Title: Administrative Policy Information Security Incident Response	**Policy No.** Part 1, County Administration, Chapter 3, Operations, Section 14
	Effective Date August 28, 2018
Policy Custodian Board of County Commissioners	**Adoption/Revision Date** August 28, 2018

Adopting Resolution(s): CC18-290

References (Statutes /Resos/Policies): Payment Card Industry Policy 4.8.1, Information Security Policy 5.4.2, Health Insurance Portability and Accountability Act 5.2.1, HB 1128 § 6-1-713.5

Purpose: To establish information security incident definitions, roles and responsibilities to ensure coordinated and effective cyber incident response.

Policy: Information Security Incident Response

A. Definitions

1. Information Security Emergency means any occurrence or imminent threat of widespread or severe loss or exposure of county information systems, data or IT resources that could result in damage, injury, loss of life or property, significant impairment or loss of ability to deliver county services resulting from cyber activity, referred to as an “Incident”.

2. "Level 1 Incident" means the occurrence or imminent threat of widespread or severe damage, injury, or loss of life or property resulting from outage of critical business processes of such severity that it cannot be handled by the county in the conduct of its normal duties. Level 1 incidents often have life impacting consequences, exceed $1 million in financial impacts, have serious legal or regulatory compliance ramifications, and have high media/public interests.

3. “Level 2 Incident” means the occurrence or imminent threat of damage, injury to or loss of property resulting from outage of business processes that can often be handled by the county in the conduct of its normal duties or with external support. Level 2 incidents may be contained within a single information technology domain or may cross boundaries to include multiple county domains. Level 2 incidents have no life impacting consequences, often have less than $1 million in financial impacts, have legal or regulatory compliance ramifications, and have minimal media/public interests.

4. “Level 3 Incident” means the possible threat of damage resulting from outage of business processes can be handled by the county in the conduct of its normal duties. Level 3 incidents are contained within a single information technology domain. Level 3 Incidents are routinely handled by the county within its normal duties and within operating budgets, and have no legal ramifications, or media/public interests.

5. "Cyber Security Management" means the marshaling of all resources available to respond to all Incident Levels.

6. "Mitigation" means any activities that eliminate or reduce the probability of the Incident.

7. "Preparedness" means the development of plans, the stockpiling and inventory of critical resources, the organization and training of response personnel, and the exercise of plans.

8. "Recovery" means those actions, both short-term and long-term, that result in the restoration of services and information for Jefferson County after an Incident. Activity includes but is not limited to notification of employees, the public and appropriate regulatory agencies.

B. Declaration of a Level 1 Incident

1. The Board of County Commissioners delegates the authority to declare, continue or discontinue a Level 1 Incident to the Chairman of the Board of County Commissioners or, if the Chairman is not available, to any Commissioner. Such declaration may be provided by email, written or verbal communications and may be continued, renewed, or discontinued at any time by the delegates defined above.

2. The declaration of a Level 1 Incident:

    a. Activates the response and recovery aspects of all applicable county resources.

    b. Authorizes the Chairman or delegate to communicate and collaborate with external parties for incident resolution.

    c. Authorizes the Chairman or delegate to execute purchases, requests and agreements for aide and assistance.

    d. Authorizes the Chairman or delegate to provide consent to search all computers and IT resources, including personally owned devices that are used for county business.

3. The Board of County Commissioners may allocate emergency funds when costs of the disaster exceed authorized emergency response budgets.

C. CISO Duties and Authority During a Level 1 or multi-department Level 2 Incident

1. The duties and powers of the Chief Information Security Officer, or designee shall include, but shall not be limited to the following:

a. Assume command of the Cyber Security Management, Mitigation and Recovery functions.

b. Marshal appropriate resources as needed.

c. Request and negotiate aid agreements as needed.

d. Request additional funds from the BCC Chairman or delegate when costs exceed operating budgets.

D. County IT Staff are authorized to implement prescribed containment steps during any incident level.

E. Cyber Security Management

1. Ransom Situations: The county shall attempt to recover ransomed resources through backups or other technical means. The county will not negotiate a ransom.

2. Containment: The county's first response to a cyber security threat shall be to isolate the infected systems. This may range from removing the infected IT resource from the network to severing all connections to other domains in response to a cyber incident.

3. Notification of a Breach: The county shall follow all Colorado State statutes and all other Legal and Regulatory Compliance requirements when responding to a breach of Sensitive, Protected, or Confidential Information.

F. Preparedness

1. The Chief Information Security Officer is hereby empowered to:

a. Prepare and keep current a plan to be known as the Jefferson County Cyber Security Management Plan. The Cyber Security Management Plan will be consistent with the standards and principles of the National

Institute of Standards and Technology (NIST) current guidelines as well as all applicable legal and regulatory compliance requirements.

b. Seek, obtain, or assist in obtaining supplies, equipment and services needed for the protection of the life and property of the people of Jefferson County.

c. Direct Preparedness coordination and cooperation between the county organizations, services and staff, and resolve questions of authority and responsibility that may arise between such organizations, services and staff.

d. Represent Jefferson County in all dealings with public or private agencies pertaining to Cyber Security Management, except to the extent it involves the duties of another County official, and then only in coordination with that official.

G. Elected Officials, Appointed Officials, and Department Directors

1. The duties and powers of the Elected Officials, Appointed Officials and Department Directors shall include, but shall not be limited to the following:

    a. Ongoing incident response planning, each Elected Official, Appointed Official and Department Director will participate when requested in the planning and preparation by providing personnel and information under their control.
    b. During any Incident, each Elected Official, Appointed Official, and Department Director will participate when requested by providing resources and incident information under their control.
    c. During any Incident, each Elected Official, Appointed Official and Department director may take steps to contain an incident according to prescribed containment steps.
    d. Following any Incident, each Elected Official, Appointed Official, and Department Director will participate when requested in the recovery and lessons learned by providing personnel and information under their control.