

Census Bureau Data Stewardship Program

DS018: Unauthorized Browsing Policy

PURPOSE

The U.S. Census Bureau's ability to gain the public's cooperation in its surveys and censuses depends on its reputation as a good data steward. Even the perception that the Census Bureau does not adequately protect personal information may damage its reputation and affect its ability to fulfill its mission. Consequently, this policy establishes that, in addition to prohibitions against misuse and disclosure of protected records, unauthorized browsing by employees of protected records also is prohibited.

BACKGROUND

This policy was originally issued in June 6, 2003 as the *"Control of Access to Personally Identified Survey and Decennial Census Data: Unauthorized Browsing Policy."* This version has only been updated to reflect current organizational names, remove outdated references to other agency documents, reference current legal authorities, and has been edited for clarity and consistency with other Census Bureau policies and procedures.

SCOPE

This policy applies to all Census Bureau employees, contractors, and individuals with special sworn status who have access to data files and records that identify or may identify persons or businesses, including, but not limited to, demographic and economic data, administrative data obtained for statistical purposes, and personnel-related records. The unauthorized browsing policy applies to all data and information contained in files and records protected by Title 13 U.S.C., Title 26 U.S.C., Title 5 U.S.C., the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), and the Privacy Act. The policy also applies to unauthorized browsing of information that has not been disseminated to the general public and information that is not authorized to be made available to the public on request.

POLICY

Unauthorized browsing is defined as the act of searching or looking through, for other than work-related purposes, protected personal or business-related information that directly or indirectly identifies individual persons or businesses.

Unauthorized browsing is prohibited. Unauthorized browsing may result in disciplinary action up to and including removal.

EFFECTIVE DATE

This policy is effective upon signature.

LEGAL AUTHORITIES

Title 13 U.S.C.

Title 26 U.S.C.

Title 5 U.S.C.

The Confidential Information Protection and Statistical Efficiency Act

The Privacy Act

IMPLEMENTATION

All employees, contractors, and individuals with special sworn status will be apprised as part of the annual Data Stewardship and IT Security Awareness Training. The Policy Coordination Office will oversee administration of the policy. Potential violations should be brought to the attention of the Policy Coordination Office; any disciplinary action will be implemented by the division of the employee in consultation with Human Resources Division.

RELATED DOCUMENTS

DS007 – Safeguarding and Managing Information Policy

DS017 – Data Stewardship Awareness Training Policy

POLICY OWNER

The Policy Coordination Office owns this policy.

SIGNATURE

Ron Jarmin
Chair, Data Stewardship Executive Policy Committee

Date

Summary Information

| | |
|--|-------------------------------------|
| Policy Title: | DS018: Unauthorized Browsing Policy |
| Date Signed: | See Signature Date |
| Last Reviewed: | 3/13/2020 |
| Intended Audience: | All Staff |
| Policy Owner: | Policy Coordination Office |
| Office Responsible for Implementation: | Policy Coordination Office |
| Office Responsible for Dissemination: | Policy Coordination Office |
| Stakeholder Vetting: | PCO, PPRC |