ADMINISTRATIVE POLICY

SECTION: 600	**POLICY#:** 604
TITLE: County Enterprise Information Technology Security Program	**R & O #:** 23-58
	IMPLEMENTED BY PROCEDURE #: N/A
SPONSORING DEPT/DIV: Information Technology Services Department (ITS)	
ADOPTED: 09/26/2023	**REVIEWED: 2/12/2026**

PURPOSE: The purpose of this policy is to provide authority to the County Administrative Office (CAO) and Information Technology Services (ITS) to select an Information Security Framework, and to develop and implement a County Enterprise Information Security Program ("Program") within the chosen framework. Notwithstanding the chosen Framework, 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. FBI Criminal Justice Information Services (CJIS) security policy;
3. Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules; and
4. Oregon Consumer Information Protection Act.

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

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

DEFINITIONS: As used in this policy:

1. **Enterprise Information Security Management Program** and **Program** mean the governance, operational policies, procedures, rules, monitoring, and training in the form of a program for protecting the County's data, assets, and critical resources from a wide range of threats to ensure business continuity and minimize security risk.

2. **Cybersecurity** is the practice of protecting the County's computing environments and the Restricted or Confidential Information contained within those environments from cyberattacks. Cybersecurity is a component of information security.

3. **Information Security** means the practice of protecting information by implementing controls to secure Restricted or Confidential Information from data breaches and unauthorized access.

4. **Restricted Data** means it 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.
    - Examples: Social Security Numbers, Personally Identifiable Information (PII), Protected Health Information (PHI), and financial records.

5. **Confidential Data** means it 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.

6. **Security Framework** or **Framework** means a set of guidelines, best practices, and standards designed to help organizations manage and reduce cybersecurity risks. The Framework provides a systematic approach to identifying, protecting, detecting, responding to, and recovering from cyber threats.

7. **Security Regulations** are official rules issued by government agencies that dictate how information must be handled, maintained, and disposed of.

GENERAL POLICY:

Washington County will adopt a Framework designed to address the County's specific needs. This Framework will ensure protection while allowing flexibility to respond to the community's needs. Additionally, a Program will be established within the Framework. This Program, along with the related operational policies, plans, and procedures, will serve as guidance for County workforce members as technical security controls are implemented.

POLICY GUIDELINES:

1. <u>Responsibilities:</u>

    a. Information Security Division: An Information Security Division (ISD) shall be created under the Chief Information Officer (CIO) and led by an Information Security Officer (ISO) to design, build, and implement a County Enterprise Information Security Program. The ISD shall:

        i. Create an appropriate Framework from industry-standard best practice frameworks, or tailor such framework or frameworks to meet County needs.

ii. Establish security controls within the Framework to be used as a measure of maturity for security within the County.

iii. Create an appropriate program to guide how information security will be addressed throughout the County. The Framework should guide the Program with regard to where the County needs to be, and the operational policies and procedures should still be tailored to the County environment. The program shall include methods and processes to continuously assess and address cyber and information security risks.

iv. Be accountable to the Board of County Commissioners or its designee for the County's enterprise information security program.

b. Governance: The County's information security governance is structured as follows:

i. **Board of County Commissioners (BCC)**: This body is ultimately accountable for Countywide governance, including information security.

ii. **County Administrator (CA)**: Delegated authority for implementing and overseeing information security governance.

iii. **Chief Information Officer (CIO)**: Responsible for Countywide cybersecurity strategy, policy approval, and executive-level advocacy.

iv. **Information Security Officer (ISO)**: Leads the Information Security Division, maintains the Countywide Security Plan, and ensures alignment with the County's risk governance framework.

v. **Technology Continuity & Security Coordinator**: This position ensures compliance with regulatory requirements, manages training, and conducts audits.

vi. **Cybersecurity Analysts**: Monitor, assess, and respond to security threats and vulnerabilities.

vii. **Departmental Security Liaisons (e.g., Data Security Officers, Privacy Managers, Local Agency Security Officer (LASO)**: Act as conduits between departments and the Information Security Division.

viii. **All County Workforce Members**: Are responsible for complying with security policies, reporting incidents, and participating in training.

2. Exceptions:

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

3. Periodic Review:

ITS shall review this policy every two years, or more often, based on changes to the County's risk landscape and new and emerging cyber threats.