Document Authorization:

	Name	Date	Signature
Owner	Yuewei Zhao	**20Jan2023**	
Operation Management	Baozhong Zhao	**20Jan2023**	
Quality Assurance	Xibo Li	**20Jan2023**	

Changes from previous version:

Section	Summary of Changes	Change Control Number
ALL	1. New document	

Document Authorization:

	Name	Date	Signature
Owner		**20Jan2023**	
Operation Management		**20Jan2023**	
Quality Assurance		**20Jan2023**	

Changes from previous version:

Section	Summary of Changes	Change Control Number
ALL	1. New document	

1. PURPOSE

The purpose of this procedure is to provide instruction for the back-up and archival of electronic data as generated.

2. SCOPE

This SOP applies to all equipment which generates electronic data as part of the daily operation.

3. INTERNAL REFERENCES

Document ID	Title

4. EXTERNAL REFERENCES

Document ID	Title

5. RESPONSIBILITIES

Job Function and/or Department	Responsibility
System Owners	It is the responsibility of the system owners to ensure that back-up are in place and back up is carried out as required by reviewing the log file on a weekly basis for failures.
Operational Managers	It is the responsibility of the Operational Management to ensure that an inspection of the successful data back-up is conducted annually.

6. DEFINITION

Term	Definition
Electronic Raw Data	Any electronic data generated during a project that could not be reconstructed from other data. The most common example is chromatographic raw data files generated from scientific instruments.
Electronic Derived Data	Any electronic data generated during a project that can be reconstructed from raw data. Common examples include integrated peak areas, spreadsheets, and calibration curves. This type of data is generally generated and held on Synoligo network drives.
Data Folder	A logical electronic container in which all raw data generated on the laboratory instrument is stored.
Scripts Folder	A logical electronic container in which the backup script file is located e.g., desktop.
Mapped Drive	A method in which Windows operating system can associate a local drive letter with a shared storage area to another computer over a network e.g., 'T:\'.
External Storage Device	A physical storage unit which resides external to a computer or equipment used to transfer data between a non-networked computer to one which is networked for the purpose of archiving.
Distributed File System	Distributed file System (DFS) is a set of client and server services that allow Synoligo using Microsoft Windows servers to organize many distributed Server Message Block (SMB) file shares into a distributed file system.
System Owner	Individual or individuals responsible for a defined analytical or manufacturing system.

7. PROCEDURE

7.1. Back-up and Storage of Electronic Raw Data

7.1.1. Electronic data generated is defined as either "raw data" or "derived data".

7.1.2. This procedure ensures that, within 96-hours of data generation, two independent electronic copies will exist—one on the local computer, and one on a dedicated server. Once the data is transferred to a dedicated server, the data is further archived by automated daily backup procedures. Upon transfer from the local computer to the

dedicated server, two log files are generated—one locally stating the start and completion time, and one on the server indicating which files were copied, updated, or skipped. The log file will be reviewed periodically by the System Owners to assure proper execution of the data backup process.

7.1.3. Raw data which can be printed (e.g., record entries, e-mail correspondence, etc.) is printed contemporaneously and archived as project data. For this procedure, it is not defined as electronic data.

7.1.4. Electronic Derived data is created and stored on network servers and backed up as per procedure.

7.1.5. Electronic raw data

7.1.5.1. All instrument data (raw files and folders) are produced into a data folder by the relevant piece of instrument software. These folders are backed up using an automated script which transfers data across the network to a designated location defined below. If the automated backup application fails to execute, or if the System Owner or operator determines necessary, the backup script can be executed manually to transfer data. In the event of network failure or if a system is incompatible with the local intranet, a System Owner or operator can manually execute the backup application to transfer data from the source computer to an external storage unit which is then transferred via networked computer directly to the designated location utilizing a second backup application specific for manual transfer. In all scenarios described, log files detailing the files transferred are generated locally and at the destination.

7.1.5.2. The data backup process is accomplished by running a local application configured to push data from the computer workstation to the designated server storage location. Each system contains a folder with the backup application and unique instructions dictating data source locations and final destination.

7.1.5.3. The backup application will execute by either manner described in section 7.2 to assure backup copies are transferred to the designated server storage location. The backup application compares files and directories in the source location with that of the destination and writes or overwrites new or newer files, respectively, in the destination folder. A log file is generated upon completion of the transfer detailing the transfer of files, including new files, newer files, and skipped files. These files are further backed up and can be restored according to WI.

7.1.5.4. Each instrument PC will transfer files for archiving to one of the following Server Destination locations:

For systems on the primary intranet:

\\Data\Instrument_Backup\Instrument\

These above examples are DFS available for file storage located on site.

Each instrument PC has its own folder location on the mapped drive, for example: T:\Instrument\ins-tiamo (Karl Fisher system with the name ins-tiamo). The full path can also be located with the following: \\data\Instrument_Backup\Instrument\ins-tiamo.

Each instrument folder has the following sub-folders:

\Data

\Logs

Wherein in files from the source folder on the local PC are copied to the \Data folder and a log file containing details of the backup is in the \Log file. The log file is updated by appending the most recent backup to the end of the file.

Only raw data is copied, to minimize the size of the DFS.

7.2. Data Backup Procedures

7.2.1. Automated Data Backup

7.2.2. The backup application is set to run automatically each day using Windows Task Scheduler application. This application contains instructions to execute the backup application at a fixed time, daily, and tracks the history of the process. There is no need to review the Task Scheduler history log unless a failure is encountered.

7.2.3. Manual Execution of Data Backup

7.2.3.1. If the automated system fails to execute, or if the System Owner or operator deems necessary, the backup application can be executed manually by double clicking on the application shortcut icon located on the

system desktop. Upon completions, the log file will be reviewed to assure successful file transfer.

7.2.4. Data Backup with External Device

7.2.4.1. If a system is removed from the intranet, or determined to be incompatible with the intranet, data will be backed up using an external device such as a dedicated USB drive. Once the drive is connected to the source computer and assigned a drive letter, the operator will execute the external drive backup application located on the desktop of the backup computer. The application transfer files from the source computer to the USB storage device, generating two log files as described in section 7.1 for traceability purposes. The USB storage device is then transferred to a networked system and the backup application located on the USB storage device executed to complete the transfer to the target server storage location. Upon completion, the log file and data storage folder will be reviewed to assure successful file transfer.

7.2.5. Storage facilities for back-up tapes (fire-safes)

7.2.5.1. Server backup, data storage protocols, and policies are detailed in WI.