

**City of Springfield  
Identity Theft Protection Policy**

Approved by: Gino Grimaldi, City Manager:



Date: 7/21/05

**I. Purpose**

To outline procedures for compliance with Senate Bill 583, the Oregon Identity Theft Protection Act (OITPA).

**II. Policy**

It is the policy of the City of Springfield to protect personal information and comply with the OITPA.

**III. Objectives**

1. **Safeguarding Personal Information:** The City of Springfield 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 a SSN, Oregon driver's license, Oregon identification card, passport number or other United States issued identification number; or a financial, credit, or debit card number along with a security or access code.
2. **Social Security Numbers (SSN) Protection:** 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); or publicly posting or displaying SSNs is prohibited. Exemptions include requirements by the State of Oregon; federal laws, including statute, such as W2s, W4s, 1099s, etc.; records for use for internal verification or administrative processes; and records used for enforcing a judgment or court order.
3. **Notification of Security Breach:** 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 as soon as possible in writing, electronically if that 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. The definition of a security breach, for the purposes of this policy, will be when it is known that sensitive data has been lost or out of city staff's physical control.

**IV. Procedures**

1. **Information Technology Department (IT):** IT is responsible to establish technical controls to safeguard personal information stored in electronic format and to document safeguard practices in writing.
2. **Human Resources Department (HR):** HR is responsible to include this Identity Theft Protection as part of new employee orientation by documenting review of this policy and the concepts in "Identity Theft - A Business Guide". The business guide can be accessed at <http://www.cbs.state.or.us/dfcs/pdf/4117.pdf>.

3. **Department Directors:** Department directors are responsible to be familiar with the Identity Theft Protection Act and to meet with their staff to assess current compliance and document appropriate safeguard practices in writing.
4. **Employees:** Employees are responsible to comply with this policy and any internal processes as directed by their department. Noncompliance may result in formal disciplinary action up to and including termination of employment. Employees should contact their supervisor if they have questions about compliance with this policy.

**REFERENCES:**

Safeguard Best Practices Checklist (pdf)  
Notification Best Practices Checklist (pdf)  
Oregon Department of Consumer and Business Services Identity Theft Web site  
Oregon Department of Justice Identity Theft Web site  
Federal Trade Commission Identity Theft Web site  
<http://oregon.gov/DAS/EISPD/ESO/IDTheft.shtml> Enterprise Security Office  
Identity Theft Web site