California Department of Justice (CADOJ)
California Justice Information Services (CJIS) Division
Security Requirements for Research Organizations, Contractors, External Entities, & Vendors

This document provides information technology (IT) security requirements for ensuring the continued protection of CADOJ Criminal Justice Information (CJI). The following are the standards and security frameworks that are to be met depending on data location.

Requirements:

Requirements			
Data Classification and Service Model	FBI Cloud Controls	FBI CJIS SP	FEDRAMP or SOC 2
CJI using Cloud Services/3rd party data center	X	X	X
Criminal Justice Information (CJI) no Cloud Services/3rd party data center		X	

1. The requirements above can be found at the following:

    a. The FBI cloud controls matrix:
    CJIS Cloud Control Catalog — FBI

    b. FBI CJIS Security Policy – Access to CORI/CJI data requires compliance to the FBI CJIS security policy. CJIS Security Policy Resource Center — FBI
    The FBI Companion document is available at the following site to assist organizations in documenting their compliance to FBI CJIS Security Policy.
    Requirements-Companion-Document_v5-9_20200601.pdf — FBI
    For noncriminal justice agencies see, "Appendix J Noncriminal Justice Agency Supplemental Guidance" within the FBI CJIS Security Policy for additional assistance.

2. As indicated above, use of cloud services and/or 3rd party data center also requires one of the following:
    a. A System and Organization Control (SOC) 2 type I or type II; **or**
    b. A Federal Risk and Authorization Management Program (FedRAMP) Authorization assessed at the moderate or high security baseline. (https://www.fedramp.gov/)

3. This document is to also serve as an addendum to any Memorandum of Understanding (MOU) that is established between CADOJ and approved research center, vendor, external entity or contractor.

California Department of Justice (CADOJ)
California Justice Information Services (CJIS) Division
Security Requirements for Research Organizations, Contractors, External Entities, & Vendors

Background Check:

- In accordance with FBI CJIS Security Policy, a fingerprint background check must be conducted for all individuals and organizations that are requesting receipt and/or storage of CADOJ data, whom have been recognized by CADOJ to be authorized to request and/or store CADOJ data and as a result would have physical and/or logical access to CADOJ data. CADOJ approval is based upon a technical security review, CJIS compliance, and a successful background check. All third party vendors that will be storing CADOJ data in support of the individual and/or organization requesting CADOJ must also complete a fingerprint background check.

I, _____, have completely read and fully understand the
Information Security Officer or IT Manager

information provided in the *CADOJ CJIS Division Security Requirements for Research Organizations, Contractors, External Entities, & Vendors* document. By signing below, I hereby acknowledge that the proper security controls are in place to meet the CADOJ security requirements.

_____ _____

Information Security Officer/ IT Manager Signature Date