California Department of Justice
California Justice Information Services

Data Request
Standard Application

Data Request Packet for
Access to California Department of Justice Data

Table of Contents

Introduction

The Department of Justice (DOJ) provides data access to authorized users. This packet contains important information about the release of DOJ data and the mandatory forms that must be completed before your team can begin receiving data. You must adhere to the Conditions of Release Form pertaining to the dataset that you are interested in requesting. Once the packet has been completed in its entirety, please mail all documentation to:

California Department of Justice
California Justice Information Services Division
Research Center
PO Box 903417, Room G-110
Sacramento, CA 94203-4170

Summary of process:

- Requestor completes the Data Request packet and sends to DOJ.
- DOJ reviews/approves/denies the submitted request.
- If approved, team members must complete a background check.
- DOJ approvals are valid for one-year.
- If project will continue past one-year, requestor will complete the renewal process. For more information on this process, please go to: https://www.oag.ca.gov/research-center.

For questions at any time during this process, you may call the DOJ Research Center's Data Request Unit at (916) 210-3260 or send an email to: researchrequest@doj.ca.gov.

DATA REQUEST PROJECT OUTLINE

Please answer the following questions in the space provided. All information must be typed. You may attach a more detailed project description if you choose.

☐ New Request ☐ Modified Request

Date: _____

Public Agency/Research Body Name: _____

Principle Investigator/Team Lead Name: _____

Address: _____

City: _____ State: _____ ZIP Code: _____

Phone: _____ Email: _____

Information Security Officer/IT Manager Name: _____

Phone: _____ Email: _____

Project Title: _____

Anticipated Completion of Project or Report Date: _____

Data Request Project Outline

Team Member Name	Part of Data Analysis Team? Yes or No	Part of IT* Team? Yes or No

*Information Technology

Data Request Project Outline

Data Request Application Checklist:

- [ ] Project Outline
- [ ] Curriculum Vitae of Team Lead
- [ ] Conditions for Release of DOJ data. Please select the form(s) specific to the dataset(s) requested.
- [ ] Data Security Checklist
- [ ] If applicable, please provide drafts of relevant research materials, such as: Proposals, endorsements, questionnaires, interview schedules, and sample informed consent statements.
- [ ] If applicable, please provide sponsoring agency's Institutional Review Board (IRB) approval.
- [ ] If applicable, for CURES data requests, please provide copies of individual's human subjects research consent form.
- [ ] Certification of Human Subjects Protection Training is required for each authorized staff. If you do not have a current training certificate, please refer to the following link for the required reading material and signature page: https://oag.ca.gov/sites/all/files/agweb/pdfs/Protection-of-Human-Research-Participants.pdf
- [ ] Requests for Personally Identifying Information (PII)
    - [ ] Criminal History Data
    - [ ] Gun Violence Restraining Order Data (GVRO)
    - [ ] Controlled Substance Utilization Review and Evaluation System (CURES)

Data Request Project Outline

Purpose of Project and Project Background

1. Purpose and objectives of the project or report: What issues is the project designed to address? Please clarify and identify how the requested data will be used to support your project. (If you need extra space to answer this question, please attach additional sheets.)

Data Request Project Outline

2. What are the expected benefits of this project? (If you need extra space to answer this question, please attach additional sheets.)

Data Request Project Outline

3. If applicable, what is the funding source? If the funding source is public or private grant, please provide the grant period and its expiration date. (If you need extra space to answer this question, please attach additional sheets.)

Data Request Project Outline

Methodology/Cohort

1. Provide a detailed description of the proposed project design and methodology including but not limited to:
   (If you need extra space to answer this question, please attach additional sheets.)
   - Where will the data analysis be conducted?
   - Please give a detailed description of your cohort.
   - Will you be providing a cohort data file?

Data Request Project Outline

Security Procedures

1. Please detail the security measures your organization has in place to guard against unauthorized access of hard copies or electronic files containing DOJ data, including, but not limited to: (If you need extra space to fill out this question, please attach additional sheets.)

   A. What are the encryption methods?
   B. What is your anti-virus software?
   C. Do you have network security?
   D. Is the location of the data in a secure location (a locked room)?
   E. Are there risks or confidentiality issues related to the storage location?
   F. Will the computer that the data is stored on be connected to the internet?
   G. What kind of software protection does the system have?
   H. Will hard copies of the data be stored?
   I. How will you ensure the elimination of individual identifiers from subject records/publications when the project is completed?

Please Note:

- DOJ does not allow DOJ data to reside on a cloud.
- For security compliance questions, please contact: nisu@doj.ca.gov.

Data Request Project Outline

Security measures continued:

Data Request Project Outline

2. Secure File Transfer Protocol (SFTP) is a network protocol that provides file access, file transfer, and file management over a reliable data stream. DOJ's preferred method of data transfer is through SFTP. Is your organization equipped to transfer data via SFTP?

Data Request Project Outline

Other Formal Project Approvals

1. If applicable, provide information pertaining to other formal project approvals, such as Institutional Review Board (IRB) approvals for the academic community. Provide a copy of all documentation submitted as part of that review and approval process including the application number and expiration date. This document should demonstrate that the IRB is aware of, and has considered, relevant federal and state laws and regulations regarding the use of human subjects in general, and specifically the use of human subjects who are incarcerated, who are minors, or who are otherwise vulnerable populations.

For the Research Center Use Only

☐ Application Approved ☐ Application Denied ☐ Further Information Required

Comments:

Signature: _____ Date: _____

California Department of Justice Data Security Checklist

The public agency or bona fide research body planning to store DOJ data in a computer system is responsible for the integrity and security of the information. Systems or networks containing DOJ data must be segmented from other applications, with controlled and limited access. It is incumbent upon the public agency or bona fide research body to ensure that their system or network remains secure throughout the duration of the research project.

1. Architecture of Criminal Justice Information System (CJIS)

Actively manage (inventory, track, restrict, and correct) all hardware and software so that only authorized assets have access to and can execute on the network.

1.1 Criminal Justice Information Technology (CJIT) associated with processing CORI shall be isolated in a protected network zone (fire-walled network segment), access to CORI shall be restricted to authorized users only, and the zone controls shall be implemented in a manner to prevent secondary dissemination. ☐

1.2 Procedures shall be implemented and followed to control the installation of hardware and software within the protected zone, and an inventory of the zone CJIT shall be maintained. ☐

1.3 Development, testing, and operational zones shall be separated to reduce the risks of of unauthorized access or changes to the operational environment. ☐

2. Secure Configurations of Hardware and Software

Establish, implement, and actively manage the security configuration of laptops, servers, and workstations using a rigorous configuration management and change-control process.

2.1 Organizations shall establish and appropriately protect and validate source code within a secure development environment. ☐

2.2 Testing of security functionality shall be carried out during software development and network architecture and implementation. ☐

2.3 Information systems shall be regularly reviewed and tested for compliance with the organization's information security policies and standards. ☐

3. Continuous Security Evaluations and Malware Defenses

Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and control the installation and spread of malicious code.

3.1 Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk. ☐

3.2 Detection, prevention, and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness. ☐

3.3 All employees of the organization and relevant contractors shall receive appropriate awareness education, training, and regular updates in organizational policies and procedures. ☐

California Department of Justice Data Security Checklist *(continued)*

4. Controlled Use of Administrative Privileges

The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications. ☐

4.1 User provisioning and the allocation and use of privileged access rights shall be restricted and controlled. Asset owners shall review users' access rights at regular intervals and adjust as required. ☐

4.2 The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled

5. Maintenance, Monitoring, and Analysis of Audit Logs

Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack. ☐

5.1 Event logs recording user activities, exceptions, faults, and information security events shall be produced and kept, protected from alteration, and regularly reviewed.

6. Data Protection

The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information. ☐

6.1 A policy on the use of cryptographic controls and key management shall be developed and implemented. ☐

6.2 Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.

7. Incident Response and Management

Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure to quickly discover an attack and to effectively contain the damage. ☐

7.1 Information security events shall be reported through appropriate management channels as quickly as possible, assessed, and decided if they are to be classified as information security incidents. ☐

7.2 The organization shall define and apply procedures for the identification, collection, acquisition, and preservation of information that can serve as evidence.

Signature of Information Security Officer/IT Manager	Date
Printed Name	Position
Name of Public Agency/Research Organization	