TITLE: Identity Theft Protection		**PROCEDURE #: 522-A**
DEPT: Business Services		**DIVISION: Risk Management**
EFFECTIVE DATE: 5/08	**REVIEWED:**	**REVISED:**

OBJECTIVE: To establish procedures to guide departments through the procedures for protecting personal identifying information.

REFERENCE: Policy #522

POLICY STATEMENT: It is the policy of Marion County to collect, use, and/or store personal identifying information only when there is a legitimate business need to do so. Marion County department heads and elected officials are responsible for ensuring the confidentiality, integrity, and appropriate use of all personal identifying information.

APPLICABILITY: All county departments

PROCEDURES:

1. The risk manager and the information technology department's designated security manager will provide coordination and leadership to ensure compliance with the Oregon Consumer Identity Theft Protection Act.

2. Departments will conduct an annual information security risk assessment of the personal information by type and location.

3. Only personal information for which there is a legitimate business need will be collected and stored. As a component of the annual information security risk assessment, departments will evaluate their need for continued collection of personal information.

4. Department heads and elected officials will be responsible for determining, based on business need and essential job functions, when to allow a member of the workforce to remove personal information from county premises.

5. Supervisors will include, as part of new employee orientation, the protection of personal information. All employees will be instructed not to send personal information electronically. When an electronic transmission of such data is necessary, the information technology department's designated security manager will be contacted for assistance with electronic security measures.

6. Department heads and elected officials will implement reasonable physical safeguards in work areas to protect against the unauthorized release or viewing of personal information. Physical safeguards will vary depending upon business needs and the extent of information kept.

7. Personal information will never be left unsecured or in plain sight in an unoccupied vehicle.

8. Personal information will be disposed of only in secure receptacles designated for confidential shredding.

9. Fax machines, copiers or printers that may receive personal information must be located away from public areas to prevent inadvertent access.

10. Access to areas that contain secure data will be limited to those employees whose essential job functions require access. Tapes, discs, zip drives, and other electronic storage media must be kept in locked cabinets or locked rooms when not in use.

11. Except as required by law or necessary to complete a required business transaction, personal information will be removed or redacted from records supplied or electronically transmitted outside the county.