DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER CONFIDENTIALITY AND NON-DISCLOSURE (CND) AGREEMENT

Company or Organization: _____

Researcher's Full Legal Name: _____

Researcher's Phone Number: _____

Researchers must complete all sections. The DOJRC will not process this CND Agreement with blank areas. Please attach supporting documentation if necessary.

The DOJ collects, stores, and disseminates confidential and sensitive information from the law enforcement community and the public to administer the various programs for which it has responsibility. This information is maintained according to provisions of various laws and regulations including the Information Practices Act, the Public Records Act, the State Administrative Manual, and in reference to associated DOJ information technology (IT) security policies. The DOJ prohibits unauthorized access, use, or disclosure of DOJ information or systems.

The following agreement has been established to address the confidentiality of DOJ data including but not limited to the California Law Enforcement Telecommunications System, California Justice Information Systems, law enforcement agency, and other DOJ data.

1. A researcher may access DOJ data when authorized by the DOJRC to fulfill research related work. Researchers may only disclose or release DOJ data to individuals that the DOJRC has authorized to receive it. Researchers may not access or use information from the DOJ network, information systems, applications, or from any databases accessible through the DOJ network, for any purpose not related to the research related work. Such use may be subject to administrative, civil, or criminal penalties.

_____ (initial here)

2. Researchers are prohibited from modifying, deleting, or destroying existing DOJ data, except as required in paragraph 4 after the conclusion of the research. _____ (initial here)

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC) RESEARCHER
CONFIDENTIALITY AND NON-DISCLOSURE (CND) AGREEMENT

3. Researchers must take precautions to protect DOJ data. Precautions include, but are not limited to, the following:

a. DOJ requires all researchers to utilize their associated organizations' IT hardware and equipment while working onsite or offsite and when accessing sensitive or confidential data including but not limited to personally identifiable information, Health Insurance Portability and Accountability Act, and DOJ data. _____ (initial here)
b. The researcher must ensure that their organizations desktop or laptop that is used to review or access DOJ data is locked at all times when left unattended. _____ (initial here)
c. Saving files on a researcher's desktop or laptop for file-sharing such as, peer-to-peer, Google drive, Dropbox, etc., or on USB drives, CD-ROMs or in a cloud environment is strictly prohibited. Storing DOJ data on the laptop is prohibited. _____ (initial here)
d. The researcher ~~**should**~~**must** immediately notify their organization's Information Security Officer**,** who~~**m, the DOJRC should**~~**must** immediately contact the DOJ's Information Security Office**,** of any security incidents involving data or any incident regarding breaches of data.

_____ (initial here)

4. Upon conclusion of the authorized research work, the researcher will provide the DOJRC with proof of destruction of all DOJ data. Destruction of DOJ data must comply with the National Institute of Standards and Technology (NIST) Special Publication 800-88, Revision 1, Guidelines for Media Sanitation (December 2014) which is incorporated by reference. _____ (initial here)

I acknowledge that I have read and understood the information provided herein, and received a copy of the DOJRC Researcher CND Agreement. I understand that failure to comply with this agreement, and the applicable California laws and regulations governing the use and disclosure of the DOJ data, may result in administrative, civil, or criminal penalties under applicable California laws and regulations.

_____ (initial here)