IN AND FOR THE CITY OF BROOKINGS
STATE OF OREGON

A RESOLUTION OF THE CITY OF BROOKINGS ADOPTING IDENTITY THEFT PREVENTION AND PROTECTION POLICIES PURSUANT TO THE OREGON IDENTITY THEFT PROTECTION ACT OF 2007.	**RESOLUTION 08-R-908**

WHEREAS, the Oregon Legislature has enacted the Oregon Identity Theft Protection Act providing consumers the ability to place a security freeze on their credit file; and

WHEREAS, the Oregon Identity Theft Protection Act contains standards to shield Social Security numbers, to notify consumers in case of a security breach, and to safeguard personal identifying information; and

WHEREAS, the City of Brookings maintains "account systems" that meet the definition provided in Section 114 of the Fair and Accurate Credit Transactions Act of 2003; and

WHEREAS, the City of Brookings has an obligation to protect and properly dispose of personal information relating to its employees and volunteers, as well as to its customers;

NOW THEREFORE, BE IT RESOLVED:

The City Council of the City of Brookings, Curry County, Oregon, does hereby adopt Administration Regulations 14 and 15, attached and incorporated herein, as policy for the protection and prevention of identity theft for its employees, volunteers and consumers.

BE IT FURTHER RESOLVED:

This resolution shall take effect immediately.

Passed by the City of Brookings, Oregon on the 27th day of October, 2008; effective the same date.

Signed by the Mayor this 28th day of October, 2008.

Larry Anderson, Mayor

ATTEST:

By

Joyce Heffington, City Recorder

City of Brookings

Administrative Regulation No. AR-14

IDENTITY THEFT PREVENTION POLICY FOR NON-EMPLOYEES

I. OBJECTIVE

The objective of this Administrative Regulation is to establish an identity theft prevention policy compliant with Federal Trade Commission (FTC) requirements for non-employees

II. AUTHORITY

The City Manager has authorized the Administrative Service Department (ASD) to create and implement an Identity Theft Prevention Program for the City of Brookings that will identify, detect, mitigate, and update Red Flags that signal the possibility of identity theft in connection with the opening of a covered account or any existing covered account.

III. DEFINITIONS

For the purpose of this Policy:

A. "Covered Account" means an account that the City of Brookings offers or maintains, primarily for personal, family or household purposes, that involves or is designed to permit multiple payments or transactions and any other account that the City of Brookings offers or maintains for which there is a reasonably foreseeable risk to customers or the safety and soundness of the City of Brookings from identity theft, including financial, operational, compliance, reputation, or litigation risks.

B. "Identity Theft" means a fraud committed or attempted using the identifying information of another person without authority.

C. "Red Flag" means a pattern, practice, or specific activity that indicates the possible existence of identity theft.

IV. RESPONSIBILITY

Under the direction of the Administrative Services Director, ASD staff shall:

A. Respond to fraud and active duty alerts.
B. Properly store and dispose of consumer report information.
C. Provide information to victims of identity theft.
D. Properly handle notice of identity theft.
E. Respond to any notification received from a victim of identity theft, to prevent refurnishing blocked information.
F. Only use the last 4 digits of a debit or credit card.
G. Provide an oral, written, or electronic notice to those who receive less favorable terms.
H. Will not furnish information to a Credit Reporting Agency (CRA).
I. Take appropriate action when the City of Brookings receives a notice of discrepancy in the customer's address.
J. Comply with the "Red Flag" guidelines.

IV. PROCEDURE

Financial identity theft occurs when someone uses another consumer's personal information (name, social security number, etc.) with the intent of conducting multiple transactions to commit fraud that results in substantial harm or inconvenience to the victim. This fraudulent activity may involve the City of Brookings opening or maintaining accounts, establishing electronic deductions for payment, or gaining access to the victim's accounts.

A. Defining actions to be taken for each of the Red Flags which relate to the opening of new accounts and monitoring of existing accounts:

   1. The ASD will develop procedures designed to protect, prevent and mitigate identity theft in connection with the opening of a covered account or any existing covered account.

   2. In an effort to ensure proper detection of any Red Flags, all customers (consumers) must provide at least the following information/documentation before any new covered account will be opened:
      a. Full Name;
      b. Date of birth (individual account);
      c. Previous and current address
      d. Identification:
         i. US Citizen
            1. Taxpayer Identification Number (Social Security Number and/or
            2. Photo-bearing documents (required in the office)
               - State issued driver's license.
               - State issues identification card.
         ii. Non-US Citizen:
            1. Taxpayer Identification Number (Social Security Number) and/or
            2. Photo-bearing documents (required in the office)
               - State issued driver's license.
               - State issued identification card.
               - Passport number and country of issuance.
               - Alien identification number and country of issuance.
               - Any other government-issued document evidencing nationality of residence.

B. Preventing, Detecting and Mitigating Breeches in Security.

   1. ASD will take steps to detect, prevent and mitigate breeches of security.

C. Responding to Notices of Address Discrepancies.

   1. The ASD will furnish a confirmed address to the consumer reporting agency (CRA) under the following conditions:
      a. The City of Brookings can form a reasonable belief the consumer report relates to the customer in the City of Brookings' records.
      b. The customer under review is a current customer with an active account.
      c. The request involves a customer opening a new account.
      d. CRA provides the request in writing.
      e. The City of Brookings has established a relationship with the CRA.
         i. Confirmation of address will be provided by the ASD to CRA in writing within 30 days of request.

D. Providing Designated Employees with Identity Theft Prevention Training.

   1. ASD will develop a training plan to train designated employees on a need-to-know basis according to job responsibilities. ASD will also develop an ongoing training schedule to ensure employees are kept up-to-date on new issues.

E. Properly Handing Reports of Suspected Identity Theft.
   1. When a customer suspects identity theft, they must notify the City of Brookings in writing, completing the Federal Trade Commission Affidavit. Instructions for completion are available through FTC.
   2. Customer must submit a copy of affidavit with policy report.
   3. ASD staff will make a copy of the customer's photo ID and record the receipt of the documents.
   4. Copies of the FTC affidavit, policy report and photo ID will be submitted to the CRA to ensure reporting to proper organizations.

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

G. Disposal of records under protective procedures.
   1. The City of Brookings will collect and protect documents and data until the time of destruction.
      a. Paper including Faxes: The exposure of customer's secured information in the office will be monitored by ASD. Examples are shredding any documents containing secured information before disposal and locking documents in secured storage until disposal time.
      b. Electronic records will be erased.
      c. CD's will be broken.
   2. The City of Brookings will maintain records of data destruction to include content, date and method of destruction.
   3. The destruction of records will be scheduled as outlined by retention schedules by the State of Oregon.

Approved by City Manager	(Signature)	10\14\08 (Date)
Made a part of the City's Administrative Regulations binder and distributed to all City staff on:		10-15-08 (Date)

City of Brookings

Administrative Regulation No. AR-15

IDENTITY THEFT PROTECTION POLICY FOR EMPLOYEES & VOLUNTEERS

I. OBJECTIVE:

The objective of this Administrative Regulation is to establish Identity Theft Protection Policy for City employees and volunteers.

II. PROCEDURE:

A. Safeguarding personal information:
   1. The City of Brookings shall implement and maintain reasonable safeguards to protect the security and confidentiality of personal information, including its proper disposal. Personal information includes an employee or customer's name in combination with SSN, Oregon driver's license or Oregon identification card, financial, credit, or debit card numbers along with a security or access code.

B. Social Security Numbers (SSN) Protection:
   1. Prohibitions:
      a. Printing SSNs on any mailed materials not requested by the employee or customer unless redacted or on cards used to access products, services, or City buildings (such as ID cards) is prohibited
      b. Publicly posting or displaying SSNs is also prohibited.
   2. Exemptions:
      a. Requirements by the state of Oregon.
      b. Federal laws, including statute, such as W2s, W4s, 1099s, etc; records that are required by law to be made available to the public.
      c. Records used for internal verification or administrative processes; and
      c. Records used for enforcing a judgment or court order.

C. Notification of Security Breach:
   1. In the event that personal identifying information has been subject to a security breach, the City will provide notification of the breach to the customer or the employee *unless* the notification will impede a criminal investigation.
   2. Notice shall be made as soon as possible in:
      a. Writing; or
      b. Electronically, if that is the primary manner of communication with the customer or employee; or
      c. By telephone, if the person is contacted directly.

III. RESPONSIBILITY:

A. Information Technology Department (IT) shall:
   1. Establish technical controls to safeguard personal information stored in electronic format.
   2. Document electronic safeguard practices in writing.

B. Administrative Services Department (ASD) shall:
   1. Include and document review of this Identity Theft Protection Policy as part of new employee orientation.

C. Department Directors shall:
   1. Become familiar with the Identity Theft Protection Act and review this policy with their staff.
   2. Meet with their staff to assess current compliance and appropriate safeguard practices.

D. All employees shall:
   1. Comply with this policy and any internal processes as directed by their Department Directors. Non-compliance with the policies outlined in this regulation may result in formal disciplinary action up to and including termination of employment.
   2. Contact their supervisors if they have questions about compliance with this policy.

Approved by City Manager	(Signature)	10\15\08 (Date)
Made a part of the City's Administrative Regulations binder and distributed to all City staff on:		10-15-08 (Date)