Security Plan Form

Institute of Education Sciences (IES)
Restricted-use Data

Name of Institution / Organization: _____

PPO Name: _____

PPO Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

PPO Phone Number: _____

Type of Security Plan: New ☐ Renewal ☐ Modification ☐

License Number: _____

Physical Location of Data

Project Office Address:
(no P.O. Box number; specify building name, department, and room number)

(Provide street address, city, state, zip code, department and building name, and office/room number.)

Project Office Phone Number: _____

Note: *The restricted-use data and computer must be secured and used **only** at this location. When the data are not being used, the data must be stored under lock and key at this location. Only authorized users of the data, as listed on the License, may have key access to this secure project office/room.*

Physical Security of Data

Describe Building Security:
(Describe building security arrangements where project office is located.)

Describe Project Office Security:
(Describe project office security arrangements for the room where the computer and data will be located.)

Computer Security Requirements

Describe Computer System:
(*Please read the **Note** below. Computer security must follow the requirements listed below.)*

Computer Operating System: _____

Anti-Virus Software Installed on Computer: _____

Note: *The restricted-use data must be copied to and run on a standalone, desktop computer.* ***Use of a laptop computer, external hard drive, or USB memory stick is strictly prohibited.*** *Absolutely no restricted-use data may be copied onto a server or computer that is attached to a modem or network (LAN) connection. Prior to attaching the computer to a modem or LAN connection, the restricted-use data must be purged and overwritten on the computer.*

The following physical location and computer security procedures must be implemented when in possession of restricted-use data. By checking the box next to each security procedure, you signify that these security procedures will be implemented for the duration of the project and License period:

- Only authorized users listed on the License will have access to the secure room. Access will be limited to the secure room/project office by locking the office when away from the office. ☐
- Data will only be secured, accessed and used within the secure project office/room (as specified on page 1 of this plan). ☐
- A password will be required as part of the computer login process. ☐
- The password for computer access will be unique and contain 6 to 8 characters with at least one non-alphanumeric character. ☐

- The computer password will change at least every 3 months or when project staff leave. ☐
- Read-only access will be initiated for the original data. ☐
- An automatic password protected screensaver will enable after 5 minutes of inactivity. ☐
- No routine backups of the restricted-use data will be made. ☐
- Project office room keys will be returned and computer login will be disable within 24 hours after any user leaves the project. The PPO will notify IES of staff changes. ☐
- Restricted-use data will **not** be placed on a server (network), laptop computer, USB memory stick, or external hard drive. ☐
- The data will be removed from the project computer and overwritten, whether at the end of the project or when reattaching a modem or LAN connection. ☐
- Post Warning notification: During the computer log-in process, a warning statement (shown below) will appear on the computer screen before access is granted. If it is not possible to have the warning appear on the screen, it must be typed and attached to the computer monitor in a prominent location. ☐

W A R N I N G

U.S. Government Restricted-use Data

Unauthorized Access to Data (Individually Identifiable Information) on this Computer is a Violation of Federal Law and will Result in Prosecution.

Do You Wish to Continue? (Y)es or (N)o

N O T I C E

Proposed Publications Using Restricted-use Data

Sample Surveys and Evaluations

Licensees are required to round all unweighted sample size numbers to the nearest ten (nearest 50 for the Early Childhood Longitudinal Study Birth Cohort) in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on or use restricted-use to the IES Data Security Office to provide feedback on uses of ESRA data.

Administrative Record/Universe Data

Licensees are required to follow the disclosure avoidance procedures transmitted with the restricted-use data in all information products (i.e., proposals, presentations, papers or other documents that are based on or use restricted-use data). Licensees are required to provide a draft copy of each information product that is based on or uses restricted-use data to the IES Data Security Office for a disclosure review. In the case of information products that are based on or use FERPA-protected restricted-use data, the IES Data Security Office will also review the product to determine if, consistent with the approved project proposal, the Licensee used the data to conduct a study to improve instruction or as an "authorized representative of the Secretary" to evaluate a Federally supported education program. The Licensee must not release the information product to any person not authorized to access the data you are using until formally notified by IES that no potential disclosures were found and, if applicable, that no FERPA issues were identified. This review process usually takes 3 to 5 business days.

The PPO shall also forward a final copy of any public presentations or reports published or released that are based on, or use FERPA-protected restricted-use data to the IES Data Security Office.

Signature Page – Management Review and Approval

I have reviewed the requirements of the License agreement and the security procedures in this plan that describe the required protection procedures for securing, accessing and using the restricted-use data.

I hereby certify that the computer system, physical location security procedures, and access procedures meet all of the License requirements and will be implemented for the duration of the project and License period.

Senior Official Signature	Date
Senior Official Name & Title (print)	Phone Number
Principal Project Officer Signature	Date
Principal Project Officer Name & Title (print)	Phone Number
System Security Officer Signature	Date
System Security Officer Name & Title (print)	Phone Number

Note: The National Center for Education Statistics (NCES) processes licenses and disseminates restricted-use data for all centers in the Institute of Education Sciences (IES) including the National Center for Education Research (NCER), the National Center for Education Statistics (NCES), the National Center for Education Evaluation (NCEE), and the National Center for Special Education Research (NCSER).