Title: Administrative Policy Information Security	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 2
	Effective Date December 11, 2018
Policy Custodian Information Technology Services Division	**Adoption/Revision Date** December 11, 2018

Adopting Resolution(s): CC18-412

References (Statutes/Resos/Policies): 45 CFR 160.103; C.R.S. § 6-1-713 – 713.5, 24-73-101 et seq; CC16-010

Purpose: To establish roles and responsibilities to ensure the security of Jefferson County information in both electronic and physical forms.

A. Definitions

1. Covered Employees and Other Individuals: County elected or appointed officials, employees, volunteers, contractors, business partners and vendors that handle or process confidential information or work in areas that handle such information for a county Department/Division or Elected or Appointed Office.

2. Criminal Justice Information Systems (CJIS): Criminal Justice Information is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property (when accompanied by any personally identifiable information), and case/incident history data.

3. Data Breach: A data breach is an Information Security Incident in which sensitive, protected or confidential information is copied, transmitted, viewed, stolen or used by an unauthorized party.

4. Information Security Incident: The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with the operations of information systems and processes.

5. ISAC Standard - Information Security Incident Response Guide: A document setting forth procedures for monitoring and analyzing of security alerts and distribution of information to appropriate information security staff and executive management, and procedures for response to Information Security Incidents and Data Breaches.

6. Protected Health Information (PHI): As defined in 45 CFR 160.103.

7. Personally Identifiable Information (PII): As defined in C.R.S. § 6-1-713 – 713.5, 24-73-101 et seq

8. Payment Card Industry Data Security Standard (PCI DSS): A proprietary information security standard for organizations that handle branded credit cards from the major card companies including Visa, Master Card, American Express, Discover and JCB. The standard was created to increase controls around cardholder data and to reduce credit card fraud via exposure of that data.

B. Applicability:

1. This Policy shall apply to all Departments/Divisions that report to the Board of County Commissioners, Elected Officials and Appointed Officials and their Offices.

2. Covered Employees and Other Individuals.

C. Chief Information Security Officer

1. The BCC authorizes the IT Services Division Director, or in the event there is a vacancy in that position, the County Manager, to designate and name an employee to serve as the CISO in a Procedure that implements this policy.

2. Responsibilities of the CISO:

a. Coordinate distribution of this policy and any applicable procedures, standards, and/or other documents, to Covered Employees and Other Individuals and applicable management. Coordinate training of Covered Employees and Other Individuals in applicable information security related policies, procedures, standards and other documents. Coordinate, as appropriate, acknowledgement from Covered Employees and Other Individuals that they have read, understand and agree to abide by this Policy, and any applicable procedures, standards, and/or other documents.

b. Serves as the Designated Security Official under Subpart C of HIPAA who shall have the authority for the development and implementation of the overall county policies and procedures required by Subpart C of HIPAA for security standards per the Health Insurance Portability and Accountability Act Policy.

c. Oversee compliance with this Policy. Assist in investigations of any reported violations of this Policy and any other applicable policies, procedures, standards, and/or other documents pertaining to Information Security Incidents or Data Breaches.

d. Oversee an annual review and update of this Policy and any applicable procedures, standards, and/or other documents needed to reflect changes to business objectives or risks in the environment.

e. Establish and maintain a Vendor Security Management program. Develop processes to manage the sharing of confidential information and the use of services such as web hosting, backup storage facilities or others that could affect the security of confidential information.

f. Oversee periodic internal and external risk assessments to measure the effectiveness of the security program and coordinate remediation plans as needed. This shall include controls for monitoring and controlling access to confidential information.

3. The CISO shall have the authority to terminate access to systems and information for any users who fail to comply with information security policies, procedures, standards and/or other documents who are deemed to create a risk to information security. The CISO may delegate this authority, in writing, to other county IT Directors/Managers as needed to ensure timely action.

D. Information Security Incident Response Responsibilities

1. The CISO will oversee operation of the ISAC Standard - Information Security Incident Response Guide. The following lead positions shall conduct Information Security Incident and Data Breach investigations as noted below in consultation with the CISO.

2. Sheriff's Information Services Director or designee: Lead investigation of Information Security Incidents, including CJIS compliance, totally within the Sheriff's offices.

3. District Attorney's Information Technology Director or designee: Lead the investigation of Information Security Incidents, including CJIS compliance totally within the office of the District Attorney.

4. Public Health's Supervisor Information Technology, Purchasing and Vital Records or designee: Lead investigation of Information Security Incidents including HIPAA and PHI compliance, totally within the offices of Public Health.

5. Human Services' Information Technology Director or designee: lead the investigation of Information Security Incidents, including HIPAA and PHI compliance, totally within the offices of Human Services.

6. Library's Information Technology Director or designee: Lead the investigation of Information Security Incidents totally within the offices of the Library.

7. CISO or designee: Lead the investigation of Information Security Incidents involving HIPAA, PCI, PII, or PHI compliance for Departments, Divisions and Offices that do not have a lead designated in this policy and those involving multiple Departments, Divisions and Offices. Reports of such incidents will be forwarded to the HIPAA Privacy Officer.

8. CISO or designee: Lead the investigation for all other Information Security Incidents and consult with other IT staff as needed.

9. Public Information Officers or designees for Library, Public Health, Sheriff, District Attorney and Human Services: Responsible for coordination of all communications with the media regarding Information Security Incidents totally within their Departments, Divisions and Offices.

10. County's Public Affairs Director or designee: Responsible for coordination of all communications with the media regarding Information Security Incidents involving multiple Departments, Divisions and Offices and those Departments, Divisions and Offices without their own Public Information Officer.

11. The Director of Human Resources or designee: Responsible for coordination of all communications with Jefferson County employees regarding Information Security Incidents involving a Data Breach of employee information.

12. County Attorney or designee: Perform analysis and provide legal recommendations for responding to Information Security Incidents and Data Breaches except that the Public Health Attorney will perform the analysis and provide legal recommendations for responding to a Security Incident or Data Breach totally within Public Health.

13. Each lead position identified above will proactively support requests for assistance from other lead positions or their designees.

14. The ISAC Standard - Information Security Incident Response Guide should be reviewed to identify other County Departments, Divisions and Offices that should be consulted as appropriate.

E. Information Security Officers and Records Managers

1. Each Department/Division Director, Elected Official and Appointed Official shall designate one or more staff to serve as their Department's, Division's, or Office's Information Security Officer and/or Records Manager.

2. The Information Technology, Information Security Officer and Records Manager staff in all Departments, Divisions, or Offices have the primary responsibilities for day-to-day oversight of Information Security and compliance with this policy and any applicable policies, procedures, standards or other documents as applicable to their organizations.

F. Department/Division Directors and Elected/Appointed Officials
Department/Division Directors and Elected/Appointed Officials shall be responsible for ensuring that their Covered Employees and Other Individuals are aware of the need to protect the County's information and resources.

G. Managers and Employees

1. All managers and supervisors shall be responsible for determining the sensitivity and criticality of the county/citizen information and records for which they are responsible. These managers shall determine who will be authorized to access their information and the use of this information.

2. Managers shall ensure that all Covered Employees and Other Individuals have passed appropriate background checks conducted or coordinated by Human Resources, and that appropriate notification is provided to the appropriate county IT Directors/Managers for terminations and transfers. Contracts with business partners, vendors and contractors must include terms requiring their company to conduct appropriate background checks on their staff who require access to confidential information.

3. All Covered Employees and Other Individuals shall be responsible for protecting county and citizen information and records from unauthorized access, modification, destruction, or disclosure, whether accidental or intentional. In addition, all Covered Employees and Other Individuals shall be responsible for complying with this and other Jefferson County policies and any applicable procedures, standards, and/or other documents specifying computer, network, document, data and information security measures. Covered Employees and Other Individuals will be required to confirm that they have read, understand and agree to abide by this Policy, and any applicable procedures, standards, and/or other documents.