Sample Data Security Plan

Executive Summary

The project researchers will connect to a NCERDC data folder through a secure file server housed on the XX University campus. All data will be viewed and modified on the server over an encrypted network connection. The data will not be downloaded to any local workstations. **Portable storage devices, including laptops, will not be used for downloading or storing data.** Desktop and laptop workstations may be used only for remote access to the secure server.

NCERDC data will NOT be shared with any other institution or any investigator not currently listed in the data use agreement. This restriction applies to source data as well as all derived data files. Project investigators, including the PI, do not have discretion to modify access to the NCERDC data. Any changes in access to the data on the secure server require explicit prior approval by the NCERDC.

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

Technical Details

LOCATION

XXU Managed Data Center
Physical Access: Data Center Staff & Technical Staff with fob recorded access doors

COMPUTING PLATFORM

Storage systems on campus export data to users through encrypted xxx/yyy connections, allowing for secure access from windows and mac environments through zzz default encryption. Connections are only allowed for authorized XXU University IP addresses.

Users authenticate to the storage system using their campus username and password. Access is controlled via user ACLs based on the users identity in the global XXU account system.

SECURITY SYSTEMS

The data are protected end to end via encrypted channel (User to Server and Server to Backup Server). On the file server, access is policed through a series of access control lists. Only the 3 designated researchers and IT system administrators will have access to the folder with the NCERDC data.

TIMELINE FOR DATA USE

These data would be under active analysis through June 30, 201X, but would be stored for up to five years. The data will be destroyed by December, 2016.