NATIONAL DATA ARCHIVE ON CHILD ABUSE AND NEGLECT

Application for Obtaining Restricted Data from NDACAN

This document is incorporated by reference into the "Data Use License Agreement for Restricted Data Provided by NDACAN" (hereafter "License") which has been signed by the Investigator and the Representative of the Investigator's Institution. NDACAN will review the security of the Investigator's computing environment described in this document and issue its approval.

INSTRUCTIONS:
This form is intended to be filled out digitally. Please provide the following information, then rename this file with your last name, first initial, the short name of the Restricted Dataset and the word 'Application.' Example: "Doe, J. NCANDS Application.pdf" Email it to NDACAN@cornell.edu.

NDACAN Review (Office Use Only)

Reviewer Comments:

NDACAN Co-Director Approval Signature and Date:

Restricted Dataset Number, Title, and Years Being Requested (e.g., NCANDS Child File 2010-2019):

I. Investigator Information

The Investigator serves as the primary point of contact for all communications involving the License. The Investigator must hold a faculty appointment or non-student research position at the Investigator's Institution and assumes responsibility for compliance with all terms of the License by employees of the Investigator's Institution, including the day-to-day security of the Restricted Data electronic data files and printed output derived from the files.

Investigator Name: _____
Investigator Title: _____
Investigator Institution: _____
Investigator Department: _____
Investigator Office and Address: _____
Investigator Email: _____
Investigator Phone Number: _____

The Investigator must also provide complete contact information via the form at the following link, please do so now:
https://www.ndacan.acf.hhs.gov/about/about-join-our-mailing-list.cfm

II. Investigator's Use of the Restricted Data

1. For what purposes are you applying for the Restricted Data? Describe your research objectives, analytical approach, and the reason(s) you are requesting these data:

2. Describe all the ways the results of your research will be used, including plans for public dissemination:

3. All linking or merging of files must be pre-approved in writing by NDACAN.

Do you propose to link or merge the Restricted Data with other data files, including other years of the same series (e.g., NCANDS Child File)?

Yes: ☐ **No:** ☐

If "Yes," provide the names, descriptions, and sources of these other files. Also, describe how the linking will be accomplished and explain why it is necessary to achieve your research objectives:

III. Registration Status of the Investigator's Institution's Institutional Review Board (IRB)

The Investigator's Institution must be an institution of higher education, research organization, or government agency that is registered with the U.S. Office for Human Research Protections (OHRP), or can demonstrate a record of using sensitive data according to commonly-accepted standards of research ethics. The Investigator must obtain and submit an IRB notice to NDACAN before receiving the Restricted Data. If the Investigator's Institution has no IRB, then the Investigator must use an external IRB (sometimes called a commercial IRB) to review the Investigator's project and issue a notice of compliance with human subjects research requirements.

Does the Investigator's Institution have an Institutional Review Board that is registered with the U.S. Office for Human Research Protections (OHRP)?

Yes: ☐ **No:** ☐

If "Yes," what is the IRB number listed at the OHRP database for registered IRBs? IRB: _____

IV. Research Staff Listing

Research Staff are individuals who are affiliated with the Investigator's Institution and with whom the Investigator is collaborating, and therefore need authorized to access the data. Research Staff must understand the conditions of the License and sign and submit a Research Staff Form (separate document) to be approved by NDACAN. In the spaces below, provide the requested information for all individuals, excluding the Investigator, who need authorized access to the Restricted Data. If additional space is required, provide the information on a separate page.

Research Staff Person 1 Name: _____

Research Staff Person 1 Title: _____

Research Staff Person 1 Institution: _____

Research Staff Person 1 Email: _____

Research Staff Person 2 Name: _____
Research Staff Person 2 Title: _____
Research Staff Person 2 Institution: _____
Research Staff Person 2 Email: _____

Research Staff Person 3 Name: _____
Research Staff Person 3 Title: _____
Research Staff Person 3 Institution: _____
Research Staff Person 3 Email: _____

Research Staff Person 4 Name: _____
Research Staff Person 4 Title: _____
Research Staff Person 4 Institution: _____
Research Staff Person 4 Email: _____

Research Staff Person 5 Name: _____
Research Staff Person 5 Title: _____
Research Staff Person 5 Institution: _____
Research Staff Person 5 Email: _____

Research Staff Person 6 Name: _____
Research Staff Person 6 Title: _____
Research Staff Person 6 Institution: _____
Research Staff Person 6 Email: _____

VI. Data Security

To ensure the confidentiality of the individuals in the Restricted Data, NDACAN requires that electronic security provisions are taken to protect the confidential data and any derived output from access by unauthorized individuals.

Servers: The Restricted Data may be stored on a network server located on the premises of the Investigator's Institution, or on a cloud service provider (CSP) that is FedRAMP Authorized. If you will be using a FedRAMP Authorized CSP to store the Restricted Data, then in the space provided please supply information and a link to the FedRAMP Authorized CSP that is deployed at your institution.

Personal computers: The Restricted Data may be installed on one personal desktop computer per authorized user. For example, if a workplace office computer stores the Restricted Data, then a home computer cannot have those data installed and must remote access the office computer using a VPN. The desktop computer which stores the restricted data must be secured in a private locked office.

Laptops or other devices: Laptops are not approved to store data. Laptops will only be approved as access devices to the restricted data stored on a secure server or on a secure desktop at an office (via remote desktop). NDACAN will review other devices on a case-by-case basis as technology develops, but the use of external hard drives to store the Restricted Data may not be approved.

In Table 1, provide a comprehensive list of all devices on which the Restricted Data will be installed, all devices that will access the Restricted Data, and indicate the electronic security measures that will be applied to each device. This includes back-up copies of the Restricted Data. If additional space is required, continue the list on a separate page. For devices connected to the Internet, all four of the electronic security measures (i.e., Password Login, Restricted Directory Access, Virus Protection, and Firewall Protection) must be in place for this application to be approved. Note: An 'access' machine means a person will sit at that machine to use the data that is either stored on that same machine (if also marked as 'storage'), to log into a different machine (e.g. a server or a secured workstation) that is marked as 'storage', or to log into a FedRAMP authorized cloud service provider.

In addition to electronic security measures, the devices on which the data are stored must be physically secured to prevent theft of the device. In the pages below, describe the physical security measures that are in place for each device. Examples of such protection include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. **The physical security systems for each device must be checked regularly. Applications that are deemed to have inadequate physical security measures in place will be denied. In particular, work spaces that are shared with or accessible by people who are not authorized Research Staff are not acceptable.**

Table 1: Inventory of All Devices Used for Storage or Access

ID	**Device Type:** Enter 'desktop', 'laptop', 'server', 'portable media', or describe other device	**Internet Enabled:** Check the box if the device has access to the Internet	**Storage or Access:** Check the box to indicate if the data will be stored on the device, and/or if it will also access the data stored elsewhere.	**Password Login:** Check the box if the device requires a login ID and password at startup and after a period of inactivity	**Restricted Directory Access:** Check the box if the directories containing the data are restricted to authorized users who have logged in to the device	**Virus Protection:** Check the box if anti-virus software is installed on the device	**Firewall Protection:** Check the box if firewall technology is in place for devices that are connected to the Internet
1		☐	Storage ☐ Access ☐	☐	☐	☐	☐
2		☐	Storage ☐ Access ☐	☐	☐	☐	☐
3		☐	Storage ☐ Access ☐	☐	☐	☐	☐
4		☐	Storage ☐ Access ☐	☐	☐	☐	☐

Cloud Service Provider (enter N/A if you are not using a CSP)

Full Name and URL	**FedRAMP Authorized**
	Yes ☐ **No** ☐

Device ID1: Details and Location

ID	Device Details: Enter the make, model, and operating system.	Device Location and User Name: Enter the street address, building name, and office number. Enter the name of the person using the device.	Declaration of Private Workspace: This workspace is used only by you or, if shared, then shared only with Research Staff on your team. Check the box. [Note: Workspaces shared with non-Research Staff persons will result in a rejected Application.]
1			**Yes** ☐ **N/A (Server)** ☐

Device ID1: Description of Physical Security

Describe the physical security of the device. Examples include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. External storage devices or media must be encrypted (*describe encryption method*) and its location & security regularly verified (*describe schedule*).

Device ID2: Details and Location

ID	Device Details: Enter the make, model, and operating system.	Device Location and User Name: Enter the street address, building name, and office number. Enter the name of the person using the device.	Declaration of Private Workspace: This workspace is used only by you or, if shared, then shared only with Research Staff on your team. Check the box. [Note: Workspaces shared with non-Research Staff persons will result in a rejected Application.]
2			**Yes** ☐ **N/A (Server)** ☐

Device ID2: Description of Physical Security

Describe the physical security of the device. Examples include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. External storage devices or media must be encrypted (*describe encryption method*) and its location & security regularly verified (*describe schedule*).

Device ID3: Details and Location

ID	Device Details: Enter the make, model, and operating system.	Device Location and User Name: Enter the street address, building name, and office number. Enter the name of the person using the device.	Declaration of Private Workspace: This workspace is used only by you or, if shared, then shared only with Research Staff on your team. Check the box. [Note: Workspaces shared with non-Research Staff persons will result in a rejected Application.]
3			**Yes** ☐ **N/A (Server)** ☐

Device ID3: Description of Physical Security

Describe the physical security of the device. Examples include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. External storage devices or media must be encrypted (*describe encryption method*) and its location & security regularly verified (*describe schedule*).

Device ID4: Details and Location

ID	**Device Details:** Enter the make, model, and operating system.	**Device Location and User Name:** Enter the street address, building name, and office number. Enter the name of the person using the device.	**Declaration of Private Workspace:** This workspace is used only by you or, if shared, then shared only with Research Staff on your team. Check the box. [Note: Workspaces shared with non-Research Staff persons will result in a rejected Application.]
4			**Yes** ☐ **N/A (Server)** ☐

Device ID4: Description of Physical Security

Describe the physical security of the device. Examples include offices that are locked when unoccupied, storage in secure cabinets when the device is not in use, and monitored access to the building where the device is housed. External storage devices or media must be encrypted (*describe encryption method*) and its location & security regularly verified (*describe schedule*).

Describe any other information relevant to the electronic or physical security of the Restricted Data: