Application and Data Protection Plan: NSCAW Restricted

National Data Archive on Child Abuse and Neglect (NDACAN)

FOR NDACAN OFFICE USE ONLY

NDACAN Review: ☐ Approved ☐ Revise and Resubmit

NDACAN Review Date: _____

NDACAN Reviewer Comments (optional): _____

INSTRUCTIONS:

Please provide the following information. When finished, save, close and rename this PDF with your Last name, First initial, and the text "NSCAW App-DPP". Example: "Doe, J. NSCAW App-DPP.pdf".

I. INVESTIGATOR

1. 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, 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 Email _____
Investigator Phone Number _____

2. Are you currently employed by a state child welfare agency? ☐ No ☐ Yes
3. The Investigator must also provide complete contact information via the following link -please do so now: https://www.ndacan.cornell.edu/about/about-join-our-mailing-list.cfm

II. INVESTIGATOR'S USE OF THE NSCAW RESTRICTED DATA

1. Describe your research purpose and analysis plan for using the NSCAW Restricted Data.

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

3. Do you propose to link or merge the dataset with other data files? All linking or merging of files must be pre-approved in writing by NDACAN. Note that linking to other data files is prohibited for some Restricted Data collections at NDACAN, and will therefore not be approved.

☐ No ☐ Yes

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

1. The Investigator's Institution must be an institution of higher education, research organization, orgovernment agency that employs the Investigator. The institution must be registered with the U.S. Office for Human Research Protections. If the institution is not registered, NDACAN may use the information in section III.2 to grant an exemption to institutions with a demonstrated record of using sensitive data according to commonly-accepted standards of research ethics.

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_____

2. If your Institution does not have an IRB assurance number, you must answer the following questions. Skip this section if you responded "Yes" to the previous question.

a. Describe your Institution in detail. What kind of work does it do? Include the type of organization, its profit/non-profit status, and primary sources of revenue:

b. What experience does the Institution have in overseeing the use of sensitive research data by its staff? Please give specific examples:

c. Does your employer have policies regarding scientific integrity and misconduct, or human subjects research that cover the secondary analysis of survey data? ☐ Yes ☐ No

Important: If Yes, submit a copy of these policies with your application.

IV. DATA PROTECTION PLAN

To ensure the confidentiality of the individuals in the NSCAW Restricted Data, NDACAN requires that security measures be in place to protect the data from loss, theft, and unauthorized access. In this form, describe the data protection plan in detail. Methods for protection will vary among Investigators depending on available technology and personnel, but it is necessary that sufficient measures are put in place. The NSCAW Restricted Data will not be distributed to the Investigator until this Application and Data Protection plan has been approved by NDACAN. Successful data protection plans will include a layered approach that provides multiple security controls with each of the following domains addressed:

- **Physical security.** Physical media upon which the Restricted Data and its derivatives are stored should be physically unavailable to unauthorized users. An example of excellent physical security is a private, locked office on a university campus with a locked filing cabinet for storing an encrypted exernal hard drive or printed detailed statistical output, and a computer that is physically secured to the work surface with a cable lock to prevent theft.
- **Electronic security.** Computing resources used for storing or accessing the Restricted Data should be protected from malware, viruses, and network intrusion. An example of excellent electronic security is a stand-alone computer running anti-virus and anti-malware software that is only periodically connected to a network for essential software updates.
- **Access control.** Access to the Restricted Data must be limited to authorized users. At least two different forms of user authentication should be provided for access. Forms of authentication include the following:
  - something one knows, such as a strong password
  - something one possesses, such as an office key, a smartcard, or a cell phone
  - something that is inherent to the user, such as a fingerprint.
- **Administrative security.** If additional Research Staff are needed for the project, the Investigator should employ trustworthy individuals who meet the licensing requirements. All Research Staff should be made aware of the Data Protection Plan requirements and be trained in how to follow the security procedures.

1. Who will be responsible for the day-to-day security of the Restricted Data?

Name _____

Email _____

2. If backup copies of the Restricted Data are made on external hard drives, discs, or other media, where will they be stored and who will have access? Please specify the building name and room number, describe where in the office the media will be secured, and list all individuals who will have access.

3. Electronic security

Approved plans ideally include workstations with anti-virus, anti-malware, and firewall software that are not connected to the Internet (except for essential software updates). Plans involving internet-connected computers or network servers are acceptable if they are adequately protected. Use of whole disk or partition encryption is encouraged, especially if it is necessary for the Restricted Data to be installed on a laptop computer.

Complete an inventory of all the devices which will store or access the NSCAW Restricted Data. The inventory should include computers, network servers, and external hard drives on which the data are installed, and all computers which don't have the data stored locally but are used for accessing the data over a secure connection.

Inventory of All Devices Used for Storage or Access

ID	Device Description	Storage Device or Access Device?	If Storage Device: Uses Drive Encryption? (Recommended)	If Access Device: Uses Secure Network Connection? (Required)
	e.g., "JD Office Computer The data will be stored on the hard drive of a Dell OptiPlex 990 running Windows 7."	*e.g.,* ☒ *Storage Device* ☐ *Access Device*	*e.g.,* ☒	*e.g.,* ☒
1		☐ Storage Device ☐ Access Device	☐	☐
2		☐ Storage Device ☐ Access Device	☐	☐
3		☐ Storage Device ☐ Access Device	☐	☐
4		☐ Storage Device ☐ Access Device	☐	☐
5		☐ Storage Device ☐ Access Device	☐	☐

4. Physical security

Describe the security arrangements for all the offices and buildings where copies of the Restricted Data will be stored. How will the storage devices be protected from theft, loss, and unauthorized physical access? Approved plans typically include workstations that are secured on the premises of the Investigator's institution in buildings with key card access and private locked offices.

ID	Location of the Device Indicate building name and office number where the device is located	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
1		
2		
3		
4		
5		

From the Inventory of All Devices table, list the all the **storage devices** in the table below and indicate the storage device type, Internet connection status, and electronic security features.

Additional Detail for Storage Devices

ID	Storage Device Type: Indicate workstation, laptop, server, portable media, or other device	Internet Enabled? Check the box if the device has access to the Internet	Password Login: The device requires a login ID and password at startup and after a period of inactivity	Restricted Directory Access: The directories containing the data are restricted to authorized users who have logged in to the device	Virus Protection: Anti-virus software is installed on the device	Firewall Protection: Firewall technology is in place for devices that are connected to the Internet
1		☐	☐	☐	☐	☐
2		☐	☐	☐	☐	☐
3		☐	☐	☐	☐	☐
4		☐	☐	☐	☐	☐
5		☐	☐	☐	☐	☐

5. Access control

Approved plans typically include possession of a key or key card to access the office where the Restricted Data are located and the use of user names and strong passwords at computer login and after a 10-15 minute period of inactivity. Strong passwords are defined as user-specific passwords that are used exclusively for accessing the Restricted Data, contain at least 9 characters, and include upper case, lower case, numeric, and special characters. Two factor authentication is the ideal scenario for controlling access. For two factor authentication, authorized users must provide two of the following three forms of identification: (1) something that is known, like a password, (2) something that is possessed, like a key, or (3) something that is inherent to the user, like a fingerprint. A stated policy of using disk-wiping software is also encouraged.

Describe how access to the NSCAW Restricted Data files will be limited to authorized users. Which forms of authentication will be used? When will authentication be required, e.g. at computer login and after a brief period of inactivity? If passwords will be used, what is the policy about how complex they need to be and how often they have to be changed? Are there policies in place to use disk-wiping software when storage devices are being retired?:

6. Administrative security

In addition to providing physical and electronic security for the Restricted Data, administrative or personnel security is also necessary. Approved plans typically include as few authorized users as possible, a stated policy of de-activating users immediately upon leaving the research team, and designation of an individual who is responsible for training and maintaining awareness about the data protection requirements and monitoring day-to-day compliance.

Describe how the Investigator will assure that all authorized users understand the importance of protecting the Restricted Data, that they are familiar with the data protection requirements, and that they are putting the security procedures into practice? How will Research Staff be trained and reminded about the requirements and how will compliance be monitored?: