

Restricted-Use Data Procedures Manual

**U.S. Department of Education
Institute of Education Sciences
National Center for Education Statistics
IES Data Security Office**

**550 12th Street, SW
Washington, DC 20202**

Publication Information

U.S. Department of Education

Arne Duncan
Secretary

Institute of Education Sciences

John Q. Easton
Director

National Center for Education Statistics

Jack Buckley
Commissioner

The National Center for Education Statistics (NCES) is the primary federal entity for collecting, analyzing, and reporting data related to education in the United States and other nations. It fulfills a congressional mandate to collect, collate, analyze, and report full and complete statistics on the condition of education in the United States; conduct and publish reports and specialized analyses of the meaning and significance of such statistics; assist state and local education agencies in improving their statistical systems; and review and report on education activities in foreign countries.

NCES activities are designed to address high priority education data needs; provide consistent, reliable, complete, and accurate indicators of education status and trends; and report timely, useful, and high quality data to the U.S. Department of Education, the Congress, the states, other education policymakers, practitioners, data users, and the general public.

We strive to make our products available in a variety of formats and in language that is appropriate to a variety of audiences. You, as our customer, are the best judge of our success in communicating information effectively. If you have any comments or suggestions about this or any other NCES product or report, we would like to hear from you. Please direct your comments to:

National Center for Education Statistics
Institute of Education Sciences
U.S. Department of Education
550 12th Street, SW
Washington, D.C. 20202

The NCES Home Page is: <http://nces.ed.gov>

Printed April 1996 (NCES publication number: 96860rev)
Reprinted October 1999
Acrobat PDF Version August 2011

Content Contact: IESData.Security@ed.gov

Restricted-Use Data Procedures Manual

This manual will be provided to organizations interested in obtaining restricted-use data, and to licensed organizations who currently have access to restricted-use data.

The goal is to maximize the use of statistical information, while protecting individually identifiable information from disclosure. The *Restricted-Use Data Procedures Manual* was created to provide a guide to the restricted-use data application process, as well as to explain the laws and regulations governing these data.

We hope that this manual answers any questions or concerns you may have regarding obtaining access to restricted-use data.

IMPORTANT

- This manual serves as a procedures guide, but it does not replace the provisions of the actual License document and the required security procedures.
- The licensee is responsible for all terms and provisions within the License and the required security procedures.
- Under no circumstances may the database be removed or telecommunicated from the licensee's site.
- Licensees are subject to unannounced, unscheduled inspections to assess compliance with security requirements.
- Violations of the Education Sciences Reform Act confidentiality provisions incorporated in the License document are subject to a class E felony and can be imprisoned up to five years, and/or fined up to \$250,000.

Table of Contents

	Page
Introduction	7
Restricted-Use Data	7
Public-Use Data	7
Overview of Laws	7
Licensing Procedures	7
Security Procedures	8
On-Site Inspections	8
Laws	9
1.1 Basic Statutes	9
1.2 Privacy Act of 1974	9
Privacy Standards	9
Computer Security Guideline	9
1.3 E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA)	9
1.4 Education Sciences Reform Act of 2002	10
Confidentiality Standards	10
Violations	10
1.5 USA Patriot Act of 2001	10
1.6 E-Government Act of 2002	11
Licensing Procedures	12
2.1 What Data Are Licensed	12
Only Restricted-Use Data Are Licensed	12
Available Restricted-Use Databases	12
2.2 What is a License?	12
Memorandum of Understanding	12
License	12
Contracts	13
Content of License Documents	13
2.3 Who Needs a License Document	13
Matching Organizations to License Documents	13
Restricted-Use Data and IES Staff	14
Pre-test Monitoring	14
Contractors	14
2.4 Applying for a License	15
Summary of Procedures	15
Formal Request	15
License Document	17
Affidavits of Nondisclosure	17
Security Plan Form	18
Receiving the Requested Materials	18

	Page	
2.5	Required Licensee Activity	19
	Maintaining the License File	19
	Submitting Research Publications	20
	Passing On-Site Inspections	20
	Outside Requests for Data	20
2.6	Amending a License	21
	Add User Amendment	21
	Delete User Amendment	22
	Add Database Amendment	22
	Modify Security Plan Amendment	23
	Extend License Amendment	23
	Close-Out License Amendment	24
2.7	Applicant/Licensee Record	25
	Security Procedures	28
3.1	Introduction	28
	Basic Statutes	28
	IES Statutes	28
	Other Statutes	28
3.2	Risk Management	29
3.3	General Security Requirements	29
	Assign Security Responsibilities	29
	Complete Security Plan Form	30
	Restrict Access to Data	30
	Use Data at Licensed Site Only	30
	Respond to Outside Request for Subject Data	31
	Return Original Data to IES	31
3.4	Physical Handling, Storage, and Transportation	31
	Protect Machine-Readable Media and Printed Material	31
	Avoid Disclosure from Printed Material	31
	Edit for Disclosures	32
	Only One Backup Copy	32
	Limit Transporting of Data	32
3.5	Computer Security Requirements	32
	Standalone Computer	33
	Limit Room/Area Access	33
	Standalone Desktop Computer Security Model	33
	Passwords	33
	Notification (Warning Screen)	34
	Read-only Access	34
	No Connections to Another Computer	34
	Lock Computer and/or Room	35
	Automatic Shutdown of Inactive Computer	35
	Do Not Backup Restricted-Use Data	35

	Staff Changes	35
	Overwrite Hard Disk Data	35
3.6	License User Training	36
On-site Inspections		37
4.1	On-Site Inspection Procedures	37
	License Procedures	37
	Security Procedures and Security Plan Form	37
4.2	On-Site Inspection Guideline	38
4.3	Violations, Penalties, and Prosecution	38
	Violations	38
	List of Most Common Violations	39
	Prosecution and Penalties	39

		Page
Appendices		
Appendix A	Definition of Terms	40
Appendix B	Public-Use Data	43
Appendix C	Privacy Act of 1974	44
Appendix D	IES-Specific Laws	45
Appendix E	Memorandum of Understanding	48
Appendix F	License Document	49
Appendix G	Affidavit of Nondisclosure	50
Appendix H	Restricted-Use Databases	51
Appendix I	Availability of Restricted-Use Data	52
Appendix J	Security Plan Form	53
Appendix K	On-Site Inspection Guideline	54
Appendix L	E-Government Act of 2002, Title V, Subtitle A, Confidential Information Protection	55
Appendix M	Close-out Certification Form	56

Introduction

Restricted-Use Data

The Institute of Education Sciences (IES) collects survey and research data containing individually identifiable information, which is confidential and protected by federal law.

IES uses the term "restricted-use data" for such information. The terms "restricted-use data" and "subject data" are synonymous. (See Appendix A, Definition of Terms.)

Public-Use Data

IES uses the term "public-use data" for survey data when the individually identifiable information has been coded or deleted to protect the confidentiality of survey respondents. Access to public-use data does not require a license, for these data are available to the general public. For more information on public-use data, see NCES online catalog at <http://nces.ed.gov/pubsearch/>.

Overview of Laws

The relevant laws about survey data that contain individually identifiable information are found in the following statutes. More information on these laws is in Chapter 1:

- The Privacy Act of 1974 and the Computer Security Act of 1987 provide for the security and privacy of personal data maintained by the federal government. These laws pertain to all restricted-use data. Unlawful disclosure is a misdemeanor and is subject to a fine up to \$5,000.
- The E-Government Act of 2002, Title V, subtitle A, Confidential Information Protection mandates the protection of individually identifiable information that is collected by any federal agency for statistical purposes. Unauthorized disclosure of these data is a class E felony, punishable by up to five years in prison, and/or a fine up to \$250,000.
- The USA Patriot Act of 2001 amended NESIA 1994 by permitting the Attorney General to petition a judge for an ex parte order requiring the Secretary of the Department of Education to provide NCES data that are identified as relevant to an authorized investigation or prosecution of an offense concerning national or international terrorism to the Attorney General.
- The Education Sciences Reform Act of 2002 requires IES to collect, analyze, and disseminate education data and to protect the confidentiality of individually identifiable information. An unauthorized disclosure is a class E felony, punishable by up to five years in prison, and/or a fine up to \$250,000.

Licensing Procedures

IES will lend restricted-use data only to qualified organizations in the United States, using a strict licensing process described in Chapter 2. Individual researchers must apply through an organization (e.g., a university or a research institution). To qualify, an organization must submit:

- An online Formal Request through the NCES electronic application system, see: <http://nces.ed.gov/StatProg/instruct.asp>,
- a signed License document (see Appendix F),

- executed Affidavits of Nondisclosure (see Appendix G), and
- a signed Security Plan Form (see Appendix J).

Security Procedures

Restricted-use data must be kept secure at all times. "Secure" means that the data are protected from unauthorized access or disclosure in accordance with the terms of the License and the specified security procedures outlined in the Security Plan Form. The security procedures described in Chapter 3 include the computer security requirements for the standalone, desktop computer configuration.

On-Site Inspections

Under the terms of the License, IES has the right to conduct unannounced, unscheduled inspections of the data user's site to assess compliance with the terms of the License and the required security procedures. The inspection procedures are described in Chapter 4.

Chapter 1: Laws

1.1 Basic Statutes

The protection of survey databases that contain individually identifiable information is founded on the following statutes:

- Privacy Act of 1974,
- E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA),
- Education Sciences Reform Act of 2002,
- USA Patriot Act of 2001, and
- E-Government Act of 2002

1.2 Privacy Act of 1974

The Privacy Act of 1974 states that federal agencies are required "to collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures...that adequate safeguards are provided to prevent misuse of such information."

To do this, the law protects the privacy of personal data maintained by the federal government. It imposes numerous requirements upon federal agencies to safeguard the confidentiality and integrity of personal data, and puts limits on the use of the data. (For the full text of the law, see Appendix C.)

Privacy Standards

Under the direction of the Office of Management and Budget, federal agencies issue policies, standards, and guidelines for protecting personal data under this law.

Computer Security Guideline

A key standard for this law is the Federal Information Processing Standard Publication (FIPSPUB) 41, *Computer Security Guidelines for Implementing the Privacy Act of 1974*. FIPSPUB 41 provides guidance to ensure that government-provided individually identifiable information is protected in accordance with federal statutes and regulations.

1.3 E-Government Act of 2002, Title III, Federal Information Security Management Act (FISMA)

The law is enacted to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." FISMA requires each agency to develop, document, and implement an agencywide information security program "providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

1.4 Education Sciences Reform Act of 2002

The Education Sciences Reform Act of 2002 (ESRA 2002) authorizes the Institute of Education Sciences (IES) to collect and disseminate information about education in the United States. Collection is most often done through surveys. This Act, which incorporates and expands upon the Privacy Act of 1974, requires strict procedures to protect the privacy of individual respondents.

This Act replaces the National Education Statistics Act of 1994 (NESA 1994). (For the full text of the law, see Appendix D.)

Confidentiality Standards

Individually identifiable information about students, their families, and their schools cannot be revealed. No person may:

- use any individually identifiable information for any purpose other than a statistical purpose, except in the case of terrorism (see USA Patriot Act below);
- make any publication whereby the data furnished by any particular person can be identified; or
- permit anyone other than the individuals authorized by the IES Director to examine the individual reports.

The Act requires IES to develop and enforce standards to protect the confidentiality of students, their families, and their schools in the collection, reporting, and publication of data. The IES confidentiality statute is found in Public Law 107-279, section 183 (or as codified in 20 U.S.C. 9573).

Violations

Anyone who violates the confidentiality provisions of this Act when using the data shall be found guilty of a class E felony and can be imprisoned up to five years, and/or fined up to \$250,000.

1.5 USA Patriot Act of 2001

The USA Patriot Act of 2001 amended NESA 1994 by permitting the Attorney General to petition a judge for an ex parte order requiring the Secretary of the Department of Education to provide NCES data that are identified as relevant to an authorized investigation or prosecution of an offense concerning national or international terrorism to the Attorney General. Any data obtained by the Attorney General for these purposes must be treated as confidential information, “consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.” This amendment was incorporated into ESRA 2002. (For the full text of the law, see Appendix D).

1.6 E-Government Act of 2002, Title V, Subtitle A, Confidential Information Protection

Following the enactment of the Patriot Act, the 107th Congress enacted the E-Government Act of 2002, Title V, Subtitle A, Confidential Information Protection (CIP 2002) which requires that all individually identifiable information supplied by individuals or institutions to a federal agency for statistical purposes under a pledge of confidentiality must be kept confidential and may only be used for statistical purposes.¹ Any willful disclosure of such information for nonstatistical purposes, without the informed consent of the respondent, is a class E felony, punishable by up to five years in prison, and/or a fine up to \$250,000.

¹ As amended by Federal Register, 62:35044-35050.

Chapter 2: Licensing Procedures

2.1 What Data Are Licensed

Only Restricted-Use Data Are Licensed

When IES conducts surveys, the data collected sometimes include individually identifiable information, which is confidential and protected by law.²

Restricted-use data is the term for survey data that contain individually identifiable information. Only restricted-use data are licensed. (Note: Public-use data are not licensed.)

The restricted-use data provided to the licensee and all information derived from those data, and all data resulting from merges, matches, or other uses of the data provided by IES with other data are subject to the License and are referred to in the License as “subject data.”

Individually identifiable information includes, but is not limited to, personal data in the following categories:

- education,
- financial,
- medical,
- employment,
- criminal, or
- personal identifiers (e.g., name, number, symbol), and
- other identifying particulars assigned to the individual (e.g., fingerprint, voiceprint, photograph).

Available Restricted-Use Databases

The restricted-use databases that are available to organizations in the United States through these licensing procedures are listed at the NCES online catalog at: <http://nces.ed.gov/pubsearch/>.

2.2 What is a License?

Three similar License documents are used to lend restricted-use data: Memorandum of Understanding, License, and Contract. All three are referred to as Licenses and, when signed, are equally binding on the licensees.

Memorandum of Understanding

The Memorandum of Understanding is used to provide data to federal agencies or offices, external to IES. A copy of the memorandum is in Appendix E.

License

The License is used to provide data to non-federal agencies or offices, including organizations working on analysis contracts with IES. Appendix F contains a copy of the License.

² Because federal laws cannot be enforced outside of the United States, restricted-use data cannot leave the United States.

Contracts

When IES has a contract involving the collection of restricted-use data, the contract “boiler plate” includes the provisions of the License.

Content of License Documents

In brief, each of the three License types:

- defines the information subject to this agreement,
- specifies the individuals who may have access to subject data (PPO and professional/technical and support staff),
- describes limitations of disclosure,
- lists administrative requirements,
- requires that publications based on the data be sent to IES prior to disseminating them to non-licensed individuals,
- requires the organization to contact IES in case of (suspected) breaches of security,
- requires the organization to agree to unannounced and unscheduled inspections,
- reviews the security requirements for the maintenance of, and access to, subject data, and
- describes penalties for violations.

2.3 Who Needs a License Document

Virtually every organization needs a License document to authorize individual access to restricted-use data. The type of organization determines the specific License document.

Matching Organizations to License Documents

Type of Organization	License Document Type
Congress	Memorandum of Understanding
Federal Agencies *	Memorandum of Understanding
IES Staff	Oath of office replaces Memorandum; staff must sign a form provided by the IES Data Security Office to obtain the data.
Non-Federal Agencies/Groups/Organizations	License
State and Local Agencies	License
Research Laboratories	License
Data Collection Contractor (to IES)	License "Boiler Plate" in Contract
Contractor (to IES Contractor)	License "Boiler Plate" in Contract
Survey Pre-Tests	License "Boiler Plate" in Contract
Analysis Contractor	License

* This includes other components of the Department of Education.

Restricted-Use Data and IES Staff

IES staff are subject to all of the obligations and restrictions protecting restricted-use data. Further, IES staff are not authorized to issue restricted-use data files.

- Any in-house staff needing access to restricted-use data must request and obtain clearance through the IES Data Security Office.
- Staff must sign a form provided by the IES Data Security Office to obtain the data.
- Staff who have restricted-use data must keep it under lock and key. These data may not be stored on a laptop computer and computer output cannot be left out in the open when not in use. (See Chapter 3, Security Procedures, for full details.)
- The data may not be removed from the office area.
- These restricted-use data **must** be returned to the IES Data Security Office prior to the departure of an employee or Fellow. IES staff should refer all requests for License documents, affidavits, or restricted-use data to the IES Data Security Office. These requests should not be handled by program staff.

Pre-test Monitoring

Staff perform pre-tests to review the data collection process and to test the validity of the survey instrument. Because respondent data are acquired to test the proposed survey design, the responses collected in this pre-test sampling may contain individually identifiable information and thus may be subject to restricted-use data security procedures.

The IES Contracting Office Technical Representative (COTR) who is responsible for conducting these pre-tests, must submit a written description of what is involved in the survey design review to the IES Data Security Office. The COTR must also obtain an executed Affidavit of Nondisclosure from all persons outside IES who will review the survey design and will have access to these data. The COTR will keep all original Affidavits of Nondisclosure in the project file and be able to produce them on request.

Contractors

An organization or individual performing work under contract must complete the licensing process **unless the collection of restricted-use data is required to fulfill the terms of the contract**. The conditions spelled out in the License are incorporated in the “boiler plate” of the contract.

- Sub-Contractors (to Contractors) are bound by the terms in the contractual agreement of the contractor.
- Those terms include the provision that **data cannot leave the licensed site**. Sub-contractors needing to use data at a remote site must get their own Licenses.

A contractor who proposes to do independent research using the restricted-use data to perform work for IES must submit a formal, written request. If the purpose of the independent research is different from the purpose for using the data as stated in the contract, the contractor must follow the standard application process for obtaining a License (see section 2.4).

2.4 Applying for a License

Summary of Procedures

To qualify for and receive restricted-use data, applicants must submit all four documents:

- Formal Request through the IES online electronic license application system, (see: <http://nces.ed.gov/StatProg/instruct.asp>),
- License Document (see Appendix E or F),
- Affidavits of Nondisclosure (see Appendix G), and
- Security Plan Form (see Chapter 3 and Appendix J).

The Formal Request will ask for specific items of information. This information will be collected through the IES electronic license application system at:

<http://nces.ed.gov/StatProg/instruct.asp>.

After the initial online Formal Request has been reviewed and approved by the IES Data Security Office, applicants are to prepare, complete and return the signed License, notarized Affidavits, and the Security Plan Form.

Mail all documents, **signed by the Principal Project Officer (PPO) and Senior Official (SO)** to the IES Data Security Office.

The IES Data Security Office staff will review the submitted documents for content and completeness.

- In the online Formal Request, you must demonstrate that the proposed research project meets basic requirements of applicability to education research.
- The Security Plan Form must be complete and must comply with the Security Procedures outlined in Chapter 3.
- IES may request additional information regarding the proposed use of the data, the resources available to the researcher to perform the analysis, or other aspects of the project that is deemed necessary. All questions IES has about an organization's application must be resolved in writing prior to the formal approval of the License.

The License documents are only submitted to the IES front office for final approval when all required information has been received and the License application is complete.

The decision to grant a License is solely that of the Director. The License approval becomes effective on the date of the Director's signature.

Formal Request

The Formal Request will ask for specific items of information (see checklist below). Your information will be collected through the IES electronic license application system at:

<http://nces.ed.gov/StatProg/instruct.asp>.

Formal Request Checklist	✓
(1) The name, title, and contact information of the Principal Project Officer	
(2) The name, title, and contact information of the Senior Official	
(3) The name, title, and contact information of the System Security Officer	
(4) The title of the database(s) requested for access	
(5) A description of the statistical research project and how the restricted-use database will be used and justification for access	
(6) The names and titles of other persons who will use and access the data	
(7) The estimated loan period (not to exceed five years)	

The Formal Request requirements are described in more detail below:

(1) The name, title, and contact information of the Principal Project Officer who will oversee the daily operations. To qualify for and receive a restricted-use data License and the restricted-use data, academic applicants must have the rank of **post-doctoral fellow or above** to serve as the Principal Project Officer (PPO). Visiting professors or scholars cannot be a PPO. Applicants in research laboratories or analytic consulting firms must have the rank of **research associate or above** to serve in this role. (The PPO is the researcher in charge of the day-to-day operations involving the use of subject data and is responsible for liaising with the IES Data Security Office.)

(2) The name, title, and contact information of the Senior Official having the signatory authority to legally bind the organization to the provisions of the License contract.

(3) The name, title, and contact information of the Systems Security Officer who will oversee the security of the data. The PPO can also serve as the SSO.

(4) The title of the database(s) the organization wants to access.

(5) A description of the statistical research project. The description must fulfill the following conditions:

- explain why the public-use version of the data is insufficient for your research needs,
- describe the final research objective and use of the data,
- describe the sector(s) of the community that will be served by the product, and
- assure IES that the data will not be used for any administrative or regulatory purpose in addition to, or instead of, the statistical purpose described.

Note: The purpose of the research for which the data are requested **must accord with the purpose for which the survey data were collected**. Descriptions of those purposes are in Appendix H.

If an applicant requests access to subject data that are currently under an IES Contract/Task Order with the applicant, the applicant must provide:

- the contract number, and
- the name of the Contracting Office Technical Representative (COTR).

(6) The names and titles of other persons who will be accessing the database. Generally, the staff is limited to a maximum of seven (7) persons. Exceptions to this limit may be authorized by the IES Data Security Office. Written documentation authorizing the exception must be obtained from IES. Please note that requests for additional data or amendments to an existing License will only be accepted from the PPO.

(7) The estimated loan period necessary for accessing the database. Loan periods are in one-year increments and may not exceed a five-year period. The loan period starts on the date that IES signs the License document.

License Document

The License document is a legally binding agreement or contract.

License Document Checklist	✓
Review the appropriate License document	
Insert the name of the Agency or organization to be licensed in the appropriate blank(s)	
The Senior Official (or appropriate government official) signs the License	
The Principal Project Officer signs the License	
Indicate loan period (not to exceed five years)	
Send the original signed License to the IES Data Security Office	

Affidavit of Nondisclosure

An Affidavit of Nondisclosure must be executed for each person who will have access to the data.

Affidavit of Nondisclosure Checklist	✓
Obtain a notarized Affidavit of Nondisclosure from each person who may come in contact with the subject data, as well as any non-security/police personnel who have key access to the secure project office. (For more information on this requirement, see Chapter 3.)	
Fill in all requested information on the Affidavit	
Send the original signed and notarized Affidavits of Nondisclosure to the IES Data Security Office	

Appendix G contains a copy of the Affidavit of Nondisclosure form.

In general, an individual who is not an IES employee and who wants access to licensed individually identifiable information must execute an Affidavit of Nondisclosure and submit it, through a licensed organization, to the IES Data Security Office. IES allows **up to seven (7) individuals per License** to have access to the subject data.

The one-page Affidavit contains:

- the name of the survey(s) to be accessed (see below),

- an oath or affirmation not to disclose individually identifiable information to any person not similarly sworn,
- the penalties for disclosure, and
- the signature and imprint of a notary public.

Affidavits are “**data-specific**”: they are only valid for the data listed on the form. **Include all data names and all subsequent followups that will be needed**; for example, “the base year data and all subsequent followups.”

Notarized documents cannot be amended by IES. To access a followup of a listed database or to access data that was not listed on the notarized affidavit, another affidavit must be executed.

Organizations must promptly notify IES of any changes in project staff. (See Section 2.6, Amending a License.)

Security Plan Form

The Security Plan Form contains the detailed procedures for protecting the subject data.

Security Plan Form Checklist	✓
Review Chapter 3, Security Procedures	
Fill out the Security Plan Form found in Appendix J	
Send the original, signed Security Plan Form to the IES Data Security Office	

Restricted-use data must be kept secure at all times, meaning that the individually identifiable information is secure from unauthorized disclosure or modification. Security procedures are explained in detail in Chapter 3; the Security Plan Form can be found in Appendix J.

Note: In lieu of the Security Plan Form, federal agencies must submit documentation verifying that the agency has an approved Certification and Accreditation (C&A) for its IT systems. Federal agencies must adhere to the security requirements set forth in the MOU.

Receiving the Requested Materials

Once the License is approved by IES, the IES Data Security Office sends the licensee the data and other items.

Final Product Package Contents	✓
The new licensee receives the License package that includes:	
• a copy of the original License and Security Plan Form	
• copies of the Affidavits of Nondisclosure	
• Restricted-use database media materials and instructional materials to assist the project staff in the use of the data. The data CD-ROM includes a - (1) Warning/Restriction Label (2) Loan Expiration Date	

The package is sent **Restricted Delivery - Certified Mail** to the licensee. All restricted-use data on CD-ROM are encrypted and require a passphrase to open. The PPO must email the IES Data Security Office with a list of encrypted files in order to obtain the needed passphrases.

Note: **Only one copy of a database in any format can be borrowed at a time.** A licensee who has a copy of the database and wants a revised version must return the original via certified mail before the revised version will be sent. (See Section 2.6, Amending a License.)

Under no circumstances may the original or a duplicate of the database be removed or electronically communicated from the licensee's secure project office.

2.5 Required Licensee Activity

The licensee is responsible for all terms and conditions in the License document, the Security Plan Form and related materials. (See the appropriate License document in Appendix E or F for full requirements.)

This section addresses three major administrative requirements:

- Maintaining the License file, including copies of all executed Affidavits,
- Submitting research publications for disclosure review **prior to publication or access by non-licensed individuals**, and
- The licensee's responsibility to be ready for inspection at all times.

Maintaining the License File

The Principal Project Officer (PPO) is accountable for having all pertinent information listed below in a License file.

License File Checklist	✓
The PPO shall maintain a License file in the secure project office where the licensee stores the restricted-use data. This file must contain the following items:	
• copies of emails received from the IES Data Security Office	
• the License and its attachments, which are: (1) a description of research (2) the Privacy Act of 1974 (5 U.S.C. 552a) and IES-specific laws (3) the Security Plan Form	
• any amendments to the License document and related emails	
• a current list of all individuals who may have access to the data, along with copies of their notarized Affidavits of Nondisclosure	

Note: All project staff shall both READ and UNDERSTAND this material. All individuals who have access to the subject data must be fully aware of the required security requirements and procedures. (The Principal Project Officer is

directly responsible for ensuring that all project staff understand and implement all of the required security procedures.)

Submitting Research Publications

If the licensee intends to publish or distribute any information product that uses the subject data where unauthorized persons will have access, then the licensee must submit an advance copy of the product to the IES Data Security Office via email prior to its publication or access by non-licensed individuals. Once the document has been cleared by the IES Data Security Office, the licensee may distribute the document as desired.

Research Publication Checklist	✓
The PPO shall forward a copy of each publication containing information based on restricted-use data to the IES Data Security Office for a disclosure review.	
For all datasets produced by IES or NCES, licensees are required to round all unweighted sample size numbers to the nearest ten (nearest 50 for ECLS-B) in all information products (i.e.: proposals, presentations, papers or other documents that are based on or use restricted-use data). For all other datasets, including administrative datasets produced by other agencies within the Department of Education (e.g. ED Facts, CRDC, etc.), disclosure avoidance standards will vary. The required disclosure avoidance measures for these non-IES datasets will be listed in a readme.txt file included with that specific dataset.	
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. The licensee must not release the information product to any person not authorized to access the data until formally notified by IES that no potential disclosures were found. This review process usually takes 3 to 5 business days.	

Passing On-Site Inspections

The License (Section IV.G) gives IES the right to conduct **unannounced, unscheduled** inspections of the licensee's secure project office to assess compliance with the provisions of the License, security procedures (see Chapter 3), and the licensee's submitted Security Plan Form. (The inspection procedures are described in Chapter 4, and a copy of the On-Site Inspection Guideline can be found in Appendix K.)

Any violation found during the inspection may subject the licensee to immediate revocation of the License by IES, or report of the violation to the U.S. Attorney.

On-site Inspection Checklist	✓
When an on-site inspection is conducted, IES will provide formal notification of any violations of the required security procedures. If violations are reported, the licensee must take the following steps:	
<ul style="list-style-type: none"> • Correct all identified security violations. 	
<ul style="list-style-type: none"> • Notify IES in writing of the corrective measures. 	

Outside Requests for Data

The licensee shall notify IES immediately when he/she receives any legal, investigatory or other demand for IES subject data, including any request or requirement to provide subject data to a state agency or state contractor. The licensee is not authorized to give IES subject data to the requester.

2.6 Amending a License

IES must be kept informed of any modifications in project operations throughout the span of the loan period. The most common changes to a License can be done online through the licensee's online License information page. **All amendment requests must be initiated by the Principal Project Officer** (or the Senior Official in the PPO's absence). A weblink to the licensee's online License information page may be obtained from the IES Data Security Office at the request of the PPO, or can be obtained through the system login page, at:

<https://nces.ed.gov/statprog/licenseapp/RequestEmail.asp>

Six types of amendments can be submitted via the online License system:

- Add User,
- Delete User,
- Add Database,
- Modify Security Plan,
- Extend License, and
- Close-out License

Note: Paper requests for these six amendments will not be accepted. These amendments, and the associated documentation required for each, are described in more detail below.

To submit the desired amendment, the PPO must click on the corresponding button on the licensee's online License information page, and complete the information on the presented web pages. Once the amendment is submitted, the PPO will receive an automatically-generated email stating that the request has been received by the IES Data Security Office. Another email will be generated when the amendment has been approved by IES. The licensee is responsible for keeping copies of these emails in the License file as discussed in Section 2.5.

Note: The online License system will only process one amendment request at a time. If another amendment has already been requested, no other amendments to the License are possible until the pending amendment has been approved or canceled.

Add User Amendment

An "Add User" amendment is requested in order to add additional project staff to the License (multiple new users may be added in the same amendment request). After the "Add User" amendment has been submitted, the licensee must then send an original signed and notarized Affidavit of Nondisclosure for each new user(s) to IES.

Once the affidavits have been received, the amendment will be approved through the online system and the users will then be approved to access the restricted-use data. Until the “Add User” amendment has been approved, the new user(s) must not be allowed access to the subject data.

Add User Amendment Checklist	✓
Notify IES of any additions to project staff via an “Add User” amendment request through the online License system.	
Send the notarized Affidavit(s) of Nondisclosure for the additional users to IES.	
Retain copies of the emails from IES confirming the initial submission and final approval of the “Add User” amendment in the License file.	

Delete User Amendment

A “Delete User” amendment is requested in order to remove listed users from the License. This amendment requires no corresponding paperwork. The IES Data Security Office usually approves these amendments in one business day. **After removal from the License, the departing individual(s) must not be permitted access to the restricted-use data.**

Delete User Amendment Checklist	✓
Notify IES of any reductions in project staff via a “Delete User” amendment request through the online License system.	
Mark Affidavits of removed users as “Void” in the License file.	
Retain copies of the emails from IES confirming the initial submission and final approval of the “Delete User” amendment in the License file.	

Add Database Amendment

A licensee may request access to another database in addition to what was agreed to in the original License, by means of an “Add Database” amendment through the online License system. This amendment must also be requested in order to obtain different waves of the database(s) requested under the original License.

Any new database requested must be covered by the Affidavits of Nondisclosure on file for each listed License user. If the requested database is covered, no paperwork is needed to complete the amendment process. If the Affidavit(s) does not cover the requested data, the licensee must send IES new original signed and notarized Affidavits for all listed users who will have access to the new database.

Upon receipt of Affidavits that cover the requested data, the IES Data Security Office will approve the amendment. The new database will be sent **Restricted Delivery—Certified Mail** to the listed address of the PPO.

Add Database Amendment Checklist	✓
Initiate the request for the additional database(s) via an “Add Database” amendment request through the online License system.	
Complete all required fields for the amendment online.	
Send in newly signed and notarized Affidavits for all license users if current Affidavits do not cover the requested database(s). Copies of all new affidavits should be retained in the License file.	
Retain copies of the emails from IES confirming the initial submission and final approval of the “Add Database” amendment in the License file.	

Modify Security Plan Amendment

As part of the License agreement, IES requires each licensee to designate a specific secure project office in which the restricted-use data will be used and stored. If the location of the secure project office is going to be changed, or an additional project office added to the License, the PPO must submit a “Modify Security Plan” amendment through the online License system *before* the relocation. The PPO must detail the new location and any changes to the established security procedures in the amendment request. The PPO must also send a completed and signed Security Plan Form with the new information to the IES Data Security Office for review before this amendment can be approved. The restricted-use data cannot be moved to the new location until the revised Security Plan Form has been approved by IES.

Note: If the secure project office must change locations temporarily (e.g. for remodeling or maintenance), and will return to the approved site within a short period of time, no “Modify Security Plan” is required. In this case, the PPO should email the IES Data Security Office with the following information: the temporary location of the secure project office, the expected duration of the relocation, and confirmation that all required security procedures will be followed at the new location. Information regarding the required security procedures may be found in Chapter 3.

Modify Security Plan Amendment Checklist	✓
Inform the IES Data Security Office of a location change for the secure project office via a “Modify Security Plan” amendment through the online License system. This amendment must be submitted and approved before the location of the restricted-use data is changed.	
Complete all required fields for the amendment online, detailing the new address and other pertinent information.	
Send in a completed and signed Security Plan Form detailing the new information.	
Retain copies of the emails from IES confirming the initial submission and final approval of the “Modify Security Plan” amendment in the License file.	

Extend License Amendment

When the loan period of the original License agreement is completed, licensees have the option of extending the loan period for up to five years, using an “Extend License” amendment request through the online License system. The licensee must meet all current licensing requirements in order to qualify for the extension. Any obsolete paperwork must be updated, and all current

security standards required by IES at the time of the extension must be adopted by the licensee before the License extension is approved.

Upon receipt of the amendment request, the IES Data Security Office will review the License file to determine if any information or paperwork needs to be updated. An email will then be sent to the licensee detailing any further steps that must be taken (if any) to complete the extension request. If updated paperwork is required, the extension request will not be approved until the new paperwork is received and approved by the IES Data Security Office.

The “Extend License” amendment request may be submitted up to one year before the expiration of the loan period, and at any point thereafter. **Note: Once the loan period for the License has ended, a licensee will only be able to extend or close-out their License; no other amendments will be accepted for an expired License.**

Extend License Amendment Checklist	✓
Submit the “Extend License” amendment through the online License system within one year of the expiration of the License loan period.	
Complete and sign any updated paperwork requested by the IES Data Security Office and send the paperwork to the IES Data Security Office.	
Retain copies of the emails from IES confirming the initial submission and final approval of the “Extend License” amendment in the License file, along with copies of all updated paperwork.	

Close-out License Amendment

When the loan period is complete and no extension is desired or the licensee does not need the restricted-use data any longer, a “Close-out License” amendment must be submitted through the online License system. After the request has been submitted online, the licensee must return all restricted-use data and associated materials to IES, along with a completed and signed close-out certification form. A copy of the close-out certification form may be found in Appendix M.

On the close-out certification form, the PPO must list all databases being returned, and confirm that all restricted-use data have been wiped from the computer, that all backup copies and any restricted-use data printouts have been destroyed, and that any remaining documents or publications using the restricted-use data will be sent to the IES Data Security Office for disclosure review prior to distribution to non-licensed individuals (the disclosure review process is described in Section 2.5). The form must also be signed by a second witness, confirming the restricted-use data have been deleted or destroyed.

This completed and signed form must be sent to IES along with all restricted-use data materials obtained under the License, and a tracking number must be used on the shipment. **Unless the restricted-use data materials and the completed close-out form are both returned to the IES Data Security Office, the License cannot be closed.**

Once all restricted-use data and the close-out certification form have been received, the “Close-out License” amendment request will be approved by IES and the licensee will receive an email

confirmation that the License has been closed. **Note: The IES Data Security Office reserves the right to conduct a close-out inspection of the project site after the License has been closed in order to ensure that all required close-out procedures have been followed.**

Close-out License Amendment Checklist	✓
Request a “Close-out License” amendment online through the online License system if the licensee no longer needs the restricted-use data or if the loan period has expired.	
Destroy all hard copy versions of subject data and backup copies. Overwrite the subject data on computer used in analysis (all data must be totally obliterated so that the data cannot be recovered by any means).	
Return the original subject data and a completed close-out certification form to the IES Data Security Office using a tracking number on the shipment.	
Submit any remaining documents or publications to the IES Data Security Office for disclosure review prior to disseminating them to non-licensed individuals.	

Changes to the License that are not covered by the six online amendments should only be initiated by the PPO through an email to the IES Data Security Office. Such changes might include changing the PPO, SO or SSO, canceling a pending online amendment, or requesting new copies of databases already obtained under the License if original copies are found to be defective.

All amendment requests and changes to the License must originate from the PPO.

2.7 Applicant/Licensee Record

The following checklist summarizes the Licensing Procedures for Restricted-Use Data.

ACTIVITY	✓
REVIEW REQUIRED PROCEDURES	
Obtain a copy of the <i>Restricted-Use Data Procedures Manual</i> .	
Review the manual.	
APPLYING FOR A LICENSE	
Submit the following to the IES Data Security Office through the electronic license application system at: http://nces.ed.gov/StatProg/instruct.asp	
Formal Request:	
(1) Contact information of the Principal Project Officer (PPO).	
(2) Contact information of the Senior Official (SO).	
(3) Contact information of the Systems Security Officer (SSO).	
(4) Title of requested database(s).	
(5) Description of the statistical research project for which the restricted-use data are needed; explanation of why the restricted-use data are needed (e.g., instead of the public data version); explanation of how the statistical research project is consistent with the specific purpose for which the study data was	

collected.	
(6) Names and titles of other persons who will use and access the data	
(7) Estimated loan period (not to exceed five years)	
Paperwork:	
Send the following three items to the IES Data Security Office:	
1) License Document - Complete and sign the License document or MOU.	
2) Affidavit(s) of Nondisclosure -	
(a) Ensure personnel who will execute Affidavits read and understand the License contract and the security procedures.	
(b) Complete, sign, and notarize the Affidavits of Nondisclosure for all project personnel, including support staff.	
3) Security Plan Form - Complete and sign the Security Plan Form found in Appendix J. Add in any additional protections due to local conditions.	

REQUIRED LICENSEE ACTIVITY	
Maintaining the License File	
Have on file at the licensed secure project office, copies of:	
(1) Emails received from the IES Data Security Office,	
(2) The License document and its three attachments,	
(3) Amendments to the License and all associated request/approval emails,	
(4) All executed Affidavit(s) of Nondisclosure , and	
(5) Licensee's submitted Security Plan Form .	
Instruct all project staff about what the License file is and where it is kept.	
Submitting Research Publications	
(1) Forward to IES for review copies of each publication or document <i>before</i> it is distributed to non-licensed individuals. IES will formally notify the licensee if the publication is cleared for dissemination (i.e., no disclosure risks were found).	
(2) A final copy of each publication containing information based on restricted-use data must be forwarded to IES.	
Passing On-Site Inspections (also see Chapter 4)	
(1) After conducting an on-site inspection, IES will provide formal notification of any violations found.	
(2) All identified security violations must be corrected.	
(3) Licensee must notify IES in writing of the corrective measures.	

AMENDING A LICENSE	
Licensee must notify IES if there will be any changes to the conditions of the License. The following six amendments must be initiated through the online License system:	
(1) Add User —After submitting online request, send in original signed and notarized Affidavits of Nondisclosure for new user(s)	

(2) Delete User —After submitting online request, IES will approve request
(3) Add Database —After submitting online request, send in new affidavits for all users if current affidavits do not cover requested data
(4) Modify Security Plan —After submitting online request, send in revised and signed Security Plan Form
(5) Extend License —After submitting online request, send in any updated paperwork requested by the IES Data Security Office
(6) Close-out License —After submitting the online request, send completed close-out certification form and all restricted-use data materials to the IES Data Security Office, using a tracking number on the shipment, destroy all hard copies of restricted-use data, purge all subject data from all computers used for data analysis, and send any remaining documents using subject data to the IES Data Security Office for a disclosure review.
Any other changes to the License must be requested via email by the PPO.

Chapter 3: Security Procedures

IES shall ensure that all individually identifiable information remain **confidential**, in accordance with the Privacy Act of 1974 and the Education Sciences Reform Act of 2002.

3.1 Introduction

Restricted-use data Licenses are used to make sensitive federal information sources available to qualified research organizations. Strict security procedures are required to protect the data on individuals who responded to these surveys; i.e., who provided individually identifiable information.

The licensees are governed by the terms of the License and these security procedures, which are the minimum requirements for protecting the individually identifiable information (referred to as "subject data" in the License) while in the custody of the licensee. The protection requirements for individually identifiable information are based on three statutes.

Basic Statutes

- The Privacy Act of 1974: Defines, and provides for the security and privacy of, personal data maintained by the federal government.
- The Computer Security Act of 1987: Increases the protection requirements for Privacy Act data and other sensitive federal information; requires a security plan for each computer system that contains sensitive federal information.
- The E-Government Act of 2002, Title V, subtitle A, Confidential Information Protection mandates the protection of individually identifiable information that is collected by any federal agency for statistical purposes. Unauthorized disclosure of these data is a class E felony.

IES Statutes

- The Education Sciences Reform Act of 2002 mandates the protection of individually identifiable information about students, their families, and schools that is collected and disseminated by IES. Unauthorized disclosure of these data is a class E felony.

WARNING

Anyone who violates the confidentiality provisions of this Act shall be found guilty of a class E felony and imprisoned up to five years, and/or fined up to \$250,000.

Other Statutes

Other statutes may apply under certain circumstances, such as the Computer Fraud and Abuse Act of 1986, which makes it a felony to gain unauthorized access to a computer system containing federal data, or to abuse the access one has, with the purpose of doing malicious destruction or damage.

3.2 Risk Management

Individually identifiable information is highly sensitive and requires high levels of confidentiality and integrity protection to prevent unauthorized disclosure or modification. The integrity of information produced from these data relies on the integrity of the source data. Licensees shall ensure that adequate security measures are continuously in place so that the subject data are secure from unauthorized disclosure, use, or modification.

The Summary of Minimum Security Requirements below provides an overview of the protection measures. Note: IES may inspect licensee facilities (see Chapter 4) and the questions that will be asked are based on these minimum security requirements. Appendix K contains a list of the questions.

Summary of Minimum Security Requirements

General Security (Section 3.3)

- Assign security responsibilities
- Complete the Security Plan Form
- Restrict key access to secure project office to license users only
- Use data at licensed project office site only
- Limit data access to only users with an affidavit on file with IES
- Permit read-only access to data only
- Permit users to access only data listed on their own affidavit
- Return original data to IES using tracking number on shipment

Physical Handling, Storing, & Transporting Data (Section 3.4)

- Protect machine-readable media/printed material
 - Store securely
 - Label/catalog/track
- Use data on a non-networked desktop computer only
- Avoid disclosure from printed material
- Restrict copying of data
- Limit backups-one copy of data
- Limit transporting of data to:
 - Sworn employees
 - Bonded couriers
 - Certified mail

Licensees (i.e., Principal Project Officers) shall assess the security of the environment in which the data will be accessed, handled, and stored to determine if the minimum security procedures, described herein, are adequate for their environment. Since facilities and computer capabilities vary considerably, there may be onsite conditions that necessitate additional protections. If so, licensees shall increase protections to make their environment secure.

Licensees must meet the spirit and intent of these protection requirements to ensure a secure environment 24 hours a day for the loan period of the License.

3.3 General Security Requirements

Assign Security Responsibilities

The Senior Official (SO), who signed the License document/contract, has overall responsibility for the security of the subject data.

The Principal Project Officer (PPO):

- is the most senior officer in charge of the day-to-day operations involving the use of subject data, and
- has full and final responsibility for the security of the subject data, shall oversee the preparation and implementation of the NCES restricted-use data security plan, and shall monitor and update the security requirements, as needed.

The SO or PPO shall assign a System Security Officer (SSO) (or assume the duties). The SSO shall be responsible for maintaining the day-to-day security of the licensed data.

The SSO's assigned duties shall include the implementation, maintenance, and periodic update of the security plan to protect the data in strict compliance with statutory and regulatory requirements.

Complete the Security Plan Form

Licensees shall complete the restricted-use data Security Plan Form before permitting any access to the subject data.

The SO, PPO, and SSO shall sign the implemented security plan and provide a copy with the original signatures to IES.

Federal agencies will submit a copy of the Certification and Accreditation (C&A) for their IT systems in lieu of a Security Plan Form. Federal agencies must adhere to the security requirements set forth in the MOU.

Restrict Access to Data

Access control is the process of determining WHO will have WHAT type of access to WHICH subject databases.

- **WHO?** Only professional/technical and support staff (P/TS) who have signed an Affidavit of Nondisclosure (which requires reading and understanding the **Security Procedures**) and who are listed as users on the License may have access to the data, as stated in Section 2.4.
- **WHAT type of access?** User access to the original version of the subject data shall be **read-only**. Restricted-use survey data are not to be modified or changed in any way. Only extrapolations and reading of the data are permitted.
- **WHICH data?** Each individual's Affidavit of Nondisclosure lists the restricted-use data that can be accessed.

Use Data at Licensed Site Only

Licensee shall retain the original version of the subject data and all copies or extracts at a single location (i.e., the licensed site) and shall make no copy or extract of the subject data available to anyone except an authorized License user as necessary for the purpose of the statistical research for which the subject data were made available to the licensee.

Licensee shall not permit removal of any subject data from the licensed site (i.e., limited access space protected under the provisions of this License) without first notifying and obtaining written

approval from the IES Data Security Program. **The data cannot be used at home or provided to a sub-contractor to use off-site.**

Response to Outside Request for Subject Data

Any researcher who requests access to subject data must sign an Affidavit of Nondisclosure under the procedures in Section IV of the License.

Licensee agrees to notify IES immediately when it receives any legal, investigatory, or other demand for disclosure of subject data, including any request or requirement to provide subject data to any state agency or state contractor under conditions that are inconsistent with any requirement of this License. Time is of the essence in notifying IES of any such request or requirement. Licensee must also immediately inform the requestor or enforcer of the request or requirement that subject data are protected under the law of the United States, as specified in Section 3.1. Licensee authorizes IES to revoke this License and, pending the outcome of the penalty procedures under Section VI of this License, to take possession of or secure the subject data, or take any other action necessary to protect the absolute confidentiality of the subject data.

Return Original Data to IES

Licensee shall return the original subject data to the IES Data Security Program by certified mail when the research or the subject of the agreement has been completed or the License terminates, whichever occurs first. All other individually identifiable information (e.g., the one backup copy, working notes) shall be destroyed using approved IES procedures.

3.4 Physical Handling, Storage, and Transportation

Protect Machine-Readable Media and Printed Material

Machine-readable media storage devices from IES will be CD-ROMs or DVD-ROMS. Note: Data stored on fixed hard disks are addressed in Section 3.5 in Standalone Desktop Computers.

Lock Up Media

Subject data on machine-readable media shall always be secured from unauthorized access (e.g., locked in a secure cabinet within secure project office when not in use, only one backup copy can be made).

Label/Catalog/Track Media

To ensure that License loan period is not exceeded, all portable media from IES has been labeled with the expiration date of the License. **If the user changes the media, or develops subsets, new labels with the expiration date must be affixed.** Additionally, use a simple, effective cataloging/ tracking system to know **who** has possession and responsibility for **what** media at all times. **Anyone having access to the data must have an affidavit on file with IES, including computer personnel who load data on the system. Data shall not be in a computer facility library unless all who have access to the library media hold affidavits.**

Avoid Disclosure from Printed Material

Lock Up Printed Material

Printed material containing individually identifiable information shall always be secured from unauthorized access (e.g., locked in a secure cabinet within the secure project office when not in use).

Edit for Disclosures

Licensee shall ensure that all printouts, tabulations, and reports are edited for any possible disclosures of subject data before such output is seen by non-licensed individuals. In planning and producing analyses and tabulations, the general rule is not to publish a cell in which there are fewer than three (3) respondents or where the cell information could be obtained by subtraction. In addition, care must be taken not to disclose information through subsequent use of the same data with variables from other databases.

Licensees are required to round all unweighted sample size numbers to the nearest ten (nearest 50 for ECLS-B) 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. The licensee must not release the information product to any person not authorized to access the subject data until formally notified by IES that no potential disclosures were found.

Only One Backup Copy

The licensee is permitted to make **only one backup copy of the entire database** at the beginning of the loan period. Protect this backup copy under the same security procedures as the original database.

If the licensee plans to make a backup copy of the restricted-use data, the licensee must state in their security plan: (1) that a backup copy of the entire database will be made, and (2) what security procedures will protect the restricted-use data from disclosure.

Limit Transporting of Data

Restricted-use data are licensed for one site only (see Section 3.3), and only the following methods shall be used for transporting the data within that site, to a new License site as approved by IES, or to and from IES:

- An individual with a signed Affidavit of Nondisclosure (that is on file at IES);
- A "bonded courier," who must sign for the sealed package, and who is responsible for the data during transport; or
- By certified mail (normal for transporting data between the IES and the licensee).

3.5 Computer Security Requirements

If prospective licensees cannot meet the security requirements, then they will not be granted a License.

Standalone Desktop Computer

A standalone desktop computer is any single-user PC (e.g., running a Windows operating system). **Laptop computers are strictly prohibited.** See “No Connections to Another Computer” below for further information.

Limit room/area access

The data must **always** be secured from unauthorized access. Computer rooms/areas that process individually identifiable data must be secure during business hours and locked after close of business. **Only users listed on the License may have key access to the secure project office.**

Standalone Computer Security Model

Minimum Security Requirements -

- **Laptop computers cannot be used**
- **Limit access to room/area to License users only**
- **Passwords**-unique, 6-8 characters with one non-alphanumeric
- **Change password** at least every 3 months
- **Notification** (warning statement)
- **Read-only access** to original data
- **Shut down any connections** to other computers prior to loading data on the system
- **Lock computer and/or room** when away from computer, or **Enable automatic "shutdown"** after 3-5 minutes of inactivity
- **No routine backups** of restricted-use data
- **Change staff passwords** accordingly when staff changes
- **Remove data by overwriting** at the end of the project or prior to the computer needing repair

Implement these security measures

Passwords

When passwords are used, they shall be unique, 6-8 characters in length, contain at least one non-alphanumeric character (e.g., ?, &, +), and be changed at least every three months. See subparagraphs “Lock Computer and/or Room” and “Automatic 'Shutdown' of Inactive Computer” for other password requirements. (For additional details on passwords, see FIPSPUB 112, *Password Usage*, Section 4.3, "Password System for High Protection Requirements.")

In the absence of an automated password generator, user-selected passwords should be unique, memorizable, and NOT dictionary words. One good way to select a password is to make up an

easy to remember phrase-My Favorite Lake Is Superior-and use the first letter in each word plus a non-alphanumeric character (e.g., ?, +, *) as your password. The result is MFL?IS.

Notification (warning screen)

During the log-in or boot-up process, a warning statement should appear on the screen before access is permitted. This statement should stay on the screen for at least ten seconds to ensure that it is readable. The statement should be worded to ensure that the intent of the following is conveyed:

Unauthorized Access to Licensed Individually Identifiable Information is a Violation of Federal Law and Will Result in Prosecution.

If it is not feasible to have this statement appear on the screen of the computer, it should be typed and attached to the monitor in a prominent location. The following is an example of the warning screen:

WARNING

FEDERAL RESTRICTED-USE DATA

**UNAUTHORIZED ACCESS TO LICENSED INDIVIDUALLY IDENTIFIABLE
INFORMATION IS A VIOLATION OF FEDERAL LAW AND WILL RESULT IN
PROSECUTION.**

DO YOU WISH TO CONTINUE? (Y)es or (N)o

Read-only Access

User access authorization to the original data shall be read-only. Restricted-use survey databases are not to be modified or changed in any way. Only extrapolations and reading of the original data are permitted.

No Connections to Another Computer

Prior to placing any subject data (individually identifiable information) on a standalone desktop computer, shut down any connections to another computer (e.g., via modem, LAN, cable, wireless). For modems, use one of the following methods to prevent unauthorized dial-in access:

- unplug the phone line connected to the modem, or
- turn off the power to an external modem, or
- disable the "answer mode" software on the computer.

The standalone desktop computer cannot be connected to the LAN while subject data are being used in the system or stored on the hard drive.

Lock Computer and/or Room

When the authorized user is away from the computer, protect the subject data by locking the computer and/or the room. For example, physically lock the computer with its exterior keylock, shut down the computer and enable its power-on password, or lock the room to prevent an unauthorized individual from gaining access to the computer.

Automatic "Shutdown" of Inactive Computer

Some computers can automatically shut down, logout, or lockup (e.g., password-protected screen-savers) when a period of defined inactivity is detected. If available, this feature may be used in place of or in addition to locking the computer and/or room. When used, the defined period of inactivity shall be three to five minutes.

Do Not Backup Restricted-Use Data

Licenses shall not make routine or system backups (e.g., daily, weekly, incremental, partial, full) of restricted-use data except for the one backup copy of the entire restricted-use database. (Also see Section 3.4.) This restriction does not apply to backing up statistical computer syntax code used to analyze the restricted-use data.

Staff Changes

Change passwords accordingly when staff changes are made. Inform the IES Data Security Office of any staff changes via "Add User" or "Delete User" amendments (see Section 2.6).

Overwrite Hard Disk Data

Even after files are deleted from computer systems, the information remains in a form that can be recovered by various techniques. Active steps must be taken to prevent this possibility.

Overwriting new data in the file storage location makes the previous data unreadable. For example, various utilities such as WIPEINFO (Norton Utilities' Wipe Information) have an option that overwrites the selected files or disk areas with 0s. Overwriting is necessary when a computer containing restricted-use data is no longer used (e.g., reallocated to other projects), the computer needs to be repaired (e.g., hard disk crashes), or when the computer is to be reconnected to a network or LAN.

Note: The "delete" and "erase" commands remove the data's address, but not the data. The data remains on the hard disk until the computer needs the space for new data. When hard disks are reformatted, old data are not overwritten--the disk appears to be empty but the data are usually recoverable.

3.6 License User Training

Each user listed on the License, including the PPO and SSO, is required to complete a short online training course that covers the data security procedures and disclosure prevention measures required under the terms of the License. Users may log into the training through the NCES website, using the following web address:

<https://nces.ed.gov/statprog/licenseapp/CertificationLogin.asp>

Compliance with this training requirement is tracked through the online licensing database. Certificates of completion will be produced upon passing the knowledge check at the end of the training program. These certificates should be printed and included in the License file for each user. Each person listed on the License (with the sole exception of the Senior Official) must complete this training once per calendar year.

Chapter 4: On-Site Inspections

The License authorizes representatives of IES to make unannounced and unscheduled inspections of the licensee's facilities, including any associated computer center, to evaluate compliance with the terms of the License and security procedures.

4.1 On-Site Inspection Procedures

Under the provisions of the License, IES may conduct **unannounced** and **unscheduled** inspections of the License site to assess compliance with the terms of the License.

Specifically, an IES-authorized security inspector will visit the licensee's facilities to evaluate compliance in the following two areas, which are explained in detail in this section:

- Operational Procedures
- Security Procedures and Security Plan

Appendix K contains the On-Site Inspection Guideline.

License Procedures

The IES inspector will review the project operations with the PPO, or the Senior Official, at the licensee's facility. This review will focus on the agreements set forth in the actual License (or Memorandum of Understanding).

This includes an inspection of the current status of the project:

- **Record of License.** The IES inspector will review the licensee's file for a copy of the License, along with copies of all of the Affidavits of Nondisclosure and a list of persons authorized to access the data.
- **Affidavits of Nondisclosure.** The IES inspector will review the names and status of all project personnel. All project personnel must have an executed **Affidavit of Nondisclosure** on file with IES. This review is to confirm that IES has the most current information on file for those individuals who have the authority to access the subject data.
- **The Project Staff.** The IES inspector will determine whether a copy of the License and a copy of the Security Plan Form have been reviewed by all members of the project staff. This is to ensure that all members of the project team are aware of the procedures required for accessing and securing restricted-use data.

Security Procedures and Security Plan Form

The IES inspector will review with the licensee all aspects of the licensee's security procedures for the restricted data. These procedures are documented in the Security Procedures (see Chapter 3).

The IES inspector will also review the licensee's submitted Security Plan Form, which is the on-site implementation document for the security procedures.

The IES inspector will review these procedures for compliance. A basic outline of these procedures, in the **On-Site Inspection Guideline**, is presented in the next section below.

4.2 On-Site Inspection Guideline

The **On-Site Inspection Guideline** in Appendix K presents a standard set of questions that will be asked by the IES inspector when performing an on-site inspection. Since this is a guide, more License-specific questions may be asked on a case-by-case basis.

The **On-Site Inspection Guideline** are provided here to ensure consistency among interviews and to ensure that all appropriate questions and topics are covered during the interview. A basic outline of the topics covered in the inspection guideline is:

- [License Information and Procedures](#)
- [Physical Security Requirements](#)
- [Computer Security Requirements](#)
- [Conclusion of the Inspection](#)

See Appendix K (<http://nces.ed.gov/statprog/rudman/k.asp>) for more information.

The on-site inspection will also include a tour of the licensee's secure project office.

4.3 Violations, Penalties, and Prosecution

Violations

- **Statement of Warning.** If IES finds the licensee to be in noncompliance in a manner that has not yet resulted in unauthorized disclosure, IES will send a Statement of Warning to the Senior Official within six weeks (30 working days) of the on-site inspection. (More serious violations may result in License revocation or criminal prosecution. See below.)

The licensee has one month (20 working days) from receipt of the Statement of Warning to provide IES a letter detailing what procedures have been implemented to restore compliance.

- **Revocation of License.** As stated in the License (Section IV, Penalties) any violation of the terms and conditions contained in the License may subject the licensee to immediate revocation of the License by IES. If violations are discovered, IES will notify the licensee, in writing, of the factual basis and grounds for revocation.

The licensee has six weeks (30 working days) to submit a written argument and evidence to IES indicating why the License should not be revoked. The IES Data Security Program shall provide written notice of a decision to the licensee within nine weeks (45 working days) after receipt of the licensee's written argument. IES may extend this time period for good cause.

List of Most Common Violations

- No three to five minute shutdown when the computer is left on
- Lack of warning statement when restricted-use data are brought up on the screen

- Accessing restricted-use data from an off-site location
- The PPO not maintaining control over the restricted-use data
- The PPO neglecting to inform the IES Data Security Office of any project personnel changes
- Neglecting to return restricted-use data to the IES Data Security Office
- Neglecting to destroy all subsets of the data at the end of the project (the IES Data Security Office must be informed that this has taken place via completion of the License Close-Out Certification Form)
- Restricted-use data leaving the licensed site
- Making a copy of the restricted-use data and allowing it to leave the licensed site
- Removing the warning label with the expiration date from the restricted-use data
- Not labeling any copies or sub-sets of the data with the warning label
- Not restricting access to the secure project office to License users only

Prosecution and Penalties

Alleged violations of the Privacy Act of 1974 or IES-specific laws are subject to prosecution by the United States Attorney after first making reasonable efforts to achieve compliance.

Any violation of this License may also be a violation of federal criminal law under the Privacy Act of 1974, 5 U.S.C. 552a, and may result in a misdemeanor and a penalty of up to \$5,000.

Anyone violating the confidentiality provisions of Section 183 of the Education Sciences Reform Act of 2002 (P.L. 107-279), or making an unauthorized disclosure, when using the data shall be found guilty of a *class E felony* and can be *imprisoned up to five years*, and/or *fined up to \$250,000*.

Penalties, fines and imprisonment, may be enforced for each occurrence of a specific violation.

Appendix A: Definition of Terms

The following are definitions of terms associated with access to restricted-use data and that are used within this manual.

Access

The legal term for the right accorded to a licensee to see and utilize the individually identifiable information in a database.

Affidavit of Nondisclosure

A one-page form that is completed by any person who may have access to individually identifiable information. This form contains: (1) the name of the database(s) to be accessed, (2) the wording of an oath not to disclose such information to persons not similarly sworn, (3) a description of the penalties for such disclosure, and (4) the imprint of a notary public.

Application

A document that is completed by a person who is requesting access to individually identifiable information. It specifies the uses to which the data will be put and the agreement to abide by all security requirements imposed by the IES Data Security Office.

Disclosure

The availability or release of a record to anyone other than the subject individual unless duly authorized by License document and Affidavit.

Individually Identifiable Information

Refers specifically to data from any list, record, response form, completed survey, or aggregation about an individual(s) from which information about particular individuals or their schools/education institutions may be revealed by either direct or indirect means.

License

This is a general term that applies to a document that is utilized by the Agency to authorize access to a database, or a subset of a database, containing individually identifiable information. The "License" specifies the obligations imposed on the licensee and the procedures that must be followed in the maintenance of that database. There are three different instruments utilized as Licenses: (1) License, (2) Memorandum of Understanding, and (3) Agency Contract.

Maintain

To collect, store, use or have available for dissemination when used in connection with the term "record"; and, to have control over or responsibility for a system of records when used in connection with the term "System of Records."

Personal/Individual Identifier

An identifying element associated with an individual, including the individual's name, or Social Security number, any identifying particular assigned to the individual (fingerprint, voiceprint, photograph), or any other identifying number, symbol, unique retriever, or coding device which is assigned to or directly correlates with the individual.

Principal Project Officer (PPO)

The PPO is the researcher in charge of the day-to-day operations involving the use of the subject data and is responsible for liaising with the IES Data Security Office.

Professional/Technical Staff (P/TS)

The P/TS conduct the research, or conduct any analysis, for which the License is issued. Only seven (7) P/TS per License may have password access to subject data unless the IES Data Security Office provides written authorization for a larger number of P/TS. P/TS also includes any non-security/police personnel that have key access to the designated secure project office.

Public Use

This describes any data that are disseminated through IES and are publicly available without restriction. These are survey data that have been coded, aggregated, or otherwise altered to mask individually identifiable information and thus are available to all external users.

Restricted-Use

This is a descriptor of any data set that contains individually identifiable information that is confidential and protected by law. Special procedures are taken to protect this information, and it can be issued only to licensees on loan.

Routine Use

The description in the Privacy Act of 1974 of the permissible uses of individually identifiable information in a system of records. Except for the use of data for statistical purposes, these routine uses are not permitted for agency databases.

Senior Official (SO)

The SO is the individual who has the authority to bind the organization to the License. The SO is responsible for signing the License, and with his/her signature certifies that: (1) the organization has the authority to undertake the commitments in the License, (2) he/she has the authority to bind the organization to the provisions of the License, and (3) the Principal Project Officer (PPO) is the researcher who has the authority to manage the day-to-day operations of the License.

Subject Data

These are all data containing individually identifiable information collected by, or on behalf of, the Agency that are provided to the licensee and are protected under the terms presented in the executed License. This includes all data/information derived from these data.

Support Staff

In addition to the P/T staff already mentioned, support staff would include any secretaries, typists, computer technicians, and messengers who potentially may have access to the subject data. The licensee may disclose subject data to support staff who come in contact with the subject data in the course of their duties only to the extent necessary to conduct the research under the License.

System of Records

A system of records is any group of records under the control of a federal agency or its contractors from which information may be retrieved by the name of the individual, or by some identifying number, symbol, or other personal identifier. The maintenance of a system of records is published by a notice in the Federal Register. Single records or groups of records which are not retrieved by a personal identifier are not part of a system of records. Papers maintained by individual employees of the Agency which are prepared, maintained, or discarded at the discretion of the employee and which are not subject the Federal Records Act (44 U.S.C. 2901) are not part of a system of records, provided that such personal papers are not permitted to be accessed or reviewed by persons not sworn to confidentiality.

System Security Officer

The SSO is the person responsible for maintaining the day-to-day security of the licensed data. The SSO's assigned duties shall include the implementation, maintenance, and periodic update of the security plan to protect the data in strict compliance with statutory and regulatory requirements.

Appendix B: Public-Use Data

National Center for Education Statistics (NCES)

The Institute of Education Sciences (IES) produces and disseminates a wide variety of publications. Their content ranges from survey documents that present little more than tabular data to sophisticated studies that present more complex analysis of raw data. The analysis documents tend to contain more textual information with occasional tabular data or graphic presentations.

The NCES website (<http://nces.ed.gov>) provides access to a wide range of publications and data sets about education in the United States and other nations. The NCES Electronic Catalog (<http://nces.ed.gov/pubsearch/>) can be used to locate both individual publications and data products, and groups of publications and data products for specific data collections.

For more information, see: <http://nces.ed.gov/statprog/rudman/b.asp>.

Appendix C: Privacy Act of 1974

The full text of the Privacy Act of 1974 can be found at:
<http://nces.ed.gov/statprog/rudman/c.asp>.

Appendix D: Agency-Specific Laws

Education Sciences Reform Act of 2002 (Public Law 107-279; codified as 20 U.S.C. 9573) -

SEC. 183. CONFIDENTIALITY.

- a. IN GENERAL- All collection, maintenance, use, and wide dissemination of data by the Institute, including each office, board, committee, and center of the Institute, shall conform with the requirements of section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. 1232g, 1232h).
- b. STUDENT INFORMATION- The Director shall ensure that all individually identifiable information about students, their academic achievements, their families, and information with respect to individual schools, shall remain confidential in accordance with section 552a of title 5, United States Code, the confidentiality standards of subsection (c) of this section, and sections 444 and 445 of the General Education Provisions Act (20 U.S.C. 1232g, 1232h).
- c. CONFIDENTIALITY STANDARDS-
 1. IN GENERAL-
 - A. The Director shall develop and enforce standards designed to protect the confidentiality of persons in the collection, reporting, and publication of data under this title.
 - B. This section shall not be construed to protect the confidentiality of information about institutions, organizations, and agencies that receive grants from, or have contracts or cooperative agreements with, the Federal Government.
 2. (2) PROHIBITION- No person may--
 - A. use any individually identifiable information furnished under this title for any purpose other than a research, statistics, or evaluation purpose;
 - B. make any publication whereby the data furnished by any particular person under this title can be identified; or
 - C. permit anyone other than the individuals authorized by the Director to examine the individual reports.
- d. ADMINISTRATION-
 1. IN GENERAL-
 - A. DISCLOSURE- No Federal department, bureau, agency, officer, or employee and no recipient of a Federal grant, contract, or cooperative agreement may, for any reason, require the Director, any Commissioner of a National Education Center, or any other employee of the Institute to disclose individually identifiable information that has been collected or retained under this title.
 - B. IMMUNITY- Individually identifiable information collected or retained under this title shall be immune from legal process and shall not, without the consent of the individual concerned, be admitted as evidence or used for any purpose in any action, suit, or other judicial or administrative proceeding.

- C. APPLICATION- This paragraph does not apply to requests for individually identifiable information submitted by or on behalf of the individual identified in the information.
2. EMPLOYEE OR STAFF VIOLATIONS- Whoever, being or having been an employee or staff member of the Department, having taken or subscribed the oath of office, or having sworn to observe the limitations imposed by subsection (c)(2), knowingly publishes or communicates any individually identifiable information (as defined in paragraph (5)(A)), the disclosure of which is prohibited by subsection (c)(2), and that comes into such employee or staff's possession by reason of employment (or otherwise providing services) under this title, shall be found guilty of a class E felony and imprisoned for not more than five years, or fined as specified in section 3571 of title 18, United States Code, or both.
 3. TEMPORARY STAFF- The Director may utilize temporary staff, including employees of Federal, State, or local agencies or instrumentalities (including local educational agencies), and employees of private organizations to assist the Director in performing the Director's responsibilities, but only if such temporary staff are sworn to observe the limitations imposed by this section.
 4. INFORMATION REQUIREMENTS- No collection of information or data acquisition activity undertaken by the Director shall be subject to any review, coordination, or approval procedure except as required by the Director of the Office of Management and Budget under the rules and regulations established pursuant to chapter 35 of title 44, United States Code, except such collection of information or data acquisition activity may be subject to review or coordination if the Director determines that such review or coordination is beneficial.
 5. DEFINITIONS- For the purposes of this section--
 - A. the term 'individually identifiable information' means any record, response form, completed survey, or aggregation thereof from which information about particular individuals may be revealed; and
 - B. the term 'report' means a response provided by or about an individual to an inquiry from the Director and does not include a statistical aggregation from which individually identifiable information cannot be revealed.
 6. VIOLATIONS- Any person who uses any data provided by the Director, in conjunction with any other information or technique, to identify any individual student, teacher, administrator, or other individual and who knowingly discloses, publishes, or uses such data for a purpose other than a statistical purpose, or who otherwise violates subparagraph (A) or (B) of subsection (c)(2), shall be found guilty of a class E felony and imprisoned for not more than five years, or fined as specified in section 3571 of title 18, United States Code, or both.
 7. ACCESS TO REPORTS OR RECORDS- Nothing in this section shall restrict the right of the Secretary, the Comptroller General of the United States, the Director of the Congressional Budget Office, and the Librarian of Congress, to gain access to any reports or other records, including information identifying individuals, in the Director's possession, except that the same restrictions on disclosure that apply under paragraphs (1) and (6) shall apply to such individuals.

e. INVESTIGATION AND PROSECUTION OF TERRORISM-

1. IN GENERAL- Notwithstanding subsections (c) and (d), the Attorney General (or any Federal officer or employee, in a position not lower than an Assistant Attorney General, designated by the Attorney General) may submit a written application to a court of competent jurisdiction for an ex parte order requiring the Secretary to permit the Attorney General (or his designee) to--
 - A. collect reports, records, and information (including individually identifiable information) in the possession of the center that are relevant to an authorized investigation or prosecution of an offense listed in section 2332b(g)(5)(B) of title 18, United States Code, or an act of domestic or international terrorism as defined in section 2331 of that title; and
 - B. for official purposes related to the investigation or prosecution of an offense described in paragraph (1)(A), retain, disseminate, and use (including as evidence at trial or in other administrative or judicial proceedings) such information, consistent with such guidelines as the Attorney General, after consultation with the Secretary, shall issue to protect confidentiality.
2. APPLICATION AND APPROVAL-
 - A. IN GENERAL- An application under paragraph (1) shall certify that there are specific and articulable facts giving reason to believe that the information sought is described in paragraph (1)(A). (B) The court shall issue an order described in paragraph (1) if the court finds that the application for the order includes the certification described in subparagraph (A).
3. PROTECTION- An officer or employee of the Department who, in good faith, produces information in accordance with an order issued under this subsection does not violate subsection (d)(2) and shall not be liable to any person for that production.

Appendix E: Memorandum of Understanding

The latest version of the Memorandum of Understanding (MOU) for federal agency access to restricted-use data is at: <http://nces.ed.gov/statprog/rudman/e.asp>.

Appendix F: License Document

The latest version of the License document is available at:
<http://nces.ed.gov/statprog/rudman/f.asp>.

Appendix G: Affidavit of Nondisclosure

The latest version of the Affidavit of Nondisclosure form is at: <http://nces.ed.gov/statprog/rudman/g.asp>.

Appendix H: Restricted-Use Databases

NCES Restricted-Use Databases

National Center for Education Statistics survey data cover educational assessment from the elementary/secondary level to the college level. The surveys focus on many different aspects of the welfare of education in the nation, tracking individuals through their educational program and assessing the well-being of education within the United States.

These are the three broad survey areas:

- **Elementary/Secondary Education**
- **Postsecondary Education**
- **National Assessment of Educational Progress**

The data that are collected from these survey efforts are analyzed and presented in many reports and documents. Research efforts are conducted both internally by the Department of Education, within NCES, and also by external educational researchers.

For a brief description of the current NCES survey databases that contain individually identifiable information, see: <http://nces.ed.gov/statprog/rudman/h.asp>. Restricted-use data availability can be found through the NCES Electronic Catalog (<http://nces.ed.gov/pubsearch/>).

Appendix I: Availability of Restricted-Use Data

Restricted-use data availability can be found at: <http://nces.ed.gov/statprog/rudman/i.asp> and through the NCES Electronic Catalog at: <http://nces.ed.gov/pubsearch/>.

Appendix J: Security Plan Form

The latest version of the Security Plan Form is at: <http://nces.ed.gov/statprog/rudman/j.asp> .

Appendix K: On-Site Inspection Guidelines

The latest version of the On-site Inspection guidelines are at:
<http://nces.ed.gov/statprog/rudman/k.asp> .

Appendix L: E-Government Act of 2002

E-Government Act of 2002, Title V, Subtitle A, Confidential Information Protection

The text of this law can be found at: <http://nces.ed.gov/statprog/rudman/l.asp> .

Appendix M: Close-out Certification Form

The latest version of the Close-out Certification Form is at:

<http://nces.ed.gov/statprog/rudman/m.asp>

The document is available as a downloadable Acrobat PDF file.