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	
ADOPTED: 09/26/2023	**REVIEWED:**

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 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. IRS 1075 Safeguard Program;
3. FBI Criminal Justice Information Services (CJIS) security policies;
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: 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. **Cyber security** means the practice of protecting the County's computing environments and the sensitive information contained within those environments from cyberattack. Cyber security is part of information security.
3. **Information security** means the practice of protecting information by implementing controls to protect sensitive business information from data leaks and unauthorized access.
4. **Security Framework** and **Framework** mean a set of standards and controls, developed by known information security agencies such as the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST).
5. **Security regulations** are security rules made by executive departments and agencies that require adherence to the regulatory rules for handling, maintaining, or disposing of information.

GENERAL POLICY:

Washington County will adopt a Framework that will meet the County's unique requirements. The County will be protected but given flexibility to be responsive to community needs. Within the Framework, a Program shall also be created. This Program and associated operational policies, plans and procedures will be used as guidance for County workforce members as technical security controls are put in place and documented.

POLICY GUIDELINES:

1. Responsibilities:

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

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

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

(C) 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.

(D) Be the accountable to the CAO or to their designee for the County's enterprise information security

(b) Governance: An Information Security Steering Committee, chaired by the CISO or ISO, will be created to provide oversight of the information security program. Membership on the Committee will be from within internal County stakeholders and must include, at a minimum, representatives from each of the County's functional areas, General Government,

Public Safety and Justice, Land Use & Transportation, Housing, Health & Suman Services and Culture, Education & Recreation. The Committee shall review and propose information security policies and procedures created by the ISD for possibly adoption by the Washington County Board of Commissioners or the County Administrator.

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:

This policy shall be reviewed by ITS annually, or more often based on changes to the County's risk landscape and new and emerging cyber threats.