

Standard Operating Procedures 3130.1
Rules of Behavior in Using Computing Systems
April 14, 2010

I. PURPOSE

Recent changes to federal security laws requires us to notify users of the Census Bureau computing systems about Rules of Behavior in using Census Bureau computing systems, and to obtain a signed form from the state partners under the Local Employment Dynamics (LED) partnership. This standard operating procedure (SOP) describes the background and provides a standard form for completing the requirement.

II. BACKGROUND

Two types of servers impact the LED state partners – the Internet web server for <http://lehd.did.census.gov> and the FTP server used for file transfers.

The following two pages describe the Rules of Behavior. The last page is a standard form for each state partner to complete, sign, and return to LED.

III. PROCEDURES

- a. Read the following Rules of Behavior for Internet Access by State Partners to LEHD Information Technology Systems Version 2010-04-14.
- b. Refer questions, if any, to did.local.employment.dynamics@census.gov.
- c. A state representative shall complete and sign the standard form on the last page.
- d. Return the completed form to did.local.employment.dynamics@census.gov or by express mail to the contact located at <http://lehd.did.census.gov/led/about-us/contact.html>.

IV. POINTS OF CONTACT

Program Manager (301)-763-8303 CES.Local.Employment.Dynamics@census.gov

Rules of Behavior for Internet Access by State Partners to LEHD Information Technology Systems Version 2010-04-14

Instructions to readers and signers

Please read, and sign the last page.

Return the signed page to LEHD by express mail to

U.S. Census Bureau
CES/LEHD Program
Attn: Holly Brown
Room 5K166C
4600 Silver Hill Rd
Suitland, MD 20746

Or scan and send signed page as an attachment of an email to

CES.Local.Employment.Dynamics@census.gov

Or fax to:

(301)-763-9473

Rules of behavior, also referred to as acceptable use policy, instruct people about acceptable ways in which they may and may not use information technology (IT) systems. These rules communicate to every individual accessing IT resources (including management, administrators, federal personnel, and contractors) their role in protecting those resources, and advise them of their obligations.

This document describes such rules for users accessing Census Bureau servers in connection with a data transaction otherwise regulated by a Memorandum of Understanding (MOU) between a State Partner and the LEHD Program at the U.S. Census Bureau.

Individual Accountability

Representatives of the State Partners are to be held individually accountable for their actions and may be subject to administrative penalties, fines, termination (removal), and/or imprisonment. The signatory to this agreement assumes responsibility for any employee or contractor transaction made on their behalf.

Data Stewardship

The Census Bureau collects and processes data from many different sources. Much of this data is sensitive in nature and is protected under the Privacy Act, Title 13, Title 26, and Title 42 of the U.S. Code. Title 5, which applies to the protection of personnel (i.e., Human Resources) data, is also found within the U.S. Code. This law makes the release of covered data a criminal act punishable by Federal Law. Therefore, the unauthorized use of sensitive data by employees and contractors is prohibited. *Sensitive data may not be transmitted in any form without the appropriate encryption.*

Instructions on how to encrypt data were transmitted to each State Partner, and signature of these Rules of Behavior signifies receipt and understanding of such instructions.

Good data stewardship requires full communication and cooperation between users and system owners. Users are to follow the instructions given by the system owners and administrators with respect to the handling of sensitive data, including restrictions on where on the system such data is to be stored.

Permission to access data is authorized on a need-to-know basis, and users should act in a manner that minimizes the likelihood of unauthorized access, by being aware of any restrictions on the use of data they are working with, and making sure that the access permissions on the files they own are consistent with these restrictions.

Government Computer Use

Use of government computers, communications systems, data, and other information is meant for authorized purposes. Unauthorized use of government equipment is prohibited.

State partners are given access to Census Bureau systems based on the need to perform the data transactions specified by the MOU. Users are requested to work within the confines of this access, and are not to attempt to access systems or applications to which access has not been authorized.

Users should understand that some data processing or system administration activities may have higher priority than their own data processing activities. System administrators will be sensitive to program activities when scheduling downtime. System administrators may from time to time ask some users to schedule their jobs differently in order to accommodate the requirements of other users with higher-priority tasks.

End-User Software Use

Users are not allowed to install any software.

Personally owned software, files, data, and other hardware or software is not permitted on government systems.

Password Use

State Information Contacts (SITCON) receive one login and password. Passwords are to be protected from unauthorized personnel. The associated logins are to be used only for the specific purpose for which they were granted.

Monitoring of Use

Any or all uses of this system and all files on this system may be intercepted, monitored, recorded, copied, audited, and inspected by appropriate enforcement parties. By using this system, the signatory consents to such interception, monitoring, recording, copying, auditing, and inspection at the discretion of the U.S. Census Bureau. Unauthorized or improper use of this system may result in civil and criminal penalties and administrative or disciplinary action, as appropriate. By using the systems that the signatory has been granted access to, consent to these terms and conditions of use is acknowledged each time. Access can be revoked at any time if the Census Bureau believes that misuse of logins is occurring. The SITCON will be contacted immediately.

Security Training

All Census Bureau employees and contractors are required to complete an Information Technology Security Awareness Training session annually. State Partners are encouraged to provide similar training to the employees and contractors accessing Census Bureau systems.

IT Security Incident Reporting

If you are aware of an IT security incident, or what you may think to be an IT security incident, you must contact the Bureau of the Census Computer Incident Response Team (BOC CIRT) immediately by email (<mailto:BOC.CIRT@census.gov>) or phone 301-763-5141. Additionally, you should contact the administrators of the systems involved, as appropriate.

Acknowledgment of Rules of Behavior
for Internet Access by State Partners
to LEHD Information Technology Systems
at the U.S. Census Bureau

NAME:

Please print.

STATE FUNCTION:

*Please describe your function
(CTO, Internet Security Officer,
etc.). You are signing as a
representative for all employees of
your agency with access to the
resources listed below.*

USER ID:

User ID is assigned by LEHD

SERVER TYPE:

- LEHD Public Web server
(<http://lehd.did.census.gov> and <https://lehd.did.census.gov>)
- Census FTP server
(<ftp2.census.gov>)

SIGNATURE:

DATE:
