

*Template for Research Data Security/Management Plan. Modify as required for the research project, sponsor terms, etc.*

**1.0 Roles and Responsibilities**

During this project, the research team will implement a set of procedures to manage and secure the data, ensure data integrity, and monitor the data security/management plan. All data access and generation, entry, cleaning, documentation and basic statistical analyses will be conducted by staff members who are hired to work on this project and will be overseen by the investigators. Specifically, as an Investigator on the project, [NAME] will have responsibility not only for overseeing study implementation in accordance with the study design, and conducting all data analyses, but also providing direct oversight for the creation and maintenance of the project datasets, storage, and, security, and analyses.

In addition, the research team will meet [insert time frame/regularity] to discuss data management, security issues, and adherence to this plan. The principal investigator will be responsible for the long-term decisions regarding the sharing and storage of the data. If the principal investigator leaves the project or the University, the responsibility for the data will transfer to [Name of who data will transfer to]. The [Department/university] shall continue to maintain the data until the completion of the project and the sharing, transfer, or long term storage can be implemented.

Cleveland State University’s (CSU’s) Information Services & Technology (IS&T) division will monitor computer activity to ensure system security and a secure network environment. Project data will be stored and managed [PHYSICAL LOCATION OR CLOUD STORAGE LOCATION].

Users

|  |  |
| --- | --- |
| **Names of Users** | **Role** |
|  |  |
|  |  |
|  |  |

**2.0 Type of Data and Format to be Shared**

We are expecting to [collect, generate, or access] [describe specific data] which will be collected and stored [physically/electronically] within [list specific area/software etc]. All data entry will be validated and data cleaning will be completed on an ongoing basis to also ensure the quality of the data. All centralized data operations will be conducted on computers in a secure network environment. The datasets will be backed up on a server protected by a hardware firewall to isolate it from network traffic. The final dataset will be in [format] for sharing. Data in this format can be loaded easily into a variety of data analytic programs. We will make the final data files available in several widely used formats, [e.g, SAS, SPSS, and Stata].

Documentation will be provided for all the raw (i.e., questions, response values and related variable names) and constructed (i.e., variable names and scoring procedures) data collected pertaining to the study.

Include a detailed narrative that clearly depicts the system boundaries, system interconnections, and key devices. (Note**:** *this does not require depicting every workstation or desktop*)

**3.0 Access Controls**

Describe the processes/procedures that will be used to provide/restrict access to authorized users and devices:

Physical protections: Escorting visitors/maintaining visitor logs, screening individuals prior to authorization access to rooms or resources.

Electronic protections: Screening individuals prior to authorization for electronic access, prohibit the use of personal devices and email, prohibit the use of portable storage devices and removable media.

**4.0 Security of Data**

Please describe how any [sensitive, restricted, or confidential] data will be secured:

Electronic files that could permit the potential disclosure of this data will be maintained [please describe]:

Paper Files that could permit the potential disclosure of this data will be maintained in locked cabinets under the direct supervision of the Principal Investigator. Data that are to be shared will not contain [describe what will be redacted/removed from shared copies].

Firewall and computer virus protection software will be maintained on all computer systems.

**5.0 Circumstances Preventing Sharing**

Per sponsor contractual terms, we will adhere to the publication restrictions requirement and submit any possible publications or public release of information to the sponsor for approval at least [*Insert number of days required by contract, typically 30-45*] days prior to the intended release.

OR, public release of information specific to this project is not allowed.

**6.0 Incident Response**

The principal investigator and research personnel shall report any suspected or actual physical and electronic security breaches immediately to the CSU IS&T division and CSU’s Office of Research. Once reported, these incidents will be tracked, documented and reported to designated officials and/or authorities both internal and external to the organization as deemed necessary.

**7.0 Data Retention/Destruction**

Data from this project [shall be/shall] not be retained by CSU and the PI for [list number of years]. Following the completion of this project, data shall be destroyed in accordance with [list specifications regarding the type of data/level of security required for verifying destruction].

**8.0 Training**

All research personnel have completed Responsible Conduct of Research training. [describe any other pertinent training of co-investigators and other project researchers]

**9.0 Record of Changes**

All changes following the approval of the data security management plan shall be recorded below:

|  |  |  |
| --- | --- | --- |
| **Date**  | **Description of Change** | **Made By:** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

PI Signature \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

This document was adapted from templates created by University of Nebraska – Lincoln.