# Logilab SDMS – 21CFR PART 11

# COMPLIANCE STATEMENT

**Agaram Technologies (P) Ltd**
76 Nelson Road, Aminjikarai
Chennai 600 029
India
Phone: +9-44-42082005, +91-44-42189406
info@agaramtech.com
www.agaramtech.com

# Contents

# Agaram's Logilab SDMS 21 CFR Part 11 Assessment

**Introduction**

CFR Part 11 of title 21 of the Code of Federal Regulations; Electronic Records; Electronic Signatures sets forth the requirements for the creation, modification, maintenance, archival, retrieval, and transmittal of electronic records and also the use of electronic signatures when complying with the Federal Food, Drug and Cosmetic Act or any other Food and Drug Administration (FDA) regulation. These rulings became law in March 1997. Since that time, both industry and the FDA have been working to interpret the meaning and intent of Part 11. The FDA has created several documents with the assistance of industry representatives, to offer guidance in interpretation of the requirements. Even with these efforts, the requirements are still somewhat of a moving target. Agaram is continuously monitoring the opinions of the FDA to ensure continued compliance with the requirements.

This document presents the requirements set forth in 21 CFR Part 11, along with Agaram's own interpretation of the requirements with respect to its product LogiLab.

| | | |
|---|---|---|
| System Name: | Logilab SDMS | |
| Type: | Scientific Data Management System | |
| Manufacturer: | Agaram Technologies (P) Ltd | |
| Supplier: | Agaram Technologies (P) Ltd | |
| Is the system supposed to be used as a closed or open system? | ☑**closed** (Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.)<br>Please fill in subpart **A, C, D, E, F, G** | ☑**open** (Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.)<br>Please fill in subparts **B, C, D, E, F, G** |
| Assessment done by: | QA Team, Agaram Technologies (P) Ltd | |

## Subpart B – Electronic Records §11.10 Controls for Closed Systems

| Section | Section Requirements | LogiLab Response |
|---|---|---|
| §11.10 (a) | Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records. | Product is tested and released for customers. It is also validated against operational qualification tests which are performed during implementation with relevant documentation to justify the same. The product can discern invalid and altered records by way of not allowing invalid data and automatic versioning of altered records |
| §11.10(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. | Data can be downloaded for copying, reviewing and printing from relevant parts of the application by users with appropriate privilege. The original data will reside within the system in electronic format for any verification. |
| §11.10(c) | Protection of records to enable the accurate and ready retrieval throughout the records retention period. | Data within the system is protected from un-authorized access or modification by applying security and access control measures. Data or records within the system can be accurately retrieved throughout the records retention period |
| §11.10(d) | Limiting system access to authorized individuals. | LogiLab system is only accessible through a valid “user- name” and “password” which gives access to only authorized users |

| | | |
|---|---|---|
| §11.10(e) | Use of 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. Such audit trail documentation shall be retained for a period of at least as long as that required for the subject electronic records and shall be available for agency review and copying. | System generates audit trail of user(s) login, log-off, user actions that create, edit, delete (records cannot be deleted in LogiLab SDMS). System audit trails are automatic and cannot be intervened or modified by users. User audit trails are available at relevant areas of application that authenticates the action by way of requesting a user name, password, pre-defined reason and a comment. The audit trail records consists of user name, LogiLab client ID, action performed, change in data if any along with server date/time stamp. The audit trail is a non editable data, searchable, printable, and exportable for review. Since no data can be deleted within the system and the system has a built-in versioning capability old or previous versions of data does not get obscured. |
| §11.10(f) | Use of operational system checks to enforce permitted sequencing of steps and events as appropriate. | System has validations in place that allows only valid sequence of operations can be performed. Also there is no sequence or operation available within the system to modify any electronic records after it has been captured. |
| §11.10(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. | Anonymous access to the system is not allowed. Only authorized user can access the system, provide input and perform operations. No record can be altered after capture. |
| §11.10(h) | Use of device (e.g. terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction. | System works in automated fashion to fetch data generated by instruments and it checks for source of data and its validity before being uploaded to server. Any change in source data like creation, editing, deleting is detected by the system and audit trailed |

## Subpart B – Electronic Records §11.10 Controls for Closed Systems

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.10(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. | LogiLab administrators and end-users are adequately trained to use the system for the intended purpose. Since LogiLab is an automated system end-user simply does not need to have any special skills to use the system, other than login to the system and view the data captured. |
| §11.10(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. | Whenever electronic signatures are to be executed, system prompts for user name, password, pre-defined reason, comments and conveys the literal meaning or implications of the action about to be taken is displayed such that it takes cognizance of the person performing such action |
| §11.10(k)(1) | Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of Documentation for system operation and maintenance. | It is the responsibility of the user organization to develop policies regarding controlled access to system manuals and system related documentation which are provided along with the product. |
| §11.10(k)(2) | Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation. | Systems necessary documentation is made available time to time whenever an update is provided to customer which are version and release controlled. |

## Subpart B – Electronic Records §11.30 Controls for Closed Systems

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.30 | Controls for Open Systems | LogiLab SDMS is a closed system |

## Subpart B – Electronic Records §11.50 Signature Manifestations

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.50(a)(13) | Signed electronic records shall contain information associated with the signing that clearly indicates all the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. | During each e-signature event we record the user name, date/timestamp, reason for e-sign, meaning of the action and with respective comments. |
| §11.50(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). | Whenever an E-signature is applied to an electronic record it appears as an electronically signed as part of the electronic record in the user display |

## Subpart B – Electronic Records §11.70 Signature/Record Linking

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.70 | 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. | LogiLab doesn't have any provision to remove or modify an e-signature applied to an electronic record. It is always linked to specific record on which the signature was applied. |

## Subpart C – Electronic Signatures §11.100 General Requirements

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.100(a) | Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. | Each individual in the organization will have their unique user ID and password, which cannot be reused or reassigned to any other user. |
| §11.100(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. | This activity is beyond the scope of the system. It is the responsibility of the organization to establish policies and procedures to verify the identity of the individuals who are authorized to use the electronic signature. |
| §11.100(c)<br>§11.100(c)( 1)<br>§11.100(c)( 2) | 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. 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. 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. | Each organization is required to notify the FDA in writing of their intention to use electronic signatures. It is the responsibility of the organization to perform this notification. |

## Subpart C – Electronic Signatures §11.200 Electronic Signature Components and Controls

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.200(a)(1) | Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. | Every user is verified based on 2 different distinct components (1) user name and (2) password before he can apply a e-signature for the electronic record in LogiLab |
| §11.200(a)(1)(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 of the electronic signature components. | For every e-signature applied the user has to enter all the signature components within LogiLab system |
| §11.200(a)(2) | Electronic signatures that are not based upon biometrics shall: Be used only by their genuine owners; and | user with valid user name and password only can access the system and apply e-signature |
| §11.200(a)(3) | Electronic signatures that are not based upon biometrics shall: 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. | This cannot be enforced by the system if passwords are shared by individual users. However when such attempts are made with mistakes will be audit trailed by the system. |
| §11.200(b) | Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. | Biometrics is not used by the system |

## Subpart C – Electronic Signatures §11.300 Controls for Identification Codes/Passwords

| Section | Section Requirements | LogiLab Approach |
|---|---|---|
| §11.300(a) | 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: (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. | System allows only unique combinations of user name and password. No two users can have either the user name or password as the same. |
| §11.300(b) | Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). | Password ageing policy is available under LogiLab password policies. |
| §11.300(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. | When loss of password or compromise is reported such user's passwords can be reset by the administrator. In the event of employees leaving the organization their user accounts can be retired. Also temporary de-activation and activation of specific users is possible |
| §11.300(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. | System is fully integrated with security policies that prevent any form of undetected or unauthorized access to the application. Any such attempt is audit trailed and such user's accounts are automatically locked after a preset failed attempts. |
| §11.300(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. | This is not applicable as there are no devices that bear or generate identification code or password information |