ADMINISTRATIVE POLICIES

SECTION: 500-Health, Safety and Security	**POLICY#:** 506
TITLE: Personally Identifiable Information Protection Policy	**R & O** #: 20-79
	IMPLEMENTED BY PROCEDURE #: 506-A
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 06/23/2020	**REVIEWED: 2/12/2026**

PURPOSE: The purpose of this policy is to define responsibilities for safeguarding Personally Identifiable Information (PII) and ensure compliance with the Oregon Consumer Information Protection Act.

APPLICABILITY: This policy and related implementing procedures applies to all individuals who use or connect to the County's network and systems, including but not limited to elected public officials, employees, volunteers, interns, consultants and contractors (collectively referred to herein as 'Workforce members').

AUTHORITY: Implements ORS 646A.600–646A.628.

This Policy will be administered by the County Administrator's Office in accordance with the authority delegated to the County Administrator in Washington County Code Section 2.04.100.

DEFINITIONS: The following are terms commonly referenced in this Policy. In the event of conflict or absence of a term, the definitions set forth in ORS 646A.600 through 646A.628 shall govern:

1. **Breach of Security:** an unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of PII that a person maintains or possesses.

   Breach of Security does not include an inadvertent acquisition of PII by a person or the person's employee or agent if the PII is not used in violation of applicable law or in a manner that harms or poses an actual threat to the security, confidentiality, or integrity of the PII.

2. **Data Security Officer:** an individual designated by the department director to be the subject matter expert on this policy and related procedures.

3. **Restricted Data:** data is classified as restricted when the unauthorized disclosure, alteration, and/or destruction of that data could cause a critical level of risk to the County. Protected or Sensitive Data is classified as Restricted Data. This includes any PII, which, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

4. **Encryption:** encryption protects restricted data such as PII in storage, when transmitting online communications, and ensures privacy. It plays a crucial role in cybersecurity by safeguarding information from being intercepted or misused by unauthorized parties. Adequate protection requires adherence to encryption standards and secure transmission protocols.

5. **Administrative security controls:** The policies, procedures, and standards established by management to govern employee behavior and manage security risks. Examples include security awareness training, hiring and termination policies, and incident response plans.

6. **CIS Controls:** The County uses the Center for Internet Security (CIS) Controls to guide its cybersecurity practices. These controls are a set of recommended actions that help protect systems and data from cyber threats. By following the CIS Framework, the County works to maintain the security of its information and minimize risk.

PII:

1. Written or electronic information, including a person's first name or first initial and last name, in combination with any one or more of the following data elements, if encryption, redaction, or other methods have not rendered the data elements unusable, or if the data elements are encrypted and the encryption key has been acquired:
    a. Social Security number;
    b. Driver's license number or state identification card number issued by the Oregon Department of Transportation;
    c. Passport number or other identification number issued by the United States;
    d. Financial account number, credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account or any other information or combination of information that a person reasonably knows or should know would permit access to the person's financial account;
    e. Data from automatic measurements of a consumer's physical characteristics, such as an image of a fingerprint, retina, or iris, that are used to authenticate the consumer's identity in the course of a financial transaction or other transaction;

f. Health insurance policy number or health insurance subscriber identification number in combination with any other unique identifier that a health insurer uses to identify the consumer; or
g. Any information about a consumer's medical history or mental or physical condition or about a health care professional's medical diagnosis or treatment of the consumer.

2. A username or other means of identifying a consumer for the purpose of permitting access to the consumer's account, together with any other method necessary to authenticate the username or means of identification.

3. Any of the data elements or any combination of the data elements described in paragraphs 1 or 2 above without the consumer's username, or the consumer's first name and first initial and last name, if:
   a. Encryption, redaction, or other methods have not rendered the data element or combination of data elements unusable; and
   b. The data element or combination of data elements would enable a person to commit identity theft against a person.
4. "PII" does not include information in a federal, state, or local government record, other than a Social Security number, that is lawfully made available to the public.

GENERAL POLICY: Workforce members must protect PII and report any suspected breaches. Guidance is provided in Procedure 506-A.

POLICY GUIDELINES

1. Workforce Member Responsibilities:
   a. Collect only necessary PII for the purpose of the business conducted.
      i. Verify an individual's identity by collecting unique identifiers. The type and number of unique identifiers will vary depending on the purpose and need of the County record.
      ii. Ensure that PII of multiple individuals is not combined into a single record inadvertently.

   b. Maintain confidentiality, integrity, and availability of PII and prevent unauthorized access

   c. Protect Social Security Numbers (SSN)
      i. Workforce members must collect only the PII necessary for business purposes. Use only the last four digits of SSNs unless the full number is legally required.
      ii. If a document contains a full SSN, it must be protected from unauthorized disclosure.
      iii. Do not share or distribute documents containing a full SSN to anyone other

than the individual named, unless permitted by state or federal law.

iv. Documents may be shared with third parties only if the SSN is redacted and the document is otherwise eligible for release.

v. Full SSNs must not be publicly posted or displayed, except as allowed by law.

vi. Full SSNs may only be included in documents sent to individuals if:

(1) There is a written request from the individual, or

(2) It is required or permitted by law.

vii. A copy of a document may be provided to a third party with the SSN redacted if the document may otherwise be released.

viii. Full SSN shall not be publicly posted or displayed, except as allowed by state or federal law.

ix. Full Social Security Numbers on any document sent must be authorized by a written request from the individual whose SSN will appear on the document, or as required or permitted by law.

d. Disposing of PII

Workforce members must properly dispose of or erase PII pursuant to County Administrative Procedure No. 506-A.

e. Report breaches immediately

Any suspected Security breach must be reported to the department's Data Security Officer or the contract administrator for any contractor. In addition, workforce members must immediately fill out an incident report for any suspected Security breach.

2. ITS Responsibilities:

ITS will ensure that:

a. The relevant administrative security controls are in place to protect the confidentiality, availability, and integrity of Restricted data not stored on County systems.

b. Ensure that the relevant CIS controls for technology owned and managed by the County are in place to protect the confidentiality, availability, and integrity of Restricted data.

3. Data Security Officer Designation:
Each department must appoint a DSO to oversee PII security and breach response.

4. Violations:
Violations may result in disciplinary action or termination of the contract. Civil penalties may apply under state law.

5. Exceptions:

   Must be approved by the Board of Commissioners unless such authority has been delegated to the County Administrator.

6. Implementation:

   Elected officials and department directors are expected to be knowledgeable of and responsible for implementing this policy within their respective departments. Compliance with this policy is mandatory for all Workforce members.

7. Periodic Review:

   ITS will review this policy at least every two years, or more often if needed, and update it as necessary.