ARAPAHOE COUNTY

Arapahoe County

5334 South Prince Street
Littleton, CO 80120
303-795-4630
Relay Colorado 711

Board Summary Report

File #: 24-294 **Agenda Date:** 6/4/2024 **Agenda #:**

To: Board of County Commissioners

Through: Philip Savino, Director, Information Technology

Prepared By:
Philip Savino, Director, Information Technology

Presenter: Philip Savino, Director, Information Technology

Subject:
1:00 PM *Information Security Policy

Purpose and Request:
The Arapahoe County Information Technology Department (IT) respectfully requests approval from the Board of County Commissioners to add the Information Security Policy to a consent agenda for formal adoption. This policy is designed to safeguard our information technology infrastructure and protect sensitive information from potential threats. This initiative is a critical step in safeguarding our digital assets, ensuring operational continuity, and upholding the trust and confidence of our community. Based on Board direction, this item will be brought forward on consent agenda for formal approval.

Background and Discussion:
This Information Security Policy is designed to enhance protection and compliance across all digital information handled by the county.

The Information Security policy is crucial for safeguarding sensitive data and ensuring that all county employees adhere to the highest standards of security. The development of the Information Security policy included thorough collaboration with the County Attorney's office and County executive leadership, to identify and integrate all applicable laws relevant to the county's operations.

This comprehensive approach ensures that the policy is both effective and compliant with legal standards, supporting our ongoing commitment to information security and integrity.

We believe that the county-wide Information Security Policy is essential for the following reasons:

- Protection of Sensitive Data: We hold vast amounts of sensitive data, including residents' personal information, financial records, and critical government data. The Information Security Policy will ensure robust safeguards are in place to protect this information.
- Operational Continuity: Cyberattacks can disrupt essential services, causing significant downtime and inconvenience. The policy ensures that our employees and systems are resilient and capable of maintaining essential operations even during security incidents.
- Compliance and Legal Requirements: Government agencies are increasingly held to stringent cybersecurity regulations. The policy will help us stay compliant with state and federal requirements,

potentially saving us from legal and financial repercussions.

- Reputation and Trust: The policy demonstrates our commitment to the safety and security of the community. It helps build and maintain trust with the public and partners.

We believe that by pursuing the adoption of this policy, we are making significant strides toward a safer and more secure digital environment for the county.

Fiscal Impact: None

Alternatives: The current state would be to remain without a formal cybersecurity policy and assume the risks that come without having one.

Alignment with Strategic Plan:

☒Be fiscally sustainable.

☒Provide essential and mandated service.

☒Be community-focused

Staff Recommendation: The Information Technology Department and E-Team recommend that the Board of County Commissioners support the adoption and approval of this county-wide Information Security Policy.

Concurrence: E-Team has reviewed and approved this policy.