

ISSUE N° 1 – MAJOR MODIFICATIONS

Version	Changes	Related Release No.
01	First issue.	SOLABS 2.8.0

PREVIOUS VERSIONS HISTORY

Version	Date	History	Related Release No.
N/A	N/A	N/A	N/A

APPROVAL TABLE

Signatures below signify that the content of the document was reviewed and approved for correctness, accuracy, reliability and completeness.

Document Author	
Prepared by: Patrice Joly, Validation Specialist, SOLABS	
Document Reviewers/Approvers	
Information Technology:	
Signature: _____	Date: _____
Validation:	
Signature: _____	Date: _____
Quality Assurance:	
Signature: _____	Date: _____

US FDA 21 CFR PART 11 ASSESSMENT FOR COMPLIANCE WITH SOLABS QM

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
Subpart B — Electronic Records					
11.10 Controls for Closed Systems					
<i>Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following :</i>	Is this a closed system (i.e. a system that does not use the public internet or public email systems and is administered by an individual responsible for its operation)?	Yes	Yes	The system is installed within a corporate network and access is controlled by system administrators.	
<i>(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.</i>	Has the system been or will the system be validated?	Yes or No (Based on Client Decision)	Yes	The system validation is the responsibility of the client. SOLABS provides a validation package to support the validation of the system. However some clients may choose to take care of the validation without any help from SOLABS.	
				<u>CLIENT Name</u>	
<i>(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.</i>	Can the system produce the requested information in both electronic and human readable form?	Yes	No	Records that are created when using SOLABS QM can be accessed in a human readable form by different means i.e. 1- directly in the GUI (Graphical User Interface) by the use of menus (e.g. accessing a Document audit trail), where the information can be printed, or 2- by using direct means (e.g. reports) of accessing the data stored in the database.	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
<i>(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.</i>	Are the Electronic records being maintained in electronic format for the time periods required by applicable regulations?	Yes	Yes	SOLABS QM system enables archiving and retrieval of records. (Retention period determination is responsibility of client and should be governed by client's SOP.) Backup and recovery procedure should be tested as part of the Installation Qualification protocol execution.	
				<u>CLIENT Name</u> SOP on Backup and Recovery	
<i>(d) Limiting system access to authorized individuals.</i>	Is system access restricted to appropriate personnel?	Yes	Yes	SOLABS System access is controlled and limited to authorized individuals by use of a valid and unique combination of User Name and Password.	
				<u>CLIENT Name</u> SOP on System Access	
<i>(f) Use of operational system checks to enforce permitted sequencing of steps and events as appropriate.</i>	Does the system use checks to enforce sequencing of steps and events? (optional)	Yes	No	SOLABS System enables operational system checks permitting sequencing majorly in documents, process and ad hoc tasks treating, superseding, referencing and retiring actions.	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand	Are adequate security measures in place to protect the system?	Yes	Yes	SOLABS System access, use and actions within system are restricted only to authorized individuals who have been given access (refer to d) and appropriate privileges. (It is client responsibility to determine level of system access per user).	
				<u>CLIENT Name</u>	
(h) Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Does the system use terminal checks to determine the validity of the source of the input? (optional)	No	No	N/A	N/A
(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Are appropriate employee qualifications documented in accordance with internal SOPs, including training records, CV's, and Job Descriptions?	Yes	Yes	SOLABS' personnel involved in system development and testing are trained on applicable procedures and training records are maintained.	
				<u>CLIENT Name</u>	
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	If electronic signatures are used, is there a corporate policy or SOP that holds individuals accountable and responsible for actions initiated under their electronic signatures?	No	Yes	<u>CLIENT Name</u>	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
<i>(k) Use of appropriate controls over systems documentation including</i>					
<i>(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.</i>	(1) Are controls in place for the distribution, access, retention and use of all system documentation?	No	Yes	CLIENT Name	
<i>(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.</i>	(2) If the system is developed /maintained in-house, are controls in place to maintain a revision history for system documentation?	Yes	Yes	SOLABS maintains a quality system based on ISO 9001 requirements. Changes to the application are documented and all relevant system documentation is reviewed in accordance with the changes. The information on changes is communicated to the user.	To system documentation
				CLIENT Name	
11.30 Controls for Open Systems					
<i>Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.</i>	Is this an open system (i.e. one that uses the public internet or public email systems)? - If yes, are controls in place to ensure authenticity, integrity, and, as appropriate, the confidentiality of electronic records?	No	No	N/A	N/A

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
11.50 Signature Manifestations					
<i>(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following :</i>					
<i>(1) The printed name of the signer</i>	(1) Does the system use an electronic signature feature? If no, move to next section.	Yes	No	SOLABS application uses electronic signature feature and signature indicates clearly the printed name of the signer	
<i>(2) The date and time when the signature was executed</i>	(2) Does the signature have associated metadata that includes printed name of signer, date and time signature was executed, and meaning of the signature?	Yes	No	SOLABS QM system indicates on signed records: - Printed name of the signer - Action performed by the signer (or meaning when the action is not self-explanatory) - Date and time. Information is also captured in the Audit Trail.	
<i>(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature</i>	(3) Is the information associated with the signature (printed name of the signer, the date, and purpose) controlled by the system and not the user?	Yes	No	In SOLABS QM, the meaning of signature is captured on documents approvals. When signing-off other records, the meaning of signature is captured by the action performed, e.g. signing-off a "QA Review" process step or a Training record as trainer.	
<i>(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout)</i>	Is the information associated with the signature (printed name of the signer, the date, and purpose) displayed by the system whenever the signature is displayed or printed?	Yes	No	The information associated with the signer (printed name of the signer, the date, and purpose) is displayed by SOLABS QM whenever the signature is displayed or printed.	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
11.70 Signatures/Record Linking					
<i>Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.</i>	Does the system accomplish, through technical means, the linking of the records to the signature?	Yes	Yes	The system uses secure relational database references for linking of electronic records to corresponding signatures. The system's database cannot be accessed by system users.	
	Does the system insure, through technical means, that signatures cannot be copied and pasted?			<u>CLIENT Name</u> Access to the database is controlled by procedure on security.	
Subpart C — Electronic Signatures					
11.100 General requirements					
<i>(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else</i>	Are electronic signatures unique to their owners?	Yes	Yes	SOLABS System access is controlled and limited to authorized individuals by use of a valid and unique combination of User Name and Password. User Names in SOLABS QM are unique and cannot be deleted. However in most cases, SOLABS QM is installed to authenticate users on the corporate network (by matching the username and password with network accounts. Then the client is responsible to ensure that reuse or reassignment of electronic signatures is not permitted.	
	Is there an SOP precluding reuse or reassignment of electronic signatures?			<u>CLIENT Name</u>	
<i>(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.</i>	Are identities verified prior to granting an electronic signature? Is there an SOP governing this procedure?	No	Yes	<u>CLIENT Name</u>	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
<i>(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.</i>					
<i>(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857</i>	(1) Has required notification been sent to FDA?	No	Yes	<u>CLIENT Name</u>	
<i>(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.</i>	(2) Have users signed a statement indicating that their electronic signatures are equivalent to their handwritten signatures?	Yes or No (Based on Client Decision)	Yes	SOLABS QM can be delivered with a System Access process in which case new users must sign-off a process step indicating that their electronic signatures are equivalent to their handwritten signatures in SOLABS QM.	
				<u>CLIENT Name</u>	
11.200 Electronic Signature Components and Controls					
<i>(a) Electronic signatures that are not based upon biometrics shall :</i>					
<i>(1) Employ at least two distinct identification components such as an identification code and password.</i>	(1) Do electronic signatures employ at least two distinct identification components, where one of the components is known only to the user, such as an identification code and password?	Yes	No	Users in SOLABS QM use a Username and Password (known only to the user) combination as their electronic signature.	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
<i>(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.</i>	Is there a defined or configurable signing period within the system? If so, is only the component of the signature known only to the user required to execute a signature within the signing period?	Yes	No	During a session opened by a user in SOLABS QM, all signing actions require the Username and Password combination. In some cases, the Username field (editable) may already be populated with the Username of the user currently logged in SOLABS QM.	
<i>(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all the electronic signature components.</i>	Once the signing period expires, are both components required to execute an electronic signature?	Yes	No	See 11.200 (a) (i) above	
<i>(2) Be used only by their genuine owners; and</i>	(2) Are there SOPs in place to ensure that electronic signatures are not shared or otherwise accessible to others?	No	Yes	<u>CLIENT Name</u>	
<i>(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.</i>	(3) Are there controls within the system that prevents or detects unauthorized access?	No	Yes	<u>CLIENT Name</u>	
<i>(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.</i>	Are biometrics used for executing electronic signatures? If so, are they designed to ensure that they cannot be used by anyone other than their genuine owners?	No	No	SOLABS QM's electronic signature is not based upon biometrics.	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
11.300 Controls for Identification Codes/Passwords					
<i>Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:</i>					
<i>Note: SOLABS QM uses the network password for system users.</i>					
<i>(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.</i>	Is the user identification and password combination for each user account unique?	No	Yes	<u>CLIENT Name</u>	
<i>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging)</i>	Does the system have technical means to expire passwords periodically? If not, do SOPs exist to govern such a process?	No	Yes	<u>CLIENT Name</u>	
<i>(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.</i>	Do SOPs exist to disable user accounts that have had their security compromised? If so, do they include procedures for re-enabling the accounts, such as issuing new passwords?	No	Yes	<u>CLIENT Name</u>	

Requirements	Interpretations	Responsibility		Relevant Feature and/or Document Reference	Meets Requirements? (Yes/No)
		SOLABS	CLIENT Name		
<i>(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.</i>	Does the system have technical means to detect and report in an immediate and urgent manner any attempts at unauthorized use of the system If not, do SOPs exist to periodically review security logs for evidence of unauthorized attempts at accessing the system?	Yes	Yes	SOLABS system will automatically lock a user upon three (3) consecutive unsuccessful attempts to log in, and send an e-mail to the system administrator.	
				<u>CLIENT Name</u>	
<i>(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.</i>	Can the system perform self-test of tokens or cards upon each use? If not, are SOPs in place to periodically require this testing?	No	Yes	<u>CLIENT Name</u>	
All requirements are met? (Yes/No):					
Completed by:				Date:	