ADMINISTRATIVE POLICY

SECTION: 600 – Information Technology	**POLICY#:** 609
TITLE: Countywide Data Governance Policy	**R & O #:** 23 - 58
	IMPLEMENTED BY PROCEDURE #: ***N/A***
SPONSORING DEPT/DIV: Department of Information Technology Services (ITS)	
ADOPTED: 5/12/25	**REVIEWED:**

PURPOSE:
This document outlines the Data Governance Plan for Washington County (hereinafter "the County"). The purpose of this plan is to establish a comprehensive framework for managing the County's data assets effectively and efficiently. This includes ensuring data quality, security, privacy, and accessibility while supporting the County's mission and strategic objectives.

Notwithstanding the general guidance this policy provides related to data governance, the County will continue to adhere to the following security regulations and any other regulations deemed applicable to the County, including, but not limited to:

1) PCI Data Security Standard
2) IRS 1075 Safeguard program
3) FBI Criminal Justice Information Services (CJIS) security policy.
4) Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules, and
5) Oregon Consumer Information Protection Act

APPLICABILITY
This policy applies to all who use or connect to the County's network and systems, including but not limited to County workforce members, interns, volunteers, elected officials, and vendors contracting with the County.

AUTHORITY:
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:

Data Assets: All data generated, collected, used, maintained, and disseminated by the County, including, but not limited to:

- **Employee data:** Personnel records, payroll, benefits.
- **Community member data:** Demographics, licenses, permits, registrations, medical records, and service requests.
- **Financial data:** Budgets, expenditures, revenues, grants.
- **Operational data:** Property records, public safety records, infrastructure data.
- **Electronic data:** Emails, documents, databases, applications, and websites.

GENERAL POLICY:

The County will classify and categorize data and systems within the enterprise based on sensitivity, business impact, and risk. Classifications will consider legal protections, contractual agreements, ethical considerations, privacy, and strategic or proprietary value. The classification level determines the security protections and access authorization mechanisms that must be used for the data.

The County will use the following classifications:

Restricted Data:

- **Definition:** 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 [1]is classified as Restricted Data.
- **Examples:** Social Security Numbers, Personally Identifiable Information (PII), Protected Health Information (PHI), and financial records.
- **Security Controls:** The highest level of security controls should be applied, including strong encryption, access controls, and regular security audits.

Confidential Data:

- **Definition:** Data is classified as confidential when the unauthorized disclosure, alteration, and/or destruction of that data could result in a moderate to high level of risk to the County. This includes, by default, all County data that is not explicitly classified as restricted or public data. Private data is classified as Confidential Data.
- **Examples:** Internal business documents, employee performance reviews, and strategic plans.
- **Security Controls:** A moderate level of security controls should be applied, including appropriate access controls, data encryption, and regular monitoring.

[1] any information that requires special security measures to prevent unauthorized access, disclosure, or modification, as it could cause significant harm if leaked, including personal details like medical records, financial information, social security numbers, or confidential business data like trade secrets; essentially, any information considered private or critical to an individual or organization.

Public Data:

- **Definition:** Data is classified as public when the unauthorized disclosure of that data would result in little or no risk to the County.
- **Examples:** Publicly available records and open data.
- **Security Controls:** While controls are not required to protect the confidentiality of public data, controls safeguarding the integrity and availability of public data remain necessary.

POLICY GUIDELINES:

Responsibilities:

Data Governance Responsibilities

- **General Data Protection training and education**
- **Data Lifecycle Management**
    - Data Planning: Identifying data needs and sources, defining data quality requirements, and developing data collection and storage strategies.
    - Data Collection: Collecting data accurately and securely, ensuring data compliance with relevant regulations.
    - Data Storage: Storing data in secure and reliable systems, implementing appropriate data backup and recovery procedures.
    - Data Use: Using data for authorized purposes only, ensuring data accuracy and integrity throughout the use process.
    - Data Sharing: Sharing data securely and responsibly with authorized parties, complying with all applicable data-sharing agreements.
    - Data Archiving: Archiving data according to legal and business requirements, ensuring data integrity and accessibility during the archival process.
    - Data Destruction: Destroying data securely and in accordance with applicable regulations.
- **Data Security**
    - Access Controls: Implementing strong authentication and authorization mechanisms, restricting access to data based on the principle of least privilege.
    - Encryption: Encrypting data both in transit and at rest.
    - Intrusion Detection and Prevention Systems (IDPS): Monitoring network traffic for suspicious activity.
    - Incident Response Plan: Developing and maintaining a plan for responding to data breaches and other security incidents.
    - Regular Security Audits and Assessments: Conducting regular security audits and assessments to identify and address vulnerabilities.
- **Data Privacy**
    - Obtaining appropriate consent for data collection and use.
    - Providing individuals with access to their personal information.
    - Allowing individuals to correct or update their personal information.
    - Protecting the privacy of sensitive personal information.

Data Governance Roles

The following roles support the data governance activities described above.

- **Data Owner:**
  - Typically, executive leadership roles (department directors, division managers) or executive leadership delegate.
  - Controls the data in a specific data domain.
  - Ensures the information within that domain is correctly maintained.
  - Responsible for data quality, accuracy, and security.
  - Determines appropriate use, access, and sharing of data.
  - Is accountable for compliance with all applicable laws and regulations.
- **Data Steward:**
  - Typically located within the organization's business side, the Subject Matter Expert (SME) is responsible for the data.
  - Manages the quality of defined datasets daily.
  - Explains the importance and use of the information. (by developing and maintaining tools like a data dictionary)
  - Supports the Data Owner in managing data quality and integrity.
  - Acts as a liaison between data owners and data users.
- **Data Custodian:**
  - Typically, Information Technology Services manages the security and storage infrastructure unless this is vendor-supported.
  - Responsible for developing and maintaining security safeguards for specific data collections.
  - Ensures compliance with the Data Classification and Handling Policy.
  - In cloud environments, the County Cloud Service Sponsor may act as the Data Owner, and the Cloud Service Provider may act as the Data Custodian.
- **ITS:**
  - Supports the County Cloud Service Sponsor when requested.
  - Performs Cloud Service Reviews.

- **Data Governance Committee:** Data Governance Committees will be established to oversee the implementation and enforcement of this data policy within specific subject matter areas. These Committees will receive support and guidance from the County Risk Manager & Privacy Officer and the ITS Information Security Division.

  - A Data Security Officer: A County employee assigned responsibility by the department director as the subject matter expert on Personal Information Protection Policy 506 and related procedures.
  - Privacy Managers: A county employee is responsible for implementing and ensuring compliance with the HIPAA Privacy Policy #501 and other specific procedures applicable to individual covered components.
  - Public Records Officer: A County employee responsible for coordinating and assisting the workforce in public records-related matters, including determining the appropriate retention schedule for email messages and attachments according

to Policy 208 - Management, Preservation, and Storage of Electronic Public Records.

Exceptions:

Exceptions may only be granted by the Washington County Board of Commissioners unless such authority has been delegated to the County Administrator.

Implementation:

Elected officials and department directors are expected to be knowledgeable about and responsible for implementing this policy within their respective departments. Observance of this policy and policies that address data governance and IT acceptable use[2] is mandatory for all County employees, and violation may result in disciplinary action up to and including termination

Periodic Review:

The Information Technology Services Department shall review this policy at least every three years, or more often if necessary, and update it as required.

[2] See Personnel Rules and Regulations (PDF 896.21 KB) and IT Acceptable Use Policy 602