****

Odum Institute Data Archive

STANDARD OPERATING PROCEDURE: SENSITIVE DATA HANDLING

This Standard Operating Procedure (SOP) document outlines procedures for the handling of dataset files containing personally identifiable information (PII), protected health information (PHI), or information otherwise considered sensitive in nature, thus requiring special security provisions during execution of data deposit workflows. Tasks involving sensitive data handling begin upon inspection of the submission information package (SIP) for sensitive data during the triage phase of the data deposit workflow as outlined in SOP: DATA DEPOSIT. The purpose of this SOP is to ensure compliance with Odum Institute Data Archive DATA SECURITY GUIDELINES, [University of North Carolina Information Technology Services Information (UNC ITS) Security Policies](http://its.unc.edu/about-us/how-we-operate/), and all applicable laws and regulations governing the protection of human subjects.

Note that the Odum Institute Data Archive DATA DEPOSIT AGREEMENT and UNC DATAVERSE TERMS OF USE Policy expressly prohibit the ingest of datasets containing PII or PHI into the archive system. Should PII or PHI be discovered during SIP file review, return the files to the data submitter along with specific information about the sensitive nature of the data and the Terms of Use regarding sensitive data.

Procedures outlined in this SOP apply only to data for which the Odum Institute has a formal agreement with the data submitter to perform data curation actions on the data. The formal agreement should include a statement of explicit acknowledgement of the sensitive nature of the data and outline the necessary provisions for sensitive data handling in the scope of work.

Secure Storage

Sensitive data files should be stored on the Secure Network-Attached Storage (SecNAS) space assigned to the Odum Institute Data Archive. Access SecNAS storage using the following file path:

[\\secnas.unc.edu\irss\_data\Archive](file:///%5C%5Csecnas.unc.edu%5Cirss_data%5CArchive)

**Under no circumstances should sensitive data files ever be stored on a computer hard drive, unauthorized cloud storage, or other file server locations!**

Electronic Transmission

Email delivery of sensitive data files from a UNC email account to any email user is permitted only when using the UNC Encrypted Email option. UNC Encrypted Email encrypts the entire email message between the sender and recipient including attachments.

1. In the Outlook **Subject** field, enter the trigger text **(secure)** followed by the normal subject line. This invokes the UNC Encrypted Email option.
2. The recipient will receive an email to notify them of the delivery of an encrypted message and to provide a link to open an attachment containing the encrypted email. Non-UNC recipients will be required to sign in using a one-time passcode delivered automatically in a separate email.

Sensitive data files that cause the email to exceed the 25 MB size limit can be shared to UNC affiliates using SecNAS.

1. Create a dataset folder in the Archive SecNAS for the sensitive data files.
2. Send the sharing request via email to the Cyberinfrastructure Group (jonc@email.unc.edu). In the request, include the folder name and the recipient’s ONYEN. Cyberinfrastructure staff will enable access for the recipient.
3. Once secure file access has been enabled, send a notification email to the recipient along with the file path to the SecNAS dataset folder.

File Encryption

For some sensitive data files, encryption may be required based on information from the data submitter who may be bound by specific human subject research laws or regulations. To encrypt these files, use the [latest version of 7-Zip](http://www.7-zip.org/).

1. In File Explorer, right-click on the name of the file for encryption. Select **7-Zip** ⯈ **Add to archive…**.
2. In the **Add to Archive** dialogue window that appears, select **zip** for the **Archive format**.
3. Enter and re-enter a password to be used to open the encrypted file. Create a password that follows the [UNC ITS Password Standard for General Users](http://its.unc.edu/about-us/how-we-operate/):
	* At least eight characters long
	* Contain at least one letter
	* Contain at least one numerical digit
	* Contain at least one special character (!@#$%&\*+={}?<>)
4. Select **AES-256** for the **Encryption method**.
5. Click on the **OK** button when completed.

To open an encrypted file:

1. Right-click on the name of the encrypted file in File Explorer and select **7-Zip** ⯈ **Extract Here**.
2. Enter the password in the dialogue box that appears.
3. Click on the **OK** button when completed.

REVISION HISTORY

This Standard Operating Procedure document was completed initially in April 2017 to be reviewed on an annual basis or when technical or workflow systems changes take effect, whichever occurs first.