

Restricted Data Protection Plan: Secure Data Enclave

1. The data will be stored and analyzed in a secure computing enclave provided by the Data and Information Services Center (DISC), the data library at the University of Wisconsin – Madison (UW). Administratively, DISC is part of the department called Social Sciences Research Services (SSRS). For purposes here, the secure computing enclave will be referred to as the “COLDRoom.” Computer services are provided by the Social Science Computing Cooperative (SSCC), another unit in the SSRS department. Other abbreviations used throughout this document include: RDM for DISC’s Restricted Data Manager, and SSCC’s sysAdmin for the Windows System Administrator.
2. Although the COLDRoom is a community resource, it is designed to ensure that only licensed researchers have access to the restricted data covered by any given license. The COLDRoom contains a single stand-alone workstation which is not connected to any network, several safes that are bolted to a concrete wall, and a printer. Restricted data for any given project are stored in a locked safe inside the COLDRoom when not in use. When a licensed researcher wishes to use the data, s/he enters the empty COLDRoom, unlocks the safe and removes the drive, inserts the hard drive into an empty bay, turns on the computer, and logs into the system. Other COLDRoom users who are not authorized under this project will not enter the COLDRoom when it is in use by another user.
3. The operating system and software are stored on a fixed hard drive. Each user is assigned a user account which is protected by a complex password. The system is set up so that Windows automatically starts up a password protected screen saver when the keyboard and mouse are idle for 5 minutes or more, and anti-virus software runs continuously from boot to shutdown. Every reasonable effort is made to prevent the user from writing data or any other information to the fixed hard drive in order to minimize the possibility that any usable restricted data might be left on the hard drive. For example, a SAS autoexec file is set up so that SAS writes log and lis files, temporary data files, new data files, and memory overflow (“swap”) space to the removable hard drive. Users are warned and asked to delete any files written to the fixed hard drive.
4. The lock on the COLDRoom door is keyed to a “security master” so that standard “master keys” carried by custodians, building managers, campus police, etc., cannot open the door. Only the RDM can issue keys for the COLDRoom. S/he issues keys only to the sysAdmin and to researchers whose access is authorized by a data agreement, license or contract. The RDM, sysAdmin, and authorized researchers have all completed human subjects training. When a user loses a key, the locks and keys are replaced with a new security master. If the person losing the key is employed by the University of Wisconsin, then that employee is personally responsible for the costs associated with replacing the locks and keys. If the person losing the key is a student, then the student’s supervisor (or, in the case of unfunded projects, the student’s advisor) are personally responsible for all replacement costs.

5. The smaller safes in the COLDRoom have an electronic keypad that can be programmed to a code of the user's choice. To open the larger safes, a user must have both a key and an electronic code number. Backup keys to these safes are stored in a separate locked and alarmed room to which only the RDM has access.
6. The original media containing restricted data is stored in a locked alarmed room to which only the RDM has access. Original media are released directly to the PI and other faculty or professional research staff only. Because students do not have administrative rights to the COLDRoom computer, the RDM or sysAdmin will check out the media sent by the data provider and assist any authorized student under this agreement to write data to their removable hard-drive and to publish electronic codebooks and any customized extraction utilities to the appropriate hard drive.
7. When the data provider has specific guidelines for backing up or printing log files and output files, or for creating safe presentations and publications that do not compromise confidentiality, the RDM reviews these guidelines with the PI, professional research staff, and any authorized students before issuing COLDRoom keys to any of these parties. For situations in which the data provider does not require compliance with specific printing, backup, or publications guidelines, the RDM provides users with sample guidelines from other data providers in order to draw their attention to the kinds of scenarios that might result in a breach of data confidentiality. The PI(s) are ethically and contractually responsible for reviewing analyses in presentations and publications, and are obligated to take all reasonable measures to ensure that students and professional research staff abide by the guidelines and the data protection plan.
8. No backups of any sort are created by the sysAdmin or the RDM. Users are warned not to create backups of any data files, but are encouraged to backup their code files. Users are advised to review their log files and output files for potential confidentiality problems per item 7 above before removing them from the COLDRoom.