Title: Administrative Policy Information Security Advisory Committee	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 3
	Effective Date December 11, 2018
Policy Custodian Information Technology Service Division	**Adoption/Revision Date** December 11, 2018

Adopting Resolution(s): CC18-412

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

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

Policy: Information Security Advisory Committee

A. Jefferson County possesses information that is sensitive and valuable. The unauthorized loss or exposure of sensitive information could cause irreparable harm to the county, its employees and our citizens and could also subject the county to fines or other sanctions. By this Policy, the county forms the Information Security Advisory Committee (ISAC) to take actions to appropriately protect such information and assign roles and responsibilities.

B. Committee Composition

1. The Committee shall be comprised of the Chief Information Security Officer (CISO) and an information technology management representative from each of the following: IT Services Division; Sheriff; District Attorney; Elections, 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 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. 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.

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

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