

RESOLUTION 2009-15

**A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF GARIBALDI, OREGON,
ADOPTING IDENTITY THEFT 'RED FLAG' POLICIES AND PROCEDURES IN
COMPLIANCE WITH THE FAIR AND ACCURATE CREDIT TRANSACTIONS ACT OF 2003
AS REGULATED BY THE FEDERAL TRADE COMMISSION**

WHEREAS, the Federal Trade Commission Fair Credit Reporting Act (FCRA), as amended in 2003 by Sections 114 and 315 of the Fair and Accurate Credit Transactions (FACT) Act established new identity theft reporting requirements; and

WHEREAS, the Federal Trade Commission Fair and Accurate Transactions (FACT) Act of 2003 effective January 1, 2008, established 'Identity Theft Red Flag Rule' provisions; and

WHEREAS, the Identity Theft Red Flag Rule provisions required entities (including utilities) to establish identify theft prevention program policies to identify potential risks regarding identity theft; and

WHEREAS, the Oregon Senate passed Senate Bill 583 and the Oregon Legislature enacted the Oregon Identity Theft Protection Act (OITPA) to be enacted by all credit entities by November 1, 2008; and

WHEREAS, the OITP Act gives consumers the ability to place a security freeze on their credit file; and

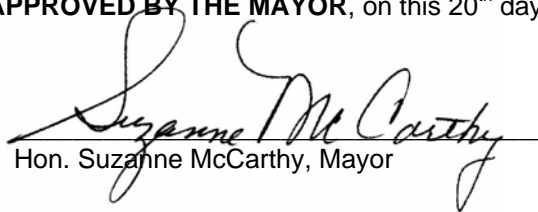
WHEREAS, the OITP Act contains standards to shield Social Security numbers to notify consumers should there be a security breach and to safeguard personal identifying information, and

WHEREAS, the City of Garibaldi has written procedures to identify, detect and respond to possible signals of identity theft known as 'Red Flags'.

THE COMMON COUNCIL OF THE CITY OF GARIBALDI RESOLVES AS FOLLOWS:

Section 1: The City Council hereby adopts the Information Security Program for the City of Garibaldi attached hereto as Exhibit A effective immediately.

PASSED BY THE COMMON COUNCIL AND APPROVED BY THE MAYOR, on this 20th day of July 2009.


Hon. Suzanne McCarthy, Mayor

ATTEST:


John O'Leary, Interim City Administrator

EXHIBIT A

CITY OF GARIBALDI INFORMATION SECURITY PROGRAM

1. **Safeguarding Personal Information**

Personal information includes the employee or customer's name in combination with a Social Security Number; Oregon driver's license or Oregon identification card; passport number; or financial, credit, or debit card numbers along with a security or access code or password. The City will implement and maintain reasonable safeguards to protect the security and confidentiality of personal information, including proper custody and disposal.

2. **Social Security Numbers (SSN)**

The City will safeguard SSNs on all City materials. Except when required by law, SSNs shall not be printed on mailed materials, shall not be printed on cards used to access products, services, or City buildings, and shall not be included on public postings or displays, including the city's web site. SSNs may be used for internal verification or administrative processes, but should be redacted whenever possible.

Exemptions include requirements by the State of Oregon; Federal laws, including Statute, such as W-2s, W-4s, 1099s, etc.; records that are required by law to be made public; records for use for internal verification or administrative process; and records used for enforcing a judgment or court order.

3. **Notification of Security Breach**

The City shall provide notification of a security breach as soon as possible in writing, or electronically if it is the primary manner of communication with the customer or employee, or by telephone if the person is contacted directly. The exception is if the notification would impede a criminal investigation.

4. **Department Heads**

Department heads shall:

- A. Be familiar with the Identity Theft Protection Act.
- B. Implement steps to be taken to safeguard sensitive documents described in the City's Personnel Policies.

- C. Establish and document in writing department specific safeguard practices needed to protect personal information.
 - D. Include training on identity theft protection as for the departmental new employees' (including temporary employees') orientation and provide the appropriate compliance sign-off statements to the Human Resources Department.
5. **Employees**
Employees shall adhere to this policy and any internal processes adopted by their department. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their department director if they have questions about compliance with this policy.
6. **Steps To Be Taken To Safeguard Sensitive Documents:**
- A. Review documents, forms, and processes that include or require personal information to determine if and when obtaining or retaining personal information is necessary.
 - (1) If the personal information is not necessary, revise the forms and process to eliminate that information.
 - (2) Redact personal information if no longer needed.
 - (3) Shred documents with personal information when allowed by records retention schedules.
 - B. If personal information is necessary, take steps to ensure that information is secure from unauthorized access. Examples include:
 - (1) Do not leave documents that contain personal information unattended at your desk.
 - (2) When not needed for work purposes, documents containing personal information should be stored in a secured area or in a locked file cabinet or drawer.
 - (3) Notary journals that contain personal information should be kept in a secured area or a locked file cabinet or drawer.
 - C. Lock or log off computers when leaving the workstation and otherwise comply with the computer workstation security protocols.