Guidelines for a Data Security Plan
For the Use of NCERDC Data

The fundamental goal of the protections outlined in the Data Security Plan is to prevent persons who are not signatories to the Data Use Agreement or the Supplemental Agreement with Research Staff from gaining access to the data. When these agreements are executed, all members of the research team are obligated to follow all aspects of the Data Security Plan.

General Information Required for all Data Requests

The names, titles, and responsibilities of all the investigators(s) and research staff (students, research assistants, and programmers) who will have access to the data. Any changes in personnel would require that this information be updated.

Confidentiality agreements signed by all project personnel should be included with the Application. Any new personnel added during the research period would require that an amended Attachment 3 be sent to the North Carolina Education Research Data Center.

A detailed description of the computer system where the data will be stored and analyzed. This description should include the following:

- All locations where the data and paper files will be kept.
- The secure network server on which data will be stored, how the networked system handles backups, and how long system backup copies of the data are kept.
- Information on the network's security protocols, including protections for original data sent by NCERDC and temporary analysis files.
- Information on how all files are tracked, accounted for, and schedule for deletion.
- The security system that would prevent unauthorized access to the data, and whether this system is used by other projects.
- The time frame for analysis of the data, including the end date of the project. This date should not exceed three years from the execution of the data use agreement. Should the research project require additional time, a request for continuation should be submitted three months prior to the specified end date. Unless prior arrangements are made with the NCERDC, all electronic and paper data must be destroyed on the project's end date.

Specific Guidelines

All original NCERDC data files, and all resulting temporary and and derived data files, should be stored on a secure server. A server is any device with an active network connection that provides services or resources to users and/or to other systems. For server security standards, please see attachment.

The use of stand-alone personal computers with data stored on the hard drive is strongly discouraged; this security plan will rarely be approved by NCERDC. In the unusual circumstance that a secure server is not available, then the personal computer must meet the current NCERDC policy. That is, the stand-alone computer must be located in a locked office, with strong password protection and access restricted to project personnel only.

No data or analysis output derived from the data can be transmitted via e-mail, e-mail attachments, or unsecured FTP.

Portable storage devices may not be used for downloading or storing data, including laptops (these may be used only for remote access to a secure server).

The data security protections apply to the original NCERDC data, derived files, and temporary analysis files.

Printouts derived from data analysis must be stored in a locked compartment when not being used. Printed information that is no longer needed should be shredded before disposal. Printouts of data from the NCERDC are not to be distributed to anyone outside of the research team.