# Rules of Behavior for U.S. Census Bureau Information Technology Systems

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 (including management, administrators, federal personnel, and contractors) accessing IT resources their role in protecting those resources, and advise them of their obligations. These rules apply whether working in a Census Bureau office, teleworking, or using remote access.

Since the access to IT systems and use of such systems are a user's individual responsibility, the receipt of this document suffices as an acknowledgement of the personal responsibilities associated with accessing Census Bureau IT resources.

*Individual Accountability*

Census Bureau personnel (including both federal employees and contractors), as representatives of the Census Bureau, are to be held accountable for their actions and may be subject to administrative penalties, fines, termination (removal), and/or imprisonment.

*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.

*Government Computer Use*

Use of government computers, personal digital assistants (PDA), communications systems, data, and other information is meant for authorized purposes. Unauthorized use of government equipment is prohibited.

Census Bureau personnel are given access to Census Bureau systems based on the need to perform their job responsibilities. Census Bureau personnel are requested to work within the confinement of this access and are not to attempt to access systems or applications to which access has not been authorized.

*End-User Software Use*

Unauthorized software may not be installed on any official government computer. Copyrighted software must be installed consistent with the respective licensing agreement and only after installation have been approved by Census Bureau management.

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

*Internet Use*

Internet access is limited to authorized Census Bureau personnel only. Use of the Internet is restricted for official (i.e. work-related) purposes when accessed through government-owned hardware and software. All Internet connections must conform to Census Bureau security and communications architecture.

*Remote Access Use*

Remote access to the Census Bureau network is available to Census Bureau personnel in the event of an emergency only and with prior Census Bureau management and Information Technology Security Office (ITSO) authorization to proceed. All system administrators are advised to remotely access the Census Bureau network using the Dial-in RADIUS server and Secure Remote or a virtual private network (VPN) over the Internet, SecurID, and Secure Shell, if possible. Remote access to Census Bureau e-mail is available to Census Bureau personnel through the Internet using a web browser with secure settings (https://dmz.notes.census.gov).

*E-mail Use*

Census Bureau personnel should take into consideration the following when utilizing the e-mail system (either through workstation software or remote Internet access):

- Consider all messages sent over the Census Bureau computer and communications systems as Census Bureau property (there should be no expectation of privacy associated with information sent through Census Bureau systems)

- Do not send sensitive data of any kind in the text of e-mail (all data must be encrypted and sent as an attachment)
- Lock the terminal, log out of the session, or use a password protected screen saver when leaving the computer while still in e-mail
- Do not send illegal transmissions (respect copyright laws)
- Follow established retention (archiving) policies
- Consent to monitoring and review activities

*Password Use*

Census Bureau personnel are required to adhere to the following Census password guidelines for individual user accounts:

- Make passwords at least eight characters long, which should contain a minimum of 5 alpha characters, 1 numeric, and preferably a special character
- Passwords are required to be changed every 90 days
- New users must change their passwords at the first login
- Easily guessed or user names are not acceptable passwords
- Do not write down or share passwords with anyone

*Security Practice*

Census Bureau personnel are responsible for securing their IT resources (i.e. computers, workstations, terminals, etc.) to prohibit unauthorized access. To better protect and secure your individual PC or workstation, always:

- Log out of secure applications running on your workstation that are no longer in use
- Lock your password-protected workstation if you leave your desk
- At the end of each workday, users must logout
- Do NOT entrust your system password to anyone. If there is a chance your password has been compromised, change it immediately.

*Security Training*

All Census Bureau employees and contractors are required to complete an Information Technology Security Awareness Training session annually. Additionally, Census Bureau employees are required to complete training on Title 13 and, if necessary, Title 26 data.

*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 e-mail (BOC.CIRT@census.gov) or phone 301-763-5141.

*IT Security and Data Stewardship Information*

Refer to the Census Bureau's Office of Analysis and Executive Support website on data stewardship (http://cww.census.gov/datastewardship) for additional guidance on using, accessing, or processing sensitive data or information.

The "IT Security Program Policy" available on the ITSO website (http://cww2.census.gov/it/itso) has additional guidance on IT security and processing sensitive data and information.

# Acknowledgement of Rules of Behavior
# for U.S. Census Bureau Information Technology Systems

NAME: _____

Please print.

USER ID: _____

User ID is assigned after beginning work.

SIGNATURE: _____

DATE: _____