Restricted-Use Data Procedures Manual

Institute of Education Sciences
National Center for Education Statistics
IES Data Security Program
U.S. Department of Education
1990 K Street, NW
Washington, DC 20006-5574

Acrobat PDF Version March 2007

Publication Information

U.S. Department of Education
Margaret Spellings
Secretary

Institute of Education Sciences
Grover J. Whitehurst
Director

National Center for Education Statistics
Mark Schneider
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
1990 K Street, NW
Washington, DC 20006-5574

The NCES World Wide Web Home Page is: **http://nces.ed.gov**

Printed April 1996 (NCES publication number: 96860rev)
Reprinted October 1999
Acrobat PDF Version March 2007

Contact the IES Data Security Program: 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 Security Procedures.
- The licensee is responsible for all terms and provisions presented within those two documents.
- 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 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

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 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. It is 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 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*.
- E-Government Act of 2002 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.
- 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.
- 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. A confidentiality violation 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, a research institution). To qualify, an organization must submit:

- a Formal Request through 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
- the Security Plan Form (see Appendix J).

Security Procedures

Restricted-use data must be SAFE at all times. SAFE means that the data are secure from unauthorized disclosure in accordance with the license and specified Security Procedures. The

Security Procedures described in chapter 3 include the computer security requirements for the standalone Computer SAFE model.

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 provisions of the license, the Security Procedures, and the Licensee's security plan. The inspection procedures are described in chapter 4.

Chapter 1: Laws

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."

1.1 Basic Statutes

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

- Privacy Act of 1974,
- Computer Security Act of 1987,
- Education Sciences Reform Act of 2002,
- USA Patriot Act of 2001, and
- E-Government Act of 2002

1.2 Privacy Act of 1974

This 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 limits the uses to which one may put the data. (For the full text of the law, see Appendix C.)

Privacy Standards
Under the direction of the Office of Management and Budget, key Federal agencies issue policies, standards, and guidelines for protecting personal data.

Computer Security Guideline
A key standard 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 adequately protected in accordance with Federal statutes and regulations.

1.3 Computer Security Act of 1987

The Computer Security Act of 1987, Public Law (P.L.) 100-235, dated January 8, 1988, requires each Federal agency to identify all Federal computer systems that contain sensitive information and implement security plans to protect these systems. The Computer Security Act defines the term "sensitive information" as any unclassified information, which could adversely affect the:

- national interest,
- conduct of Federal programs, or
- privacy to which individuals are entitled under the Privacy Act of 1974.

Agencies are required to protect this information against loss, misuse, disclosure or modification.

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. IES' complete 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 the pledge of confidentiality must be kept confidential and may only be used for statistical purposes. Any willful disclosure of such information for nonstatistical purposes, without the informed consent of the respondent, is a class E felony.

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.[1]

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.

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

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.

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 documents:

- 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 publications based on the data be sent to IES,
- 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 the Data Security Program log book when obtaining 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 inhouse staff needing access to restricted-use data must request and obtain clearance through the Data Security Program.
- Staff must sign the Data Security Program's log book when obtaining the data.
- Staff who have restricted-use data must keep it under lock and key. These data may not be stored on a computer and the data files cannot be left open when not in use. (See chapter 3, Security Procedures, for full details.)
- The data may not be removed from the office area without clearance from the Data Security Program.
- These restricted-use data **must** be returned to the Data Security Program prior to the departure of an employee or Fellow from IES. IES staff should refer all requests for licensing documents, affidavits, or restricted-use data to the Data Security Program. These requests are not 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 actual sample 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 Data Security Program. The COTR must also obtain an executed Affidavit of Nondisclosure from all persons outside the IES who will review the survey design and will have access to these sampling data. COTRs will forward all original Affidavits of Nondisclosure to the Data Security Program.

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 obtained to perform work for IES must submit a formal, written request. (See section 2.4.) If the purpose of the independent research is different from the purpose for using the data stated in the contract, the contractor must follow the standard application process for obtaining a license.

2.4 Applying for a License

These are the current standard licensing procedures for the authorization of external use of restricted-use data.

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

- Formal Request through NCES' electronic 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).

Applicants are to prepare, complete and return the signed License, notarized Affidavits, and the Security Plan Form.

Mail all correspondence, **signed by the Principal Project Officer (PPO) and not by a staffer**, to the IES Data Security Program.

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

- In the Formal Request, you must demonstrate that the proposed research project meets the basic requirements, and the Restricted Use Data Security Plan Form is complete and complies with the Security Procedures outlined in chapter 3.
- All questions IES has about an organization's application must be resolved in writing prior to the formal granting of the license.

The original license document is only **submitted for final IES approval** when all required information has been received and the license application is complete.

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 projects that are deemed necessary.

The decision to grant a license is solely that of the Director. The authority granted in the license becomes effective on the date of the Director's signature.

The **Formal Request** will ask for specific items of information. Your information will be collected through IES' electronic application system at: http://nces.ed.gov/StatProg/instruct.asp .

Formal Request Checklist	✓
(1) The title of the database(s) the organization wants to access;	
(2) A description of the statistical research project necessitating access to the restricted-use database;	
(2) The name and title of the Senior Official;	
(4) The name and title of the Principal Project Officer(s);	
(5) The name and title of the System Security Officer;	
(6) The names and titles of the professional/technical and support staff; and	
(7) The estimated loan period (not to exceed five years).	

The Formal Request requirements are described in more detail:

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

(2) A description of the statistical research project that necessitates accessing the survey database. 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, or 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).

(3) The name and title of the Senior Official having the authority to legally bind the organization to the provisions of the license.

(4) The name and title of the Principal Project Officer(s) 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 liaison with the IES Data Security Program.)

(5) The name and title of the Systems Security Officer(s) who will oversee the security of the data.

(6) The names and titles of the professional/technical and support staff who will be accessing the survey 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 Program. Written documentation authorizing the exception must be obtained from IES. (Requests for data or amendments to an existing license will only be accepted from the PPO.)

(7) The estimated loan period necessary for accessing the survey 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.

An executed **License Document** is a legally binding agreement.

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.	
Send the original signed license to the IES Data Security Program.	

An **Affidavit of Nondisclosure** must be executed for each person who may have data access.

Affidavit of Nondisclosure Checklist	✓
Obtain a notarized Affidavit of Nondisclosure from each employee and sub-contractor staff who may come in contact with the subject data.	
Fill in **all** requested information on the Affidavit.	
Send the original signed and notarized Affidavits of Nondisclosure to the IES Data Security Program.	

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 Program. IES allows **up to seven (7) individuals per project** to access the subject data. (IES may require that the supervisor of the applicant organization's computer facilities be one of those seven.)

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 "**survey-specific"**: they are only valid for the survey(s) listed on the form. **Include all surveys and all subsequent followups that will be needed**; for example, "the base year survey and all subsequent followups."

Notarized documents cannot be amended by IES. To access a followup of a listed survey or to access a survey that was not listed on the notorized affidavit, another affidavit must be executed. Organizations must promptly notify IES of **any changes in project staff**. (See section 2.6, Amending a License.)

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 Program.	

Restricted-use data must be kept SAFE at all times. SAFE means 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. Federal agencies do not need to submit the Security Plan Form. Federal agencies must adhere to the security requirements set forth in the MOU.

Receiving the Requested Materials

Final Product Package Contents	✓
The new Licensee receives the final product package, including	
• a copy of the original license,	
• copies of the Affidavits of Nondisclosure, and	
• **database** media materials and instructional materials to assist the project staff in the use of the data. Materials accompanying data files include - (1) Warning/Restriction Labels (attached to all enclosures) (2) Loan Expiration Date (attached to all enclosures)	

The package is sent **Restricted Delivery - Certified Mail** to the Licensee.

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 communicated from the licensee's site.

2.5 Required Licensee Activity

The Licensee is responsible for all terms and provisions in the License document and related materials, including the Security Procedures. (See the appropriate license document in Appendix E or F for full requirements.)

This section addresses three of the major administrative requirements-maintaining the License file, with copies of the Executed Affidavits, and submitting research publications-**and the Licensee's responsibility to be ready for inspection at all times**.

The security requirements are explained in detail in chapter 3.

Maintaining the License File
The Licensee's Principal Project Officer (PPO) is accountable for having all pertinent information in this file.

License File Checklist	✓
The Licensee shall maintain a license file at the same facility where the Licensee stores the restricted-use data. The file is to contain the following items:	
• copies of emails you received from the IES Data Security Office;	
• the license and its attachments - (1) a description of research, (2) the Privacy Act of 1974 (5 U.S.C. 552a), IES-specific laws, and (3) Security Procedures;	
• any amendments to the license document;	
• a current list of all individuals who may have access to the data, along with copies of their notarized Affidavits of Nondisclosure; and	
• a copy of the Licensee's submitted Security Plan Form.	
All project staff shall both **READ** and **UNDERSTAND** this material. All individuals who may have access to the subject data must be fully aware of the required security precautions and procedures. (This is the Principal Project Officer's responsibility.)	

Submitting Research Publications
If the Licensee intends to publish any information that would include unweighted sample size numbers, Licensee must submit an advance copy of the document to the IES Data Security Program prior to its publication. Otherwise, the Licensee shall submit to the IES Data Security Program a copy of the final version of each publication or any other data product containing information based on subject data.

Research Publication Checklist	✓
The PPO shall forward a final copy of each publication containing information based on restricted-use data to the IES Data Security Program. If the PPO suspects a publication might disclose individually identifiable information, **the PPO must forward an advance (before public release) copy of that publication to IES for review** and delay public release until formally notified by IES that no potential disclosures were found. For example, any proposed publication that contains any unweighted sample size numbers must be submitted to IES for a disclosure review prior its public release. (IES generally clears all publications within a week.) When tabulations are produced, any table having a cell with 1 or 2 unweighted cases must be recategorized to insure that each cell in the table has at least 3 unweighted cases. This rule excludes table cells with zero cases because there are no data to protect in the cell.	

Passing On-Site Inspections
The license (section IV.G) gives IES Data Security Officials the right to conduct **unannounced, unscheduled** inspections of the Licensee's site 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, On-Site Inspections, and a copy of the On-Site Inspection Guideline can be found in appendix K.

Any violation 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	✓
If an on-site inspection is conducted, IES will provide formal notification of any violations in the required security procedures.	
• Correct all identified security violations.	
• Licensee must notify IES in writing of the corrective measures.	

Outside Requests for Data
The Licensee shall notify IES immediately when it receives any legal, investigatory or other demand for subject data, including any request or requirement to provide subject data to any State agency or State contractor, and shall keep a record of how the matter was resolved.

2.6 Amending a License

IES shall be kept informed of any modifications in project operations throughout the span of the loan period.

To change any of the terms and conditions agreed upon in the license, the Licensee shall submit a request to the IES Data Security Program. (Including the license number will result in faster turnaround.)

All correspondence must be initiated by the principal project officer (or the senior official in the PPO's absence).

Addition to Project Staff Checklist	✓
Notify IES of any additions to project staff.	
Include the notarized Affidavit(s) of Nondisclosure for the additional staff with the letter requesting an amendment.	
The IES response letter accepting (or rejecting) the proposed amendment is to be kept in the License's file.	

Reduction of Project Staff Checklist	✓
Notify IES of any reductions in project staff.	
Affidavits of personnel withdrawn from the project shall be marked "VOID," or destroyed.	
The IES response letter or e-mail accepting the proposed amendment is to be kept in the Licensee's file.	

When informed that a Licensee staff person is no longer accessing the restricted-use data, the Data Security staff will mark that person's Affidavit of Nondisclosure "VOID."

Requesting an Additional Database
A Licensee may request access to another database in addition to what was agreed upon in the original license.

If the database request can be accommodated under the same licensing instrument, then the applicant need only submit the following information to IES:

Requesting an Additional Database Checklist	✓
(1) The title of the survey(s) requested	
(2) A description of the research purpose which necessitates accessing the restricted-use data, and	
(3) The names of the personnel who will have access to the database. (Include executed Affidavits for any staff who do not have the additional database listed on their original Affidavits.)	

The Data Security Program will review the request. If judged complete, the request for an additional database will be included in the Licensee's file as an amendment to the license instrument and the database will be sent.

2.7 Closing-Out the License Period

Closing-Out Checklist	✓
Notify IES in writing that the project necessitating use of the data has been completed.	
Return the original subject data to IES by certified mail.	
Return any additional database materials and documentation to IES.	
Destroy all hard copy versions of subject data and purge all electronic versions, including all copies and subsets, from any computer system used in analysis.	

The Licensee shall return to IES, **by certified mail**, the data product containing the original subject data and any additional materials and documentation.

The Licensee shall also **overwrite** the subject data on any computer system used in analysis; that is, totally obliterate erased (deleted) data so that it cannot be recovered by any means. One method would be to use the Norton Utility WIPEINFO, which can be used on single files or entire disks.

2.8 Applicant/Licensee Record

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

ACTIVITY	✓
REVIEW REQUIRED PROCEDURES	
Obtain a copy of the *Restricted-Use Data Procedures Manual*.	
Review the manual.	
APPLYING FOR A LICENSE	
Submit the following to the IES Data Security Program (through the electronic application system at: http://nces.ed.gov/StatProg/instruct.asp) -	
Formal Request:	
(1) Title of survey(s).	
(2) 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 survey was conducted.	
(3) Name and title of the Senior Official.	
(4) Name and title of the Principal Project Officer(s).	
(5) Name and title of the Systems Security Official.	
(6) Names and titles of the professional/technical staff.	
(7) Estimated loan period (not to exceed five years).	

Send the following three items to the IES Data Security Program:	
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 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 facility, copies of:	
(1) Emails received from the IES Data Security Office,	
(2) The **License Document** and its three attachments,	
(3) **Amendments** to the license document,	
(4) All executed **Affidavit(s) of Nondisclosure**, and	
(5) Licensee's submitted **Security Plan Form**.	
All project staff must know where these documents are kept.	
Submitting Research Publications	
(1) Forward to IES for review an advance (before public release) copy of each publication that might disclose individually identifiable information. [IES will formally notify the Licensee of acceptance of the publication (i.e., no security violations 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 in the security procedures.	
(2) All identified security violations must be corrected.	
(3) Licensee must notify IES in writing of the corrective security measures.	
AMENDING A LICENSE	
Licensee must notify IES if there have been any changes to the conditions of the license.	
(1) IES must be notified of new and/or departing project personnel.	
(2) New personnel must complete Affidavits of Nondisclosure; those of departing personnel must be destroyed or otherwise canceled.	
(3) Changes in project purpose or product require a contract amendment approved by IES.	
(4) Changes in, or additions to, licensed database(s) require a contract amendment approved by IES.	

CLOSING-OUT THE LICENSE PERIOD	
(1) Formally notify IES when the data project is completed.	
(2) Return the original subject data to IES by certified mail.	
(3) Return any additional data materials and documentation to IES (if applicable).	
(4) Double check that a final copy of each publication containing information based on restricted-use data has been sent to IES.	
(5) Destroy all hard copy versions of the subject data and purge all traces of the subject data, including all copies and subsets, on any computer system used in analysis.	

Review
IES will review the submitted License document and supporting documentation for content and completeness. If all requirements have been met, the requested materials will be sent to the new Licensee.

Under no circumstances may the database be removed or communicated from the Licensee's site (as described in the Security Plan form).

Chapter 3: Security Procedures

IES shall ensure that all personally identifiable information remain **confidential**, in accordance with the Privacy Act of 1974.

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

- Privacy Act of 1974: Defines, and provides for the security and privacy of, personal data maintained by the Federal Government.
- 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.
- 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

- 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 SAFE at all times. SAFE means 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 access to data
- Use data at licensed site only
  - Who-affidavit signers only
  - What type access-read only
  - Which data-listed on affidavit
- Return original data to IES

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

- Protect machine-readable media/printed material
  - Store securely
  - Label/catalog/track
- 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 SAFE.

Licensees must meet the spirit and intent of these protection requirements to ensure a SAFE environment 24 hours a day for the 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. Federal agencies do not need to submit the Security Plan Form . Federal agencies must adhere to the security requirements set forth in the MOU.
The SO, PPO, and SSO shall sign the implemented security plan and provide a copy to IES.

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**) 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 staff member 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. This includes using data **at home** or providing it 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 under IES supervision or by approved IES procedures.

3.4 Physical Handling, Storage, and Transportation

Protect Machine-Readable Media and Printed Material
Machine-readable media storage devices include, but are not limited to, tapes, CD-ROMs, floppy diskettes, and removable hard disks.

Note: Data stored on fixed hard disks are addressed in section 3.5 in Standalone Computers.
Lock Up Media. Subject data on machine-readable media shall always be secured from unauthorized access (e.g., locked in a secure cabinet when not in use, only necessary copies made).

Label/Catalog/Track Media. To ensure that license dates are not exceeded, all portable media from NCES 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 possession of the data must hold an affidavit, 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 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. 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.

Restrict Copying of Data
Copying Restrictions. The Licensee is accountable for any copies of the subject data, or subsets, that are made. If the data are copied, the Licensee shall ensure that each copy is:

- Made only when **necessary** for performing the licensed statistical research;
- Protected at the same level as the original confidential data;
- Made available only to those persons authorized to access the subject data; and
- Destroyed upon completion of the purpose for which the copy was created.

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 Computer
A standalone computer is any single-user PC (e.g., running DOS or 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.

Standalone Computer Security Model

Estimated Risk: Safe
providing required security measures are adequately implemented

Minimum Security Requirements -

- **Laptop computers cannot be used**
- **Limit access room/area**
- **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

***If* security measures cannot be adequately implemented, *do not use this model for individually* identifiable information.**

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. When processing individually identifiable information on a standalone 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 computer cannot be connected to the LAN while subject data are on the system.

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, shutdown 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 shutdown, 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. Licensees 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 information extrapolated from the restricted-use data.

Staff Changes. Change passwords accordingly when staff changes are made.

Overwrite Hard Disk Data. Even after files are deleted from computer systems, the information remains in a form that can be recovered by various relatively simple techniques. Active steps must be taken to prevent this possibility. Overwriting writes new data in the file storage locations, thus making the previous data unreadable. For example, under DOS, 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 for an NCES project (e.g., reallocated to other projects) or when the computer needs to be repaired (e.g., hard disk crashes).

Note: The DOS "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. On hard disks, most versions of the DOS FORMAT command reinitialize the system area but does not overwrite the data area--the disk appears to be empty but the data are usually recoverable.

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 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, security officials 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 an On-Site Inspection Interview Guideline.

License Procedures
IES Data Security Officials will review the project operations with the Principal Project Officer, or the Senior Official, at the Licensee's facility. This review will focus on the agreements set forth in the actual license, memorandum of understanding, or Department of Education contract.

This includes an inspection of the current status of the project, as discussed below.

- **Record of License.** IES Security officials will review the Licensee's file for a copy of the license, along with copies of all of the Affidavits of Nondisclosure, or a list of persons authorized to access the data.
- **Affidavits of Nondisclosure.** IES Security officials will review the names and status of all project personnel. All project personnel must have an executed **Affidavit of Nondisclosure** or be authorized, and these original Affidavits must be on file at 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.** IES Security officials will investigate whether a copy of the license and a copy of the Security Procedures 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 restricted-use data.

Security Procedures and Security Plan Form
IES Data Security Officials 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).

IES Data Security Officials will also review the Licensee's submitted Security Plan Form, which is the on-site implementation document for the Security Procedures.

IES Data Security Officials will review these procedures for compliance. A basic outline of these procedures, in the form of 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 IES Data Security officials 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** is offered 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 guide follows.

- Introduction
- Risk Management
- General Security Requirements

  Assignment of Security Responsibilities
  Development and Implementation of Security Plan Form
  Restriction of Access to Data
  Use of Data at Licensed Site Only
  Return of Original Data to IES

- Physical Handling, Storage, and Transportation

  Protection of Machine-Readable Media and Printed Material
  Avoidance of Disclosure from Printed Material
  Restrictions on Copying of Data
  Restrictions on Methods of Transporting Data

- Computer Security Requirements

  Standalone Computer

The on-site inspection will include a tour of the Licensee's computer facilities.

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 Program of any project personnel changes
- Neglecting to return restricted-use data to the IES Data Security Program
- Neglecting to destroy all subsets of the data at the end of the project (the IES Data Security Program must be informed that this has taken place)
- 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

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 the access to restricted-use information 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 Agency.

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 the liaison with the Agency. The licensee shall disclose subject data to the PPO on the same basis as those data are disclosed to professional/technical and support staff.

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 may have password access to subject data unless the Agency provides written authorization for a larger number of P/TS.

Public Use
This describes any data that are disseminated through the Agency, 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 licensee.

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
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 . The MOU is available at this website as HTML or as a downloadable Acrobat PDF file.

Appendix F: License Document

The latest version of the License Document is available at: http://nces.ed.gov/statprog/rudman/f.asp . The License Document is available at this website as HTML or as a downloadable Acrobat PDF file.

Appendix G: Affidavit of Nondisclosure

The latest version of the Affidavit of Nondisclosure form is at: http://nces.ed.gov/statprog/rudman/g.asp . The Affidavit of Nondisclosure form is available at this website as HTML or as a downloadable Acrobat PDF file.

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.

Following are general descriptions of the current NCES survey databases that contain individually identifiable information, but that are available under the Privacy Act of 1974 and the National Education Statistics Act of 1994, as amended. Each database description serves to define the purpose(s) for which the survey data were collected.

For a fuller description, 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 . The Security Plan Form is available at this website as HTML or as a downloadable Acrobat PDF file.

Appendix K: On-Site Inspection Guideline

The latest version of the On-site Inspection Guideline document is at: http://nces.ed.gov/statprog/rudman/k.asp . This Guideline document is available at this website as HTML or as a downloadable Acrobat PDF file.

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 .