

## **OasisLIMS compliance with 21 CFR Part 11**

### **Input data, data processing, output data system implementation and operation requirements, to ensure 21 CFR Part 11 compliance**

- The system shall be validated to ensure accuracy, reliability, and consistent intended performance. It shall have ability to detect invalid or altered records (11.10a).
- The records shall be protected to enable their accurate and ready retrieval throughout the records retention period (11.10c).
- There shall be provision to create secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information (11.10e).
- Operational system checks shall be used to enforce permitted sequencing of steps and events, as appropriate (11.10f).
- Appropriate controls shall be used over systems documentation including revision and change control procedures to maintain an audit trail that documents modification of systems documentation (11.10k - 2).
- The system shall provide ability to generate accurate and complete records in both human readable and electronic form suitable for inspection, review and copying by the inspection agency (11.10b).

### **Data and system security requirements to ensure 21 CFR Part 11 compliance**

- The system shall limit system access to authorized individuals (11.10d).
- Authority checks shall be used to ensure that only authorized individuals can use the system, access the operation, alter a record, or perform the operation at hand (11.10g).
- Appropriate controls shall be exercised by the User company over systems documentation including adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (11.10k - 1)
- Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to assure the authenticity, integrity, and as appropriate, the confidentiality of electronic records from the point of their creation to the point of their use. (11.30).

### **Electronic signatures**

- Electronic signature, assignment, security, Essential services including customer service support relating to Electronic signatures, available through CA (Certifying Authority)

## 21 CFR Part 11 Electronic Record Requirements

**Technical** versus **Procedural** Controls:

- **Technical Controls** require *Testing*
- **Procedural Controls** require *Verification*
- In some cases, both methods are needed

System Class	For USA Suppliers FDA 21 CFR 11 Section	ELECTRONIC RECORDS Requirement Summary	Y/N Reference:
2,3,4,5	11.10(a)	<b>Validate the system; ensure ability to detect invalid or altered records</b>	
		<ul style="list-style-type: none"> <li>• Validate the system</li> </ul>	Yes Acceptance testing at user company
		<ul style="list-style-type: none"> <li>• Verify that the system can detect invalid records (ex: invalid field entries, fields left blank that should contain data, values outside of limits, ASCII characters in numeric- only fields, incorrect file formats, etc.)</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>• Verify that the system can detect altered records (usually via audit trails) [See Section 11.10 (e)]</li> </ul>	Yes
2,3,4,5	11.10 (b)	<b>Provide ability to generate accurate and complete records in human readable and electronic form</b>	
		<ul style="list-style-type: none"> <li>• Verify that the capability exists to view and print the entire contents of the database</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>• Verify that all reports can be generated electronically in a format that can be put on a portable medium (e.g., diskette or CD) or transferred electronically</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>• If there is information in the database that does not appear on any reports (e.g., hidden meta data or electronic “sticky notes”), verify that this capability is not used or is very tightly controlled.</li> </ul>	Database is password protected
2,3,4,5	11.10 (c)	<b>Protect records to enable their accurate and ready retrieval</b>	
		<ul style="list-style-type: none"> <li>• Ensure that there is an SOP for the backup and restore process</li> </ul>	User company, Users manual
		<ul style="list-style-type: none"> <li>• Ensure that there is an SOP for the data archiving &amp; retrieval process</li> </ul>	User company, Users manual
		<ul style="list-style-type: none"> <li>• Ensure that the archived data is controlled and maintained for the required retention period</li> </ul>	User company, FUN 4B (FS)

System Class	For USA Suppliers FDA 21 CFR 11 Section	ELECTRONIC RECORDS Requirement Summary	Y/N Reference:
		<ul style="list-style-type: none"> <li>Ensure that data files are protected against intentional or accidental modification or deletion</li> </ul>	User company
2,3,4,5	11.10 (d)	<b>Limit system access to authorized individuals</b>	
		<ul style="list-style-type: none"> <li>Ensure that there is an SOP for system security (including physical, logical, and procedural controls)</li> </ul>	User company, SEC 14, 15 FUN 4G (FS)
		<ul style="list-style-type: none"> <li>Ensure that there are different levels of access based on user responsibilities (if appropriate) and that this is documented and controlled</li> </ul>	User company
		<ul style="list-style-type: none"> <li>Ensure that there is a controlled, documented process for granting access to a new user, or to change privileges for an existing user</li> </ul>	User company, SEC 1, 2, 5-7, 10-12 FUN 4H (FS)
2,3,4,5	11.10 (e)	<b>Create secure, computer- generated, time-stamped audit trails; don't obscure preceding data with changes</b>	
		<ul style="list-style-type: none"> <li>Verify that the system generates automatic, electronic audit trail information for <u>all operator</u> entries and actions that create, modify, or delete records</li> </ul>	Yes SEC 9, 13, 16 FUN 4C
		<ul style="list-style-type: none"> <li>Verify that audit trail generation is completely transparent to, and outside the control and access of users (except for view-only access)</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>Verify that the audit trail function is always ON and can not be disabled</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>Verify that the audit trail contains Name, Date, Time (to the second), and indication of record creation, modification, or deletion</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>Verify that the audit trail detects and records altered records (from 11.10 (a))</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>Verify that users cannot easily change the system time and date</li> </ul>	User company
		<ul style="list-style-type: none"> <li>Verify that there is a mechanism to periodically ensure that the time and date are correct</li> </ul>	User company
		<ul style="list-style-type: none"> <li>Verify that previous data is somehow maintained when records are changed</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>Verify that audit trail data is protected from accidental or intentional modification or deletion</li> </ul>	Database is password protected
		<ul style="list-style-type: none"> <li>Verify that electronic audit trails are maintained for at least as long as their respective electronic records</li> </ul>	Yes, User company

System Class	For USA Suppliers FDA 21 CFR 11 Section	ELECTRONIC RECORDS Requirement Summary	Y/N Reference:
		<ul style="list-style-type: none"> <li>• Verify that electronic audit trails are readily available for:               <ul style="list-style-type: none"> <li>• Inspection and review</li> <li>• Viewing and printing of selected sections</li> <li>• Extracting and copying onto transportable electronic format, e.g. disks</li> </ul> </li> </ul>	Yes
2,3,4,5	11.10 (f)	<b>Enforce step sequencing (as appropriate)</b>	
		<ul style="list-style-type: none"> <li>• If there are sequences of operations, sequential events, or sequential data entry, that is important to this system, verify that the system ensures that steps are followed in the correct sequence</li> </ul>	Yes FUN 4D
2,3,4,5	11.10 (g)	<b>Perform authority checks of users (for access and use privileges)</b>	
		<ul style="list-style-type: none"> <li>• Ensure that the system (or procedure) verifies that an individual is authorized to access a system/ application before it allows them into the system/ application</li> </ul>	Yes SEC 2, 3 (FS)
		<ul style="list-style-type: none"> <li>• Ensure that the system (or procedure) verifies that an individual has the appropriate privileges to perform specific functions within the system/ application before allowing to do so</li> </ul>	Yes SEC 10, 12 (FS)
		<ul style="list-style-type: none"> <li>• Ensure that the system (or procedure) verifies that an individual has the authority to electronically sign a record before allowing them to do so</li> </ul>	N.A.
2,3,4,5	11.10 (h)	<b>Use device checks to verify validity of data (as appropriate)</b>	
		<ul style="list-style-type: none"> <li>• For input or output devices for which it is critical that the data be coming from a specific device, ensure that the system checks for the correct device</li> </ul>	No input interface (except keyboard)
		<ul style="list-style-type: none"> <li>• For terminals, consoles, etc., that are specially authorized to issue certain commands (e.g. system commands for security), verify that those commands can only be issued from the designated physical station(s)</li> </ul>	User company
2,3,4,5	11.10 (i)	<b>Verify training of system users, developers, and maintenance staff</b>	

System Class	For USA Suppliers FDA 21 CFR 11 Section	ELECTRONIC RECORDS Requirement Summary	Y/N Reference:
		<ul style="list-style-type: none"> <li>• Verify that there is documented evidence of appropriate qualifications and training for               <ul style="list-style-type: none"> <li>• system developers</li> <li>• users</li> <li>• maintenance personnel,</li> </ul>               that will enable them to perform their assigned tasks (including contract and temporary staff).             </li> </ul>	Yes
2,3,4,5	11.10 (j)	<b>Establish and follow written accountability policies against falsification of records or signatures</b>	
		<ul style="list-style-type: none"> <li>• For systems not using E-sigs, this section is not required (but is recommended). For E-sig systems, this section is covered under “Electronic Signature Requirements” below</li> </ul>	N.A.
2,3,4,5	11.10 (k)(1)	<b>Control access to, and use of, system operation and maintenance documents (including SOPs)</b> <ul style="list-style-type: none"> <li>• For documents containing sensitive information (e.g., how to perform password maintenance), verify that controls are in place governing the distribution, access, and use of those documents</li> </ul>	User company
2,3,4,5	11.10 (k)(2)	<b>Implement change control with audit trails for system documentation changes (including SOPs)</b> <ul style="list-style-type: none"> <li>• Verify that there is a Change Control (or equivalent) SOP governing revisions to system documentation</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>• Verify that audit trails are maintained for changes to system documentation</li> </ul>	Yes
		<ul style="list-style-type: none"> <li>• Verify that audit trails are maintained electronically (and automatically) for systems documentation that is created and maintained electronically</li> </ul>	Yes
3,4,5	11.70	<b>... handwritten signatures executed to electronic records shall be linked to their respective e-records</b>	
		<ul style="list-style-type: none"> <li>• If handwritten signatures are used to attest for the data contained in electronic records so, verify that the handwritten signature is linked to the electronic record(s)</li> <li>• If the electronic record is changed, ensure that the signer is prompted to re-sign (via either manual procedures [SOP] or technical means)</li> </ul>	N.A.
<b>§ 11.30 Controls for Opens Systems (additional measures beyond § 11.10)</b>			

System Class	For USA Suppliers FDA 21 CFR 11 Section	ELECTRONIC RECORDS Requirement Summary	Y/N Reference:
2,3,4,5	11.30	<b>Implement document encryption &amp; digital signatures (suggested)</b>	
		<ul style="list-style-type: none"> <li>Verify that document encryption (or alternative technology) is used to protect the confidentiality of the electronic records on the system, as appropriate</li> </ul>	N.A.
		<ul style="list-style-type: none"> <li>Verify that digital signatures (or alternative technology) are used to protect the authenticity and integrity of the electronic records on the system</li> </ul>	N.A.

**Excerpt from Project Plan document  
(Under Documentation)**

The documents shall be prepared in such a way that relevant and applicable parameters of V model life cycle are covered appropriately. These documents (along with the generated print formats) will be stored and controlled as per the User Company policy xxxxxx.

Following documentation shall be used for the OasisLIMS project:

Users manual

System concept including risk analysis and system feasibility  
Project plan including training plan / training log (format annexed)

User requirement specification  
Traceability matrix (against URS)  
Vendor audit

Functional specifications  
Traceability matrix (against FS)  
Business process diagram  
Hardware design / requirement specifications

Software installation acceptance testing (IQ report)  
Traceability matrix (against IQ)  
System / user acceptance testing  
Test protocol results  
Problem resolution forms  
Operational / performance qualification report  
Traceability matrix (against OQ/PQ)  
Validation summary

**Excerpt from Project Plan document  
(under Project scope)**

As the package is an off-the-shelf, proprietary product of M/s Oasis, and is already designed, constructed, integrated, the validation activity will not cover the following activities under V model life cycle:

1. Software design specification (under design phase)
2. Design review (under design phase)
3. Software module specification (under construction phase)
4. Code the modules (under construction phase)
5. Software module testing (under construction phase)
6. Review and unit test the modules (under construction phase)
7. Software integration testing (under testing phase)

A certificate to this effect shall be obtained at the time of acceptance testing, for recording the same by the User Company.

**Excerpt from Project Plan document  
(Under Training)**

Oasis will conduct 3 days on-site training after the software is installed and system acceptance phase is completed. The company will organize interactive sessions and group instruction during training. Oasis team will remain on-site during implementation of software to provide on-the-job training to operators and users.

During training those who are directly or indirectly related with the system, will know in detail what their roles will be, how they can make efficient use of the system and what the system will or will not do for them. Both system operators and users need training.

Training will include the operation of the system itself, with proper attention being given to data handling techniques. Users of system will be properly trained in methods of entering, editing, deleting and inquiring records.

Training will ensure familiarization with procedures, and will involve working through the sequence of activities needed to use the system on an ongoing basis.

The necessary knowledge to use the basic functions of the new system will be provided to the concerned technical staff. Training logs shall be maintained.

User company would nominate a LIMS administrator. This person would have training in administrative activities, like servicing requests for access to additional functions / options / new users or other adhoc requests. He would also be trained in periodic house keeping activities like archiving and purging of the old data etc. This person would prepare SOP for all these activities and administer for the user company's site.

Maintenance of communication links and other hardware on the site would be co-ordinated through authorised user company's IT staff.

***Excerpt from FS***

Security Requirements within OasisLIMS:

This shall cover system security within the LIMS application. It shall provide several levels of security to ensure that each user has access to only those tasks for which he is responsible. The following features shall be provided under security system to secure OasisLIMS for Windows.

<b>Req. #</b>	<b>Details</b>
Sec 1	An account must be created in LIMS for each user before the user may gain access to the system. The account must specify the user's full name and assigned LIMS authority level, user password.
Sec 2	Access to create user accounts shall be restricted to the LIMS Administrator.
Sec 3	User accounts shall be prohibited if a user no longer requires access to the system.
Sec 4	Users must enter a confidential password at the time of entry to LIMS.
Sec 5	A password shall be assigned initially when a user's account is created.
Sec 6	In the event that a user forgets the password, it shall be possible for the LIMS Administrator or LIMS Coordinator to reset the password.
Sec 7	The user shall be able to change his password at any time.
Sec 8	No user, with exception of the LIMS Administrator, shall have access to modify LIMS data external to the LIMS. In such cases, access is controlled by approved procedures and is fully documented.
Sec 9	Logs shall be maintained recording user access to the system and identifying all reports that are printed in audit trails.
Sec 10	User access shall be controlled by menu options. Users can execute roles based only on their assigned menu options. A menu option can be assigned to one or more users.
Sec 11	An authorized administrator shall be able to assign or remove access to specific application functions.
Sec 12	The system shall provide the ability to ensure that menu options restricted from a user cannot be seen by the user.
Sec 13	The system shall provide and maintain a user log of the time and date of login and functions accessed. The audit trail log shall contain date, time, user name, old value, new value and reason for change.

Sec 14	The system shall allow the application or operating system to automatically lock user account after three (3) unsuccessful password attempts.
Sec 15	Illegal attempts to login into OasisLIMS for Windows shall be recorded in background by its security system with the information used while breaking security such as user identification, password tried, date and time. Only OasisLIMS administrator shall have the right to access this report.
Sec 16	The system shall support user and system audit trails of transactions.
Sec 17	Oasis LIMS system shall provide password aging feature which shall be programmable by system administrator.
Sec 18	The length of the password shall be minimum 8 characters with at least two numerical and two alphabetical characters in it. The password shall be case sensitive.