Procedure Part 5, Staff Policies Chapter 4, Information Technology Security and Safety Section 2, Information Security, Chief Information Security Officer	**Last Update:** August 8, 2021

References: County Policy Manual- Information Security

Purpose: To designate a Chief Information Security Officer

Procedure: Chief Information Security Officer

A. Designating an Employee to Serve as Chief Information Security Officer

1. Chief Information Security Officer shall be:
   Jill Fraser, Chief Information Security Officer
   Jefferson County Information Technology Services
   3500 Illinois Street – Suite 2500
   Golden CO 80401
   303-271-8828

B. Responsibilities of the CISO:

1. Coordinate distribution of information security policy and any applicable procedures, standards, and/or other documents, to Covered Employees and Other Individuals and applicable management.

2. Coordinate training of Covered Employees and Other Individuals in applicable information security related policies, procedures, standards and other documents.

3. Coordinate, as appropriate, acknowledgement from Covered Employees and Other Individuals that they have read, understand and agree to abide by information security Policy, and any applicable procedures, standards, and/or other documents.

4. 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.

5. Oversee compliance with information security Policy.

6. Assist in investigations of any reported violations of information

security Policy and any other applicable policies, procedures, standards, and/or other documents pertaining to Information Security Incidents or Data Breaches.

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

8. Establish and maintain a Vendor Security Management program.

9. 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.

10. 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.

11. 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.