Title: Administrative Policy Information Security Advisory Committee	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 3
	Effective Date November 2, 2021
Policy Custodian Business, Innovation and Technology	**Adoption/Revision Date** November 2, 2021

Adopting Resolution(s): CC21-543

References (Statutes /Resos/Policies): C.R.S. § 6-1-713 – 713.5, 24-73-101 et seq; CC16-010, CC18-412

Purpose: To prevent the unauthorized loss or exposure of county information or the unauthorized access or modification of county systems that could cause harm to the county, its employees and our citizens or could subject the county to fines or other sanctions.

Policy: Information Security Advisory Committee

A. By this Policy, the county forms the Information Security Advisory Committee (ISAC) to take actions to appropriately protect county information and information systems, assign roles and responsibilities, and communicate risk.

B. Committee Composition

1. The Committee shall be comprised of the Chief Information Security Officer (CISO), a representative from Public Affairs, Human Resources and the County Attorney's Office, and an information technology management representative from each of the following: Business Innovation and Technology; Sheriff; District Attorney; Parks, Public Health; Human Services, and Library.

2. Representatives of other County Departments/Divisions or Elected or Appointed Officials are encouraged to participate in the Committee.

C. Procedures

1. The CISO or designee shall act as the chair of ISAC.

2. ISAC shall meet on a regular basis to review the effectiveness of information security policies, procedures and training and evaluate the impacts of changes in technology and threats that may affect compliance with legal and regulatory requirements or the risk to county information. ISAC shall provide reports on findings as needed.

3. ISAC shall draft and/or provide comments on all proposed draft policies, procedures, standards, other documents or training courses related to information security.

4. Each ISAC member shall be responsible for
    a. Communicating information security policies, procedures, standards, courses or other documents related to information security to the executive management and employees of their Department, Division or Office.
    b. Providing feedback on proposed policy changes as well as recommending new policy or changes to existing policy when policy gaps are identified.
    c. Maintaining compliance with county technology policy, procedure and standards within their Department, Division or Office.
    d. Identifying risk related to their Department, Division or Office and reporting that information to the CISO and ISAC so that information can be maintained in a countywide risk register.
    e. Remediating risk related to their Department, Division or Office is by using county IT staff or 3rd party resources.
    f. Completing trainings to act as an Incident Commander.

5. The CISO shall be responsible for communicating information security policies, procedures, standards, courses or other documents related to information security to the Departments/Divisions or Offices who are not represented in ISAC.

6. The ISAC shall provide reports to the Board of County Commissioners and Elected/Appointed Officials annually or more often as needed.

7. Annually, ISAC shall identify and recommend project requests to support the upcoming year's security roadmap.