliance with policy. The reports will be used to evaluate effectiveness of and amend the Identity Theft Detection Prevention Program.

An annual report reviewing all incidents, program revisions and goals will be submitted to the General Manager of Utilities.

Reporting Tools

The following forms will be used to report Identity Theft Incidents:

Identity Theft Prevention Program Incident Report
GRU

Date: _____
Prepared by: _____
(Employee designated to track and record information)

Committee Members:

_____

_____

_____

_____

_____

It is the policy of GRU to provide an Identity Theft Prevention Program for customers and employees. The purpose of this report is to promote continued evaluation of effectiveness of current policies and procedures in compliance with the FACTAct (2003). This document will be used to drive recommendations for changes to the program due to evolving risk and methods of theft.

Identity Theft Prevention Program Incident Report

Page 2

Date	Scope	Employee	Employee Trained	Incident/“Significant Event”	Management Response	Mitigation

Identity Theft Prevention Program Incident Report
Page 3

Describe current strengths of Utility Identity Theft Program:

_____

_____

_____

_____

_____

Describe areas for Improvement:

_____

_____

_____

_____

Goal for Improvement	Steps Needed	Person(s) Responsible	Date

Committee Signatures

(Name)	(Title)	(Date)
(Name)	(Title)	(Date)
(Name)	(Title)	(Date)
(Name)	(Title)	(Date)
(Name)	(Title)	(Date)

Reviewed and approved by: _____

Robert Hunzinger, General Manager for Utilities Date

NOTICE OF IDENTITY THEFT (form)

NOTICE OF IDENTITY THEFT Form.doc

Identity Theft Prevention Program Checklist for IT

Website and External Applications

About

The Identity Theft Prevention Program Checklist for IT is used to help reduce risks associated with GRU web sites and external applications. The checklist is specifically focused on risks associated with customer information that can be used in identity theft. The checklist segments risk into two groups, external and internal.

The checklist should be conducted when:

1) new programs or services raise privacy issues; or
2) changes to programs or services affect the collecting, use, or disclosing of personal information; or
3) On a basis as outlined in GRU's ID Theft Prevention Program.

External checklist

1. Is a customer's personal information protected by encryption as it is transmitted to and from GRU? Sensitive is defined as the customer's name and one or more of the following:
    a. Social security number.
    b. Driver's license number or Florida Identification Card number.
    c. 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 an individual's financial account.

Internal checklist

1. Is the storage of a customer's personal information on GRU computer systems encrypted or masked for all of the following items:
    a. Social security number.
    b. Driver's license number or Florida Identification Card number.
    c. 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 an individual's financial account.
2. Is access to customer information defined and restricted by employee responsibilities?
3. Are all databases and other data repositories containing sensitive information, including all organizational servers, secured behind firewalls?
4. Is anti-virus software installed, and does it have a minimum compliance level of more than 95% at any given time?
5. Does GRU maintain a patch management program that is designed to address desktop and server patches within days of patch release?
6. Does GRU maintain technical standards for system setup and configuration and assess a sample of systems against these standards every month?
7. Does GRU prohibit employee access to certain categories of Web sites?
8. Does GRU assess employee passwords for strength at least quarterly, and force password changes on weak accounts?
9. Does GRU have processes that help automate the user identity management lifecycle (e.g., removing access immediately on employee termination)?