This document reflects the technical and procedural requirements for part 11 compliance.

|  |  |  |
| --- | --- | --- |
| System Name: | Aqualink4 Part11 | |
| Type: | Software | |
| Version / Date: | 24-Jul-2013 | |
| Manufacturer: | Decagon Devices/Aqualab | |
| Supplier: | Decagon Devices Aqualink | |
| Assessment completed by: | Joran Beasley/Software Engineer(Decagon Devices)/24-Jul-2013 | |
| Approved by System Owner: | Date: | Signature: |
| Approved by QA: | Date: | Signature: |

**Note:**

The use of the word “shall” & “must” indicates a mandatory requirement.  
The use of the word “should” indicates recommended measures as opposed to mandatory requirements or directs activities in tailoring an activity-specific standard, in that the activity must include, exclude, or tailor the requirement, as appropriate.  
The use of the word "may" & “could” is similar to "should", in that it designates optional requirements.

| **21 CFR11**  **Reference** | **Decagon Interpretation** | **Manufacture Solution** | **Compliant?** | **Proposed Measure**  **(if not compliant)** | **Final Compliance Status Statement** |
| --- | --- | --- | --- | --- | --- |
| **General** | | | | | |
|  | Is a Quality Management System implemented?  Is the QM System certified? | ISO  9001:2008  Yes | ☑ Yes  No |  |  |
| **Electronic Records** | | | | | |
| § 11.10 (b) | The Computerized System (CS) **must** either support the viewing of e-records or the generation of valid paper copies. The CS **should** provide viewing & printing capabilities for all relevant e-records. (In certain cases, controlled database queries or accurately performed screen dumps may satisfy this requirement.). | Supports both viewing and printing | ☑ Yes  No  N/A |  |  |
| § 11.10 (b) | The CS should allow for the export of e-records to portable file formats, preferably automatically. Recommended formats are: *Common/ global XML standards, ANSI, PDF, SGML.* | Export as PDF supported also (CSV/XLS) | ☑ Yes  No  N/A |  |  |
| § 11.10 (c) | Preferably e-records should be archived to write-protected media (Write-once Read-many media like WORM tape media or optical media) or archiving solutions with WORM type safeguards should be used. | This would fall under the user of the software to export records to write once read many media. | Yes  No  ☑ N/A |  |  |
| § 11.10 (c) | If automated archiving is put into practice, transaction safeguards should prevent the e-records in the source system from deletion until confirmation that they have been successfully archived. | e-records are protected from deletion | Yes  No  ☑ N/A |  |  |
| § 11.10 (d) | If the CS is accessed through workstations which bear more than one application, the application must have its own security layer (*e.g. application specific User ID/ password versus workstation “power-up” User Id & password*). | Uses the windows login credentials. | Yes  ☑ No  N/A |  |  |
| § 11.10 (d) | Ensure that the CS has a security mechanism that uses at least two distinct identification components (*e.g. User ID/ password, PKI mechanisms*) or biometrics. | Requires workstation login by windows user with required permissions/groups  secondary password requirement on CS startup | ☑ Yes  No  N/A |  |  |
| § 11.10 (d) | The CS must allow for the use of individual accounts, shared accounts for access levels other than read are not acceptable. | Yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (d) | The CS should provide a mechanism to lock out/ interrupt access of any user after a configurable period of non-attendance/ non-interaction with the system (Recommendation 15 minutes at a maximum). Password protected screensavers are acceptable means to fulfil this requirement provided that the security mechanisms of the application are not compromised. | Windows Security Administration should enforce lockouts | ☑ Yes  No  N/A |  |  |
| § 11.10 (d) | The implementation of the lock out process should be well investigated in regard to safety needs. Access to safety relevant functions & operations must always be possible and should be given priority. It is recommended to purchase CS with safety relevant functions and operations detached from general system security mechanisms.  **§ 11.10 (d) – SYSTEM ACCESS** | See: Windows Security Accounts Administration | ☑ Yes  No  N/A |  |  |
| § 11.10 (d) | If technically possible passwords must be stored in the CS in encrypted form. In case were encryption of passwords is not possible, the file(s) containing passwords and user-Ids must be secured by technical means and their access strictly controlled (no read option for any user, SOP/strict instruction for administrators about password file handling, password file not accessible for users). | Uses windows security system. | ☑ Yes  No  N/A |  |  |
| § 11.10 (d) | When password entry fields are shown on the screen, password entries must be obscured (e.g. "\*\*\*\*\*\*\*\*\*"). | yes | ☑Yes  No  N/A |  |  |
| § 11.10 (d) | The system should allow for quality passwords (at least 8 alphanumeric characters) and enforce their use. | See windows password settings | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | Computer generated audit trails should contain information about:  - person/ equipment performing the activity (WHO)  - date and time of its execution (WHEN)  - (WHAT) was changed/ done  - the reason for the activity (WHY) if appropriate. | yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | Computer generated audit trails should at least record the hour and minute and must be as precise as required by the business process (e.g. to verify correct sequencing of events). | yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | Time & date settings should be subject to rigorous control to ensure the accuracy of time stamps, the CS should provide the ability to restrict access to time settings. Users should not be able to change time & date settings. | Yes (uses system timestamps / windows date settings) | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | CS spanning multiple time zones should be able to display & print the time zone used with the time stamp. | no | Yes  ☑ No  N/A |  |  |
| § 11.10 (e) | The CS should have a mechanism to prevent that changes to e-records obscure or destroy the original recorded information. Secured references/ pointers from computer generated audit trails to the original recorded information are acceptable. | Industry standard AES encryption and checksums as well as highly coupled audit data should prevent tampering with any data | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | If audit trail information is not part of the record itself, the CS must implement mechanisms to establish a secured link between audit trail & the respective record. | yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | The ability to change computer generated audit trails must be restricted to a minimum number of individuals and to duly authorize personnel. | Audit Trail is locked from editing. | ☑ Yes  No  N/A |  |  |
| § 11.10 (e) | It is recommended to purchase CS, which have implemented search tools, data filter and/ or report functions for the audit trail to support its review. | Yes. Filtering of data is enabled. And there are many options for viewing the audit trail of given record(s) | ☑ Yes  No  N/A |  |  |
| § 11.10 (f) | If appropriate, the CS should support the logical execution of workflows, sequences and programs:  This concerns in particular:   * Sequential data entries (enforce a logical sequence where order of entry is critical) * Sequential execution of controlled tasks where the order is critical * Sequential data processing (i.e. do not allow to take a decision before all results are feed into the system) * Enforce logical review / approval sequence (make sure approvals are only occur once all pre-conditions are satisfactorily fulfilled) | yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (g) | The CS should apply authority checks to ensure that only authorized individuals can  - make use of system functions & features  - electronically sign a record  - create, modify, inactivate/ logically delete, delete records  - access input and/ or output devices  - perform operations at hand. | Yes through windows security management. There is no electronic signing implemented | ☑ Yes  No  N/A |  |  |
| § 11.10 (g) | Records may be linked to an authorization code that identifies the title or organizational unit of those individuals who are allowed to modify and/ or sign records. Based on this authorization code, the CS should provide or reject access to records/ e-signature functions. | Most of each record is not editable by any user. Any user who is eligible to use the software on a given machine will be able to add annotations and/or modifiable data to records. The administrators only additional role is to approve rollbacks due to attempted tampering or database corruption. | Yes  No  ☑ N/A |  |  |
| § 11.10 (g) | The CS should enforce record specific access rights (*e.g. only the originator of a record is allowed to modify it*) whenever the business process asks for such controls. This can be achieved by maintaining a list of those records, an individual is allowed to modify/ sign. Before access to a record is provided for an individual, the CS should check if this record is part of the individual’s list. | Most of each record is not editable by any user. Any user who is eligible to use the software on a given machine will be able to add annotations and/or modifiable data to records.  The administrators only additional role is to approve rollbacks due to attempted tampering or database corruption. | Yes  No  ☑ N/A |  |  |
| § 11.10 (g) | Records in scope of this guideline which are automatically captured by a CS (*e.g. process data* …) must not be modified. The CS should provide mechanisms that prevent users -except system administrators- from having access other than “read” to such records. If the CS lacks such controls, computer-generated audit trails must be implemented. | Audit trails are implemented. Records are automatically captured from device. Most of each record is not editable by any user. Any user who is eligible to use the software on a given machine will be able to add annotations and/or modifiable data to records.  The administrators only additional role is to approve rollbacks due to attempted tampering or database corruption. | Yes  No  ☑N/A |  |  |
| § 11.10 (h) | In cases where the physical identity of a HW item/ device/ equipment is relevant, the CS should check the identity of such devices | yes | ☑ Yes  No  N/A |  |  |
| § 11.10 (h) | The CS should not have a mechanism to complete empty data fields within a record without the opportunity for the user to review them. OR: Features that enter automatically information into a field when the field is by-passed should not be used. | there is no ‘auto complete’ functionality built in | ☑ Yes  No  N/A |  |  |
| § 11.10 (k) | The vendor should provide accurate and updated documentation for system operation and maintenance | 4.2 version of the software only has help documentation available online.   4.3 has help files included | Yes  ☑ No  N/A |  |  |
| § 11.10 (k) | The new systems should be designed to support self-documentation of system parameters and configuration settings and changes including:   * Document version control (however the system should not have a switch for enabling / disabling version controls). * Automatic check-in / checkout procedures for documents and files, with an easy way to show differences between versions. * Self-documentation of "block" logic, with easy indication of changes made. * Self-documentation of configuration changes with indication of portions of code added, code deleted and code modified | We use subversion version control on our source.  within the software the audit trail contains all changes and revisions to editable data | ☑ Yes  No  N/A |  |  |
| **Electronic Signatures** | | | | |  |
| § 11.50 (a) | Ensure that all users are uniquely identifiable in the CS. Where the User ID is not the user’s full name, ensure it is traceable to the user’s full name.  **§ 11.50 (a)** | Managed by internal IT dept. linking windows accounts to personnel | Yes  No  ☑ N/A |  |  |
| § 11.50 (a) | The CS must record/ link  - the unique identifier of the person executing the signature  - the date & time of the signature  - the meaning of a signature (e.g. approval; review)  for/ to each signature event. Ideally, e-signatures should be applied directly to records. Alternatively, separate e-signature records are allowable if they are unambiguously linked with the record to which they apply. | e-signatures not supported | Yes  No  ☑ N/A |  |  |
| § 11.70 | It is recommended to purchase CS, which have implemented or have plans to implement technical link mechanisms such as hash functions. | Hash functions are used for each report generated based on the data in the report. | ☑ Yes  No  N/A |  |  |
| § 11.100 (a) | The CS must not accept duplicate user accounts. | Windows does not allow duplicate accounts | Yes  No  ☑ N/A |  |  |
| § 11.300 (b) | The CS should support password-aging processes (prompts for password renewal after 60 calendar days). | Windows Account Settings | Yes  No  ☑ N/A |  |  |
| § 11.300 (b) | The CS should allow for configuration of the password aging parameter.  The setting of the password aging parameter should be limited to duly authorized personnel only. | Windows Account Settings | Yes  No  ☑ N/A |  |  |
| § 11.300 (d) | Check that the system is able to lock an user account after a specified number of failed access attempts (*preferred option: 3 unsuccessful attempts until log out*). | Windows Administration | ☑ Yes  No  N/A |  |  |
| § 11.300 (d) | The CS should be able to detect potential misuse and notify the responsible individual. | Reports Violations to system administrator through the windows event log | ☑ Yes  No  N/A |  |  |
| § 11.300 (d) | The CS should be able to log unauthorized access attempts. | Yes | ☑ Yes  No  N/A |  |  |

Reason for change:

New.