DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

Researcher Name:		Phone Number:	
		Email Address:	
Information Security Officer (ISO) ***or*** Information Technology (IT) Manager/Official's Name:		Phone Number:	
		Email Address:	
Organization Name:		Office/Branch:	
		Address:	
Organization Leader Name:		City, State, and Zip:	

The following agreement has been established to address conditions when a researcher is authorized to establish a remote access connection to their organization's network to access DOJ data remotely using a personally-owned or organization-issued IT device/equipment. The researcher and their supervisor/manager and/or organization leadership are to acknowledge that they have read, understood, and agree to adhere to the requirements in this agreement.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

Security precautions must be taken when accessing DOJ data remotely. The minimum security precautions include the following:

- Researchers who are accessing DOJ data located at their research organization must use Virtual Private Network encryption while remote. DOJ data must not be copied to a mobile device.
- Researchers must ensure that a host firewall is turned on at all times.
- DOJ data shall not be copied, duplicated, transferred, printed, or otherwise manipulated through the researcher's personal printing devices due to possible loss of control, and the unintentional storage of DOJ data.
- Researchers shall ensure that manufacturer-recommended security updates and configuration changes are applied regularly to the software on their personally-owned or organization-issued IT device/equipment that relate to security updates to fix vulnerabilities. Researchers shall ensure these updates are applied the software in the required timeframe specified by the vendor if it is used to remotely connect to their organization to access DOJ data.
- If an IT device/equipment from the researcher's organization is used to remotely connect to the researcher's organization to access DOJ data, the IT device/equipment must have all current security patches updated and have malware protections enabled.

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

The following is a checklist of the security controls or configurations that must be put in place if a researcher is accessing DOJ data from a personally-owned or organization-issued IT device/ equipment. Check each box to confirm compliance with the previously listed minimum security requirements.	
Ensure the firewall software included with the computer is turned on and set to block all incoming connections from other computers, outside sources on the Internet, and sources that have not been approved or permitted.	**I (we) confirm compliance:** ☐
Disable non-essential services, such as file and print sharing.	**I (we) confirm compliance:** ☐
Disable unnecessary networking features such as wireless network access features (e.g., IEEE 802.11a/b/ g/n, Bluetooth, and infrared).	**I (we) confirm compliance:** ☐
Configure the personally-owned or organization-issued IT device/equipment so that they do not automatically attempt to join detected wireless networks.	**I (we) confirm compliance:** ☐
Antivirus and antispyware software (software that detects and blocks malicious code).	**I (we) confirm compliance:** ☐ **Please identify what antivirus or antispyware is being used if it applies (e.g. Norton Anti-virus, McAfee, TotalAv, etc.):**
Remote access users shall review manufacturer documentation for each software program their personally-owned or organization-issued IT device/ equipment contains in these categories to determine each program's update capabilities and enable automatic updates where possible.	**I (we) confirm compliance:** ☐
Web browser settings are securely configured, which requires, at a minimum, to keep the browser up to date, to block third party cookies, to block pop-ups, and to disable features that might cause vulnerabilities.	**I (we) confirm compliance:** ☐

DEPARTMENT OF JUSTICE (DOJ)
RESEARCH CENTER (DOJRC)
RESEARCHER DATA ACCESS USER AGREEMENT

I (We) have read, understood, and acknowledge the DOJRC Researcher Data Access User Agreement. I (We) agree to comply with the agreement terms of the security controls that need to be put in place on my (our) personally-owned or organization-issued IT device/equipment before accessing DOJ data. If I am (we are) unable to comply with all the security requirements, a DOJRC Security Variance Form for Data Access Non-Compliance of Security Requirements form will be completed and submitted to DataRequests@doj.ca.gov to identify the security controls with which I am (we are) not in compliance and I (we) will identify a mitigation plan that will be used to minimize or compensate for the associated risk(s).

Employee Signature:		Date:	
ISO/IT Manager/ Official Signature:		Date:	
Organizational Leader Signature:		Date:	