SECTION:	**Health, Safety & Security**	**POLICY #:**	**522**
TITLE:	**Identity Theft Protection**	**PROCEDURE #:**	**522-A**
		ORDER #:	**08-62**
DEPT:	**Business Services**	**DIVISION:**	**Risk Management**
ADOPTED:	**5/08** **REVIEWED:**	**REVISED:**	

PURPOSE: To establish a policy that protects employees and customers from identity theft as a result of accidental disclosure of personal identifying information.

AUTHORITY: The Marion County Board of Commissioners may establish rules and regulations in reference to managing the interest and business of the county under ORS 203.010, 203.035 and 203.111.

The Marion County Board of Commissioners expresses the governing body's formal, organizational position of fundamental issues or specific repetitive situations through formally adopted, written policy statements. The policy statements serve as guides to decision making for both elected and appointed officials on the conduct of county business.

The Marion County Administrative Policies and Procedures manual of the Board of Commissioners outlines the forms and process through which the board takes official action on administrative policy, and is the official record of county administrative policy.

APPLICABILITY: All county departments

GENERAL POLICY: This policy establishes the requirements to protect personal identifying information and required steps in the event of a security breach, as mandated by the Oregon Consumer Identity Theft Protection Act (ORS 646A.600 through 646A.628) enacted by the Oregon Legislature in 2007.

POLICY GUIDELINES:

I. Definitions:

a. Personal Identifying Information and Personal Information: An individual's first name or initial and last name, in combination with any of the following: social security number, driver license number, state identification number, passport number or other federal identification, financial account numbers, and debit or credit card numbers in combination with the required security information necessary to access the financial account. Information

other than social security number that is required by federal, state or local government to be made available to the public is not included.

b. Breach of Security: The unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of the personal information maintained by the county.

c. Workforce Member: Employees, volunteers, and other persons whose conduct in the performance of work may provide them access to personal information. This includes full- and part-time employees, affiliates, associates, students, agents, volunteers, and staff from third-party entities who provide services.

II. Responsibilities:

Effectively safeguarding personal information includes several components. The following will be included in the county program:

All workforce members are responsible for protecting personal information that is maintained electronically and in document form. Marion County department heads and elected officials are responsible for ensuring the confidentiality, integrity, and appropriate use of all personal information.

Personal information will be collected, used, and/or stored only when there is a legitimate business need to do so. Departments will evaluate their need for personal information and, where possible, reduce the collection of sensitive consumer data.

Requests for and access to personal information will be limited to only those members of the workforce having a legitimate business need for the information. Department heads and elected officials will determine which members of the workforce have a legitimate business need for such information.

All departments will provide regular training and awareness for workforce members on the policy and procedures for safeguarding personal information.

All departments must regularly identify, define and prioritize risks to the safeguarding of personal information. The identification, definition and prioritization of risks must be based on a formal documented risk assessment process. The risk assessment process will be conducted annually and will be coordinated by risk management. Departments will develop and submit to risk management plans to address deficiencies identified in the risk assessment.

Personal information hosted on Marion County information systems will be protected. The information technology department will be responsible for implementing controls necessary to reasonably safeguard personal information contained on information systems. Securing that data may include but is not limited to:

a. Encryption and decryption policies
b. Password management
c. Log-in monitoring
d. Portable electronic device data security protocols
e. Electronic device and media disposal procedures

III. Breach:

The information technology department's designated security manager and the county's risk manager, in cooperation with the appropriate department head, will investigate any and all alleged breaches that involve personal information.

In the event of a breach to the security of computerized personal information, Marion County must notify Oregon residents whose information is believed to have been compromised by the unauthorized person(s). Security breach notification must adhere to the following:

a. Notification must be done as quickly as possible.

b. Notification may be delayed if a law enforcement agency determines that notification will impede a criminal investigation and the agency has made a written request that the notification be delayed. Notification shall be made after the law enforcement agency determines that the disclosure of the breach will not compromise the investigation.

c. The preferred method of notification is in writing. However, electronic notification can be used if that is the primary means of communication with that consumer.

d. In the event that notification costs are more than $250,000 or the number of individuals requiring notification is more than 350,000, notification may occur through mass media.

e. Violation of this policy may result in discipline up to and including discharge, subject to applicable collective bargaining agreements and personnel rules.