

SUBJECT <b>IDENTITY THEFT PREVENTION POLICY</b>	ISSUED BY <b>CITY COUNCIL</b>	EFFECTIVE DATE <b>NOVEMBER 3, 2008</b>
--	----------------------------------	---

**POLICY STATEMENT:*****Purpose:***

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.

***Contact Information:***

The Senior Management Person responsible for this program is:

Name: Kurt Hassler  
 Title: City Administrator  
 Phone number: 785-325-2284

***Risk Assessment***

The City of Washington 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 and/or 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 upon receipt of payment
- Account information accessed in person
- Account information accessed via telephone (person)

**PROCEDURE:*****Detection (Red Flags):***

The City of Washington 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.
- Application appears altered or destroyed and reassembled
- Personal information provided by applicant does not match other sources of information (e.g. credit reports, SS# not issued or listed as deceased)
- Lack of correlation between the SS# range and date of birth
- 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 City Administrator.

- New accounts:
  - Ask applicant for additional documentation (e.g. valid driver's license, social security card, or military ID card)
  - Notify City Clerk or City Administrator as soon as possible.
  - Notify law enforcement: The utility will notify the Washington County Sheriff's Office of any attempted or actual identity theft.
  - Do not open the account.
- Existing account:
  - Notify City Clerk or City Administrator as soon as possible.
  - Close the account with approval of the City Administrator.
  - Terminate services with approval of the City Administrator.

### ***Personal Information Security Procedures:***

The City of Washington adopts the following security procedures.

1. Paper documents and files containing secure information will be stored in the vault.
2. Only specially identified employees with a legitimate need will have keys to City Hall.
3. Files containing personally identifiable information are kept in the vault except when an employee is working on the file.
4. Employees will not leave sensitive papers out on their desks when they are away from their workstations.
5. Employees store files when leaving their work areas.
6. Any sensitive information shipped using outside carriers or contractors will be encrypted.
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 codes or allowed unescorted access to the office.
10. 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.
11. Passwords will not be shared or posted near workstations.
12. When installing new software, immediately change vendor-supplied default passwords to a more secure strong password.
13. Anti-virus and anti-spyware programs will be run on individual computers on a weekly basis and on servers daily.
14. When sensitive data is received or transmitted, secure connections will be used
15. Computer passwords will be required.
16. User names and passwords will be different.
17. The use of laptops is restricted to those employees who need them to perform their jobs.
18. Laptops are stored in a secure place.

19. Laptop users will not store sensitive information on their laptops.
20. Employees never leave a laptop visible in a car, at a hotel luggage stand, or packed in checked luggage.
21. If a laptop must be left in a vehicle, it is locked in a trunk.
22. The computer network will have a firewall where your network connects to the Internet.
23. Any wireless network in use is secured.
24. Maintain central log files of security-related information to monitor activity on your network.
25. Monitor incoming traffic for signs of a data breach.
26. Monitor outgoing traffic for signs of a data breach.
27. Implement a breach response plan as described in the HIPAA plan.
28. Check references or do background checks before hiring employees who will have access to sensitive data.
29. New employees sign an agreement to follow your company's confidentiality and security standards for handling sensitive data.
30. Access to customer's personal identity information is limited to employees with a "need to know."
31. 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.
32. Implement a regular schedule of employee training.
33. Employees will be alert to attempts at phone phishing.
34. Employees are required to notify the City Administrator immediately if there is a potential security breach, such as a lost or stolen laptop.
35. Employees who violate security policy are subjected to discipline, up to, and including, dismissal.
36. 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.
37. Paper records will be shredded before being placed into the trash.
38. Paper shredders will be available in the office, next to the photocopier.
39. 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 City Council. Appropriate employees have been trained on the contents and procedures of this Identity Theft Prevention Program.

## ***Annual Report***

A report will be prepared annually and submitted to the City Council to include matter related to the program, the effectiveness of the policies and procedures, a summary of any identify theft incidents and the response to the incident, and recommendations for substantial changes to the program, if any.

---

Harold H. Jones, Jr., Mayor