Title: Administrative Policy Access Authorization and Identification Access Badges	**Policy No**. Part 5, Staff Policies Chapter 5, Safety Section 2
	Effective Date February 23, 2021
Policy Custodian Facilities Management	**Adoption/Revision Date** February 23, 2021

Adopting Resolution(s): CC21-058

References: Health Insurance Portability and Accountability Act of 1996 (HIPAA); Access Form, Background Check Procedure; Security and Safety Committee Policy; CC17-188, CC19-428

Purpose: To implement security standards regarding Identification Access Badges and Physical Access Authorization.

A. Definitions

1. Authorized Representative: An employee who has been designated by the Elected/Appointed Official or Department/Division Director to approve access requests for employees, members of an Appointed Board or Commission, contract worker, vendor, state employee, and/or volunteer within the Department, Division, or Office.

B. Applicability

1. This policy applies to all employees of Jefferson County regardless of position or status, contract workers, vendor, state employees and volunteers, excluding the District Attorney and Sheriff employees.

2. Members of Boards and Commissions are subject to these requirements if issued an identification access badge by Jefferson County.

C. Individual Responsibilities

1. Display

a. All individuals who are issued an identification access badge shall wear it in such a way that the badge is clearly visible while in a county building, facility or on county property. The District Attorney may identify circumstances when his/her employees do not need to display identification access badges while in a county building, facility or on county property.

b. The Elected/Appointed Official or Department/Division Director may require individuals whom they supervise to wear the identification badge be worn while conducting county business off premise.

c. All employees required to have CJIS clearance shall ensure they obtain and wear an access badge that clearly displays the clearance.

2. Individuals shall not alter/deface his/her identification access badge.

3. Lost Identification Access Badges
   Lost identification access badges shall be reported immediately to Facilities Management. A new Access Form must be completed, signed and submitted by the Division/Office Authorized Representative before a replacement identification access badge will be issued. A replacement fee will be charged for lost or damaged badges.

4. Separation from the County
   Identification access badges shall be left with the supervisor or Authorized Representative upon separation from the county.

5. The individual shall not possess a duplicate identification access badge.

D. Authorized Representative Responsibilities

1. Prior to a new employee's start date, the Authorized Representative must approve and submit the Access Form to Human Resources.

2. Prior to a state employee, volunteer, contractor, vendor, or appointed board or commission member's start date, and prior to a re-issuance of a lost or stolen badge, the Authorized Representative must approve and submit an Access Form to Facilities Management.

3. The Authorized Representative(s) for Human Services, Business Innovation & Technology Services, Public Health, and Facilities Management shall be responsible for the issuance and monitoring of unassigned access badges. These badges must be kept in a secured work area and within a locked drawer or cabinet when not in use. A log must be kept to track the issuance and use of these badges. Facility Management must be notified immediately if an unassigned access badge is not returned.

4. The Authorized Representative shall, with the approval of the Elected/Appointed Official or Department/Division Director, determine access to areas based on the individual's role or job function. Access to areas that are not relevant to or necessary for an individual's job function, such as another building, division/office, or areas that contain confidential information or data servers, is not permitted.

5. An Authorized Representative may initiate a background check for employees, members of an Appointed Board or Commission, and/or volunteer within the Department, Division, or Office prior to authorizing access.

6. Contractor and Vendor Badges

   a. The Authorized Representative must ensure that an appropriate background check has been conducted for a contractor or vendor who is issued an access badge.

   b. Contractors working in areas that contain data servers must be escorted by an employee, even if the contractor is background checked, unless the Authorized Representative obtains a signed waiver from the Elected/Appointed Official or Department/Division Director or designated HIPAA Security Official.

7. The Authorized Representative must complete the audits initiated by Facilities Management to ensure that authorized access is consistent with current job function access requirements.

8. Deactivation
   The Authorized Representative shall notify Facilities Management and return the identification access badge for the following individuals when:

   a. An Elected/Appointed Official's term is concluded.

   b. An appointed board or commission member who has been issued an access badge is no longer a member of the board or commission.

   c. A state employee separates from a position associated with the county courts or other county Division or Office.

   d. A contractor or vendor is no longer involved with a county project or work.

   e. A volunteer ceases to participate in the activity for which he/she volunteered.

   f. An Employee, including a temporary employee, separates from the county.

9. Job Function Change
   The Authorized Representative shall notify Facilities Management when an individual experiences a job function change and access permissions need to change. Any access associated with the badge shall be deactivated immediately upon notification of change. An identification access badge associated with the new job function may be issued.

E. Facilities Management and Business Innovation &Technology Services Responsibilities

1. Facilities Management shall ensure that each Department/Division Director or Elected/Appointed Official has identified an Authorized Representative.

2. Identification access badges will be programmed by Facilities Management to allow only access to facilities and work areas as authorized per the Access Form.

3. Access requests to the Data Center in the Laramie Building, or any room that hosts a county server, data center, or closet, must be approved by the Chief Information Security Officer (CISO); the Business Innovation & Technology representative from that Office or Department; or the designated HIPAA Security Official. During an emergency, the CISO may request that Facilities Management immediately allow access to a specific individual.

4. Access Control System

   a. The Business Innovation &Technology Services Division shall maintain the access control system servers.

b. The Facilities Management Director or designee shall be the application administrator of the access control system.

5. The Facilities Management application administrator shall initiate audits every twelve months to ensure that authorized access is consistent with current job function access requirements. The results of the review, along with any concerns about access, will be forwarded to the CISO and the HIPAA Designated Security and Privacy Officials.

F. Requests for information

1. Records of identification access badge use shall not be released to the public due to security considerations unless otherwise approved by the Sheriff.

2. Records of identification access badge use may be requested and reviewed by county employees for county business purposes, such as by the HIPAA Security Official and the Privacy Official, or by Human Resources, the Authorized Representative, or a supervisor.

3. Badge Access card logs are not intended to be used as a method of tracking the work or productivity of county employees.