1.0 Purpose

This procedure establishes a process that ensures laboratory electronic documentation is controlled and protected.

2.0 Scope

This procedure applies to all laboratory documents that are in electronic form.

3.0 Responsibility

3.1 It is the responsibility of Management to ensure the functionality of the computer systems that control laboratory activities or processes within Ion Labs through a software validation.

3.2 It is the responsibility of the Quality Systems Manager to implement this procedure and to ensure that the procedure is followed.

4.0 Definitions

None

5.0 References

5.1 QS-108, SOP, Corrective and Preventive Action

6.0 Procedure

6.1 Electronic Documentation and Data

6.1.1 Ion Lab's Management is responsible for approving the functionality of the computer systems that control laboratory processes within the organization. Approval is indicated by the existence and functionality of the system(s) in use.

6.1.2 Management manages the data generated in the electronic system and electronic backups. All personnel have access to the data and information needed to perform assigned laboratory activities.

6.1.3 The Lab's information management system used for the collection, processing, recording, reporting, data storage, or retrieval of data is validated for functionality, including the proper functioning of interfaces within the Lab's information management system(s) by the Lab before introduction. This validation will be documented in the Lab Software Validation Log which identifies the application(s) and records the results of the validation(s).

6.1.4 Whenever there are any changes, including laboratory software configuration or modifications to the commercial off-the-shelf software, they will be authorized, documented, and validated on the Lab Software Validation Log before implementation.

6.1.4.1 Justification may be used if a validation is not required for changes to the commercial off-the-shelf software.

6.1.5 Documents, data and records managed electronically are protected from unauthorized access, tampering and loss, unauthorized changes, unintended alterations, corruption, and physical damage as described in Table 1 below.

Table 1

Application	Use	Access Control	Protection
Microsoft Office Suite	LMS documents, data and records	LMS documents, data, and records only on computers in the Lab Username and password, Read/write folder permissions or no access	N/A
DicksonOne Cloud Web Application	Interface for the Display Data Loggers (DWE) and Touchscreen Data Loggers (TWE/TWP)	Username and password	Cloud based System. Data is stored by company.
Agilent OpenLabs	Acquire Digital data from chromatographic equipment	Username and password, Read/write folder permissions or no access	Windows-based Server control Software firewall Daily Server backup Anti-virus protection
ThermoScientific Chromeleon	Acquire Digital data from chromatographic equipment	Username and password, Read/write folder permissions or no access	Windows-based Server control Software firewall Anti-virus protection
Agilent Masshunter	Acquisition of data for ICP-MS	Username and password, Read/write folder permissions or no access	Windows-based Server control Software firewall Anti-virus protection
ThermoScientific Omnic	Acquisition of data from Nicolet FTIR	Username and password, Read/write folder permissions or no access	Windows-based Server control Software firewall Daily Server backup Anti-virus protection
Win-Lab	Acquire Digital Data from UV/Vis instrument	Username and password Read/write folder permissions or no access	Windows-based Server control Software firewall Anti-virus protection
Force Recorder Professional	Acquire Digital Data from Texture Analyzer	Username and password for computer system	Windows-based Server control Software firewall Daily Server backup Anti-virus protection
Agilent Mass Hunter	Acquire Digital Data from QQQ	Username and password, Read/write folder permissions or no access	Windows-based Server control Software firewall Daily Server backup Anti-virus protection

6.1.6 Electronic LMS documents, data and records residing on computers, servers, and/or the network are protected through the following methods:

- Windows-based server control; domain and user account restrictions,
- Software firewall built into server,
- Daily Server backup: scheduled and controlled by Ion Labs,
- Each computer workstation has anti-virus protection,
- Cells in spreadsheets are protected from alteration as necessary,
- Limited access to archive or obsolete folders.

6.1.7 The information management systems are operated in an environment that complies with the application providers' or the Lab's specifications and the operating systems have proven to be effective through years of successful use.

6.1.7.1 System failures are identified, and appropriate immediate corrections and corrective actions are taken in accordance with the QS-108 Corrective and Preventive Action procedure.

6.1.8 The methods described above ensure the integrity of the data and information is maintained. Additional methods to protect data integrity include, but are not limited to:

6.1.8.1 Record integrity is tested during application upgrades to ensure that data contained in records is legible and appears in the same format as when the data was originally entered.

6.1.8.2 Records scanned into portable data formats (pdf) are reviewed to ensure the scan is legible and both sides of double-sided originals are captured.

6.1.8.3 Discontinued applications are reviewed to determine the data contained and where necessary, data mapping is completed, or alternate solutions are developed.

6.1.9 Calculations and data transfers are checked in an appropriate and systematic manner. This occurs during routine testing and when Lab Management deems appropriate.

6.1.10 The Lab's information management system is maintained off-site and on-site.

7.0 Revision History

Revision	Date	Description of Changes	CCR #	By
0	11/30/21	New	N/A	J. Sassman