Privacy Standards for SSCC Staff

Approved by the SSCC Steering Committee 1/28/00

SSCC staff have varying degrees of access to privately owned files maintained by faculty, staff and students of the SSCC's member agencies. The extent of a file's inaccessibility to any non-privileged user is determined by the file's owner. In the normal course of their professional duties the SSCC staff have no need to read the contents of user-owned files and no interest in doing so. But because certain SSCC staff are granted administrative privileges that would permit them to examine the contents of any file stored on disks or other media hosted by SSCC network servers, all SSCC staff members are required to be conscientious in observing the following principles in working with privately owned data:

1. SSCC staff are required to observe the level of privacy that file owners have established for their files. File owners are able to establish a particular level of privacy by 1) applying protection levels using built-in operating system commands: or 2) making known to the SSCC staff that certain files require special treatment

2. The information contained in users' files stored on SSCC systems is not to be examined or made available to others unless one of the following circumstances applies:

    a. the file's owner gives consent either explicitly or implicitly through file protection settings that permit general user access.
    b. a privately owned file (for example, the UNIX history file) must be examined in order to track down a security threat to SSCC computing facilities.
    c. an emergency requires immediate access to personal information that may exist in a privately owned file.
    d. the SSCC is required by a court, the police, some other legal authority, or the university administration to examine or copy a file.

3. All media containing privately owned files must be properly secured so that they are not physically accessible to anyone who is not entitled to them.

4. Any account or password that grants unusual data access privileges must be guarded and made available only to staff who require them.

5. System console terminals and staff terminals displaying privileged logins are not to be left unattended or unlocked.

Nothing in this document is intended to compromise the application of the university's or the SSCC's appropriate use policies.

Addendum on Confidential Data

Researchers who are members of the SSCC's member agencies often acquire data that include confidential information on individuals. In order to protect the confidentiality of these data the researchers themselves are generally required to agree to specific practices in the handling of certain files or to a set of principles that will apply to the handling of all confidential files.

SSCC staff do not usually know which files contain confidential data and do not generally handle or maintain files individually. Most often they touch user-owned files only in the process of maintaining the Co-op's disk resources and, indirectly, in creating system backup tapes. Although SSCC staff are generally uninterested in the identity or content of individual files, confidential or not, it is important for them to be

aware of the standards followed by researchers in their use of confidential data files and to be bound by a similar set of constraints to the extent that they manage any such files.

The following principles for handling confidential data are derived from the Confidentiality Agreement that is signed by all research staff of the Institute for Research on Poverty. SSCC staff are required to observe these standards in their handling of user-owned data files to avoid compromising confidential information

1. All information obtained during the course of research concerning studied individuals is privileged information and must never be reported to any other persons unless it is necessary to resolve an issue related to one's professional work.

2. The anonymity of studied individuals will be respected and no information will be released which would permit their identification.

3. All confidential information, records, and documents must be properly secured. These materials may not be used, disseminated or distributed by any means except in the performance of duties directly related to the function of the job.

    a. Access protection of computer directories and files is the responsibility of the data owner.
    b. Materials that identify respondents will not be left where they might be observed by others not immediately involved in the research.
    c. All passwords giving access to confidential data are personal to the operator authorized to access data and must themselves be kept confidential.
    d. An SSCC staff member will not leave a terminal unattended and unlocked if the current terminal session permits access to confidential data.
    e. It is strictly prohibited to copy or download any computer directories or files containing case or individual record information to removable storage media or systems external to servers maintained by the SSCC except for the purposes of making, copying, and storing system backups. Removable storage media include, but are not limited to, diskette, disk cartridge, tape cartridge, CD, and DVD. Systems external to the servers maintained by the SSCC include, but are not limited to, all other mainframes, servers, personal computers, and internal or external hard disks.

4. All printed and written materials containing confidential information that would normally not be retained for documentation must be shredded.

Staff agreement: I have read the document "Privacy Standards for SSCC Staff" and its "Addendum on Confidential Data" and acknowledge that I am required to follow these standards of data privacy and confidentiality in the course of my professional work in the Social Science Computing Cooperative.

Signed:

Date: