Title: Administrative Policy Information Security	**Policy No.** Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 2
	Effective Date July 20, 2021
Policy Custodian Business Innovation and Technology Division	**Adoption/Revision Date** July 20, 2021

Adopting Resolution(s): CC21-196

References (Statutes/Resos/Policies): 45 CFR 160.103; C.R.S. § 6-1-713 – 713.5, 24-73-101 et seq; CC16-010, CC18-412; CJIS Policy, Payment Card Industry Data Security Standard (PCI DSS)

Purpose: To establish and maintain a set of practices and roles and responsibilities to manage physical and electronic information security risk cost-effectively over time through informed decision making.

A. Definitions

1. Covered Employees and Other Individuals: County elected or appointed officials, employees, volunteers, contractors, business partners and vendors.

2. 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.

3. 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.

4. Risk: Probable frequency and probable magnitude of future loss.

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. Core Principles

The Information Security Program will develop, maintain and follow practices to perform its work according to the following principles:

1. Security is everyone's responsibility.

2. Security is a process of continuous improvement.

3. Our security efforts must first be focused on our high value targets: targets posing a physical security risk, a significant financial impact or a compliance, legal or regulatory risk.

4. Security must be built-in to business processes and systems from the start.

5. Threats are mitigated through the right combination of people, processes, and technology and are prioritized commensurate with the risk.

6. Compliance is the result of excellent security practices.

7. Security must be efficient – only those security resources necessary to achieve our mission are acquired, deployed and retained.

8. Security must be effective – security must be results-oriented, and outcomes must be measured, tracked, and compared to the resources expended.

9. When possible, security should be effortless – the most effective controls and solutions are those that are transparent.

10. Collaboration is critical - partnering will allow us to accomplish far more than what might be possible when working in isolation.

D. Goals

Understanding and reducing the risk footprint, preventing data loss and business interruption, detecting and responding efficiently to compromise, and educating and empowering employees and citizens.

E. Information Security Responsibilities

1. Chief Information Security Officer

    a. The BCC authorizes the BIT 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.

    b. The CISO will oversee operation of Information Security Advisory committee and the county's information security program.

2. Incident Response

The following lead positions shall conduct Information Security Incident and Data Breach investigations as noted below in consultation with the CISO.

a. CISO, Incident Commander or Incident Lead: Lead the investigation of Information Security Incidents for Departments, Divisions and Offices that do not have a lead designated in this policy and those involving multiple Departments, Divisions and Offices.

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

c. 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.

d. 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.

e. 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.

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

g. 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.

h. 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.

i. 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.

j. County Attorney or designee: Perform analysis and provide legal recommendations for responding to Information Security Incidents and Data Breaches.

3. Information Security Officers and Records Managers

    a. 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.

    b. 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.

4. 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.

5. Managers and Employees

    a. 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.

    b. Managers and supervisors 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.

6. Information Technology Employees
   All IT employees shall be responsible for understanding and complying with Information Technology policy, procedures and standards, reporting non-compliant matters, timely remediation of known vulnerabilities, responding to incidents according to the Incident Response Plan, and keeping current with training, trends and technology.

7. 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.