North Carolina Education Data Center

Data Protection Plan

The purpose of this Data Protection Plan (Plan) is to become part of the signed agreement between the North Carolina Education Data Center (NCERDC) and the Restricted Data Investigator Jane Smith. If the agreement is executed, all members of the research team with access to the data are contractually obligated to follow all aspects of the Plan. The fundamental goal of the protections outlined in this plan is to prevent persons who are not signatories to the Restricted Data Use Agreement or the Supplemental Agreement With Research Staff from gaining access to the data.

This Plan also applies to both the raw data files received from NCERDC as well as any copies made by the research team, and any new data derived solely or in part from the raw data files.

This Plan also reflects how computer output derived from the data will be kept secure. This applies to all computer output, not only direct data listings of the file.

Title of Research Project:

Analyzing Educational Outcomes

Principal Investigators:

John Williams, Professor of Economics, Learning University

Elizabeth Davis, Assistant Professor of Economics, Learning University

Executive Summary

The project researchers will connect to a NCERDC data folder through a secure file server housed on the Learning University campus. All data will be viewed and modified on the server over an encrypted network connection.

ALL storage and analysis of NCERDC data will take place exclusively on the secure server. Data may not be downloaded to local workstations, or to any external devices, including laptops. Desktop and laptop workstations may be used only for remote access to the secure server.

Portable storage devices, including laptops, will not be used for downloading or storing data. 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.

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

Technical Details

LOCATION

Data will be stored and analyzed on a secure server located at Learning University Data Center, Room A-025, 123 Main Street, Boston, MA 02468 (keypad code and card scan are required in order to enter the controlled data center).

COMPUTING PLATFORM

- Data will be stored and analyzed on a secured cluster of Linux servers located at Learning University Data Center, Room A-025, 123 Main Street, Boston, MA 02468 (keypad code and card scan are required in order to enter the controlled data center). Only analysis results including output tables and figures will be removed from the server; no original data will be removed.

- In no case should data be downloaded from the Server or otherwise be copied onto media or devices not approved in this DDP.

- Only the designated researchers and IT system administrators will have access to the folder with the NCERDC data.

- **Encryption:** server can only be accessed only via encrypted communications protocols: ssh, scp, sftp, nx,

- **Back-up data storage:** NCERDC will be excluded from server backups. Upon researchers' request, data will be excluded from backups.

- **Patches on workstations:** The relevant personal computers are configured for operating system updates at least once per week.

  The relevant personal computers are protected with antivirus software (ESET, for example) and configured for antivirus updates at least once per week.

- **Network segregation**: The data is stored on a Netapp filer, and mounted via a private network interface. Only the IP addresses in the private range are allowed to access the filer. Logging into the private network requires first authenticating to the research computing environment (RCE).

- **Security:** Each project is given a separate Unix group to control access to their data. For groups managing confidential data, group membership is reviewed annually, and any changes to group membership must be approved by the designated group owner.

- **Security audit process:** Servers are formally certified by Learning University IT Security for L3 data. Requirements for various security levels can be explored here and here is information on Level 3 requirements.

- **Researchers found in violation of security protocol**: For a researcher with an academic position, administrators consult with Academic Affairs. We use university policies and as well as the signed agreements covering the terms of the data-use to determine the appropriate course of action.

  Depending on the gravity of the violation, some violations are handled at the department level under the advisement of Academic Affairs and, if necessary, the University Office of the General Counsel (OGC).

  For a non-academic position, again depending on the gravity of the violation, some violations are handled at the department level under the advisement of University Human Resources (HR). If necessary, HR will respond to the violation according to its policies, with guidance from the OGC.

  Server and application operators are obligated to inform the proper authorities of any possible breaches promptly.

- **Data destruction:** Data destruction protocols are governed by the relevant Data Use Agreement and the IRB data security designation. Information designated level 3 must be properly disposed of by securely overwriting the information or physically destroying the media when no longer needed.

- **Passwords:**
  1) The accounts on personal computers are required to have strong passwords, by University standards (http://security.learning.edu/choosing-strong-passwords)

  2) Accounts used on any remote computers (RCE, for example) must have equally strong passwords and these passwords cannot be saved locally (i.e., they must be typed in each time one connects to the remote account)

  3) The relevant personal computers are configured such that a screensaver lock will activate after a short period of time and that the screensaver is blocked with a strong password

- **IT manager access:**
  Five administrators, who are all Learning University employees trained in IT practices including managing confidential data. All University employees annually renew their agreement to protect confidential data securely.

TIMELINE FOR DATA USE
These data would be stored up to 12/31/2021, upon which it will be destroyed or the contract extended.

7/29/2019