NON-PUBLIC INFORMATION

Purpose. The city adopts this policy to help protect customers, employees, contractors and the city from damages related to loss or misuse of non-public or sensitive information. This policy outlines procedures for compliance with Senate Bill 583, the Oregon Identity Theft Protection Act (OITPA).

Policy. Public records exempt from disclosure are defined in ORS 192.502 and include information of a personal nature such as but not limited to:

- personally identifiable information about customers or names, dates of birth, driver license numbers, government issued identification numbers, telephone numbers, electronic mail addresses, or Social Security numbers;
- public body employee or volunteer addresses, Social Security numbers, dates of birth, telephone numbers, medical or workers compensation claim records;
- personal and corporate financial statements and information including tax returns, credit reports, and records submitted to or inspected by a governmental body, or information submitted to a public body in confidence.

The city will implement and maintain reasonable safeguards to protect the security and confidentiality of personal information, including proper custody and disposal. Documents, forms, and processes that include or require personal information will be reviewed to determine if and when obtaining or retaining personal information is necessary. If the personal information is not necessary, the forms and process will be revised to eliminate that information. Personal information if no longer needed shall be redacted.

Procedures.

- Social Security numbers shall not be printed on mailed materials except when required by law, shall not be printed on cards used to access products or services, and shall not be publicly posted, publicly displayed, or made available to the general public. This does not prevent the collection, use, or release of a Social Security number as required by state or federal law.

- File cabinets, desk drawers, cabinets and other storage space containing documents with non-public or sensitive information will be locked when not in use. City Hall and all facilities used for record storage shall be locked at the end of each workday.

- Internally, non-public information may be transmitted using approved city email. Non-public information sent externally must be encrypted and password protected and only to approved recipients.

- Office computers are password protected and computer screens lock after a set period of time. Computer virus protection is updated as it becomes available. Select service providers capable of maintaining appropriate safeguards and require those safeguards by contract.

- All city personnel will be provided with a copy of this policy. City personnel are encouraged to use common sense judgment in securing non-public information to the proper extent. Employees should contact their supervisor if they have questions about compliance with this policy.

- City employees should use reasonable care when accepting applications for service and be aware of any suspect activity.

- Disposal of personal information, after it is no longer needed for business purposes or as required by law, includes burning, shredding or modifying a physical record, and by destroying or erasing electronic media so that the information cannot be read or reconstructed.

- 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. Any security breach or identity theft incident shall be reported to the City Manager and City Council.

Amended by City Council motion November 13, 2008