ADMINISTRATIVE PROCEDURES

SECTION: 500-Information Technology	**PROCEDURE #:** 506-A
TITLE: Procedures to Safeguard Personal Information	**IMPLEMENTS POLICY #: 506**
SPONSORING DEPARTMENT/DIV: Department of Information Technology Services (ITS)	
EFFECTIVE DATE: 10/31/2025	**REVIEWED: 2/12/2026**

OBJECTIVE: To establish procedures for protecting and properly disposing of Personally Identifiable Information (PII) and reporting security breaches in compliance with applicable laws and County policies.

DEFINITIONS:

The following are terms referenced in this procedure. In conflict or absence of a term, the definitions outlined in ORS 646A.600 through 646A.628 shall govern:

1. **Personally Identifiable Information (PII):** Information that can be used to distinguish or trace an individual's identity, such as name, Social Security number, driver's license number, biometric data, or financial account information, alone or combined with other personal or identifying data.

2. **Proper Disposal or Erasing:** Secure destruction of PII to prevent reconstruction or retrieval.

3. **Technical Risk Assessment:** the process of assigning a risk rating by vetting a third-party vendor to ensure that their environment, policies, and procedures meet the County's security and compliance standards based on the sensitivity of data processed by the third party.

Refer to Policy 506 for all other definitions.

PROCEDURES:

1. Safeguarding PII:
    a. Departments must establish written procedures to protect PII. Follow Policies 506 Personal Information, 605 Acquisition of IT Solutions, 606 Cloud Service, Procedure 606-A Cloud Service Procedure, and other related policies for safeguards.

b. Workforce members must:
    i. Secure physical and digital PII (e.g., locked cabinets, encrypted devices).
    ii. Avoid storing PII on unencrypted portable media or local drives.
    iii. Use secure communication methods for transmitting PII.
    iv. Limit access and disclosure to authorized individuals only.
    v. Keep PII under control when transported.
    vi. Complete annual Security Awareness Training.

Departments must keep an inventory of systems and records containing PII and, if requested, participate in periodic audits.

2. Disposal of PII:
    a. For paper records, use county-approved shredding services managed by the Procurement Division. Department-purchased shredding devices for paper are not permitted without the approval of a County Privacy Manager.
    b. ITS is responsible for erasing PII from County-owned devices (smartphones, computer devices, including but not limited to workstations, laptops, tablets, hard drives, and copy machines).
    c. Personally owned devices used for County business must be wiped by the user in accordance with County guidelines.
    d. Portable media must be encrypted and disposed of via the Procurement Division.

3. Security Breach Reporting:
    a. Report suspected breaches immediately via the County's Incident and Risk Assessment Form process. Examples include lost devices, misdirected documents, or unauthorized access.
    b. Notify the Supervisor, Department Security Officer (DSO), Privacy Manager, and ITS as appropriate.
    c. Vendors must notify the County within 10 days of discovering a breach involving County data.
    d. Breach Notification
        i. Department Data Security Officers must notify affected individuals within 45 days of discovering a breach, unless delayed by law enforcement.
        ii. Notification must include:
            - A general description of the breach.
            - Type of PII involved.
            - Steps individuals can take to protect themselves.
            - Contact information for further inquiries.
        iii. Consult County Counsel and notify the Oregon Department of Justice when required by Oregon State law.
        iv. Documentation of low-risk incidents must be retained for 5 years. The Privacy Manager will determine whether an incident qualifies as low risk.