White Paper

21 CFR PART 11 COMPLIANCE

SCHMIDT HAENSCH
innovators by tradition since 1864

21 CFR PART 11 COMPLIANCE

SCHMIDT + HAENSCH is a world-renowned manufacturer of precision measuring instruments and analytical systems based in Berlin, Germany. Founded in 1864, the company has a rich history in the field of optical measurement technology and has established itself as a global leader in the field of analytical instrumentation technology. With a focus on innovation and exceptional customer service, SCHMIDT + HAENSCH specializes in the production of polarimeters, refractometers, density meters, and other analytical instruments that are used in a wide range of industries. Their products are known for their accuracy, reliability, and robust design, making them a top choice for businesses around the world.

INTRODUCTION TO 21 CFR PART 11:

In 1997, the U.S. Food and Drug Administration (FDA) issued 21 CFR Part 11, a regulation that outlines requirements for electronic records and signatures in FDA-regulated industries, including pharmaceuticals, biotechnology, and medical devices. The regulation was established to ensure that electronic records and signatures are trustworthy, reliable, and equivalent to paper records and handwritten signatures.

21 CFR Part 11 requires that electronic records be created, managed, and maintained in a manner that ensures their authenticity, integrity, and confidentiality. Electronic signatures must also be trustworthy and legally binding, and they must be linked to their respective records to ensure accountability.

The full text of 21 CFR Part 11 can be seen at FDA website at: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11

ABOUT AQUISYS 3:

AQUISYS 3 is a comprehensive software solution for controlling and analysing data from SCHMIDT + HAENSCH refractometers, polarimeters, and density meters of the VariFamily. The software allows for real-time monitoring and control of measurement processes, data collection and analysis, and automated reporting. The software is designed to improve productivity, accuracy, and data integrity for laboratory applications.

This white paper explains the key regulatory requirements that apply to AQUISYS 3 software and how the software meets those requirements. This document, however, does not provide comprehensive information on 21 CFR Part 11 or legal advice for full compliance.

Detailed checklists for the specific requirements are available on requests and are subject to a valid quotation for an instrument.

On the following pages we are presenting the general solutions in AQUISYS 3 (regular font) in comparison to the original 21 CFR part 11 guideline text (bold italic font).

As it may be possible that you have specific solutions implemented in your CFR compliance management please contact us for more detailed information.

SUB-PART B: (ELECTRONIC RECORDS)

Control for closed systems

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:

a. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Instrument validation is done through IQ, OQ, and PQ by following validation protocol and results are documented. Software validation is done to ensure accuracy and reliability of data storage and retrieval. Invalid data is be controlled through use of electronic signatures. Records can´t be altered. All data is encrypted inside the instrument which guarantees data integrity at all times.

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.

AQUISYS 3 provides complete information about recorded data on the system as well as in digital format in the form of PDF or CSV, which can be printed. The printed data contains date and time stamps of when the data was printed with a watermark so that the data is traceable by the agency. No data is extracted from the instrument. All reports are only a mirror image of the original raw data.

c. Protection of records to enable their accurate and ready retrieval throughout the records retention period.

All raw data is stored encrypted, tamper-proof and permanently in the device and in encrypted backups. The electronic records cannot be changed, added to or deleted. This ensures the authenticity, integrity and confidentiality of data.

d. Limiting system access to authorized individuals.

Only authorized persons can access the system. Additionally, role-based user permissions is implemented to ensure that users only have access to the features and functions that are necessary for their job functions. An automatic logout after a defined time can be set.

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 at least as long as that required for the subject electronic records and shall be available for agency review and copying.

All relevant processes and configuration changes are stored in the audit log with date and time stamp and user ID. This means that all changes can be tracked to the second and without gaps. The data in the audit log cannot be subsequently changed either. The audit log can be exported as a text file, but the original data remains encrypted on the device.

f. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

AQUISYS 3 has provisions for creating methods in a system to enforce permitted sequencing of steps and events. Method are pre-set orders of events/commands that occur when a user clicks on an action button.

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.

AQUISYS 3 contains an user management matrix which reflects the typical user hierarchy creating different users and assigning role-based user permissions to ensure that users only have access to the features and functions that are required for their current job functions.

h. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

AQUISYS 3 includes features that allow data input and operational instructions to be provided by creating methods and sequences.

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.

SCHMIDT + HAENSCH system developers are well qualified, trained, and experienced, and their qualifications and experience reports are well-documented. Additionally, the company is ISO 9001 qualified and follows all guidelines when developing the product. The service engineers and external maintenance engineers are also well trained and experienced. For users of the system SCHMIDT + HAENSCH is offering training sessions to provide the necessary knowledge and understanding of the use of AQUISYS 3

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.

This requirement is beyond the scope of AQUISYS 3 and is the responsibility of system owner to have this written policies in place.

k. Use of appropriate controls over systems documentation including:

1. Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

The instrument is supplied with document for operation and its maintenance. However, it's the responsibility of system owner to control its distribution, access and its use.

2. Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

SCHMIDT + HAENSCH maintains revision and change log documents for AQUISYS 3. The change log process includes version and revision numbers for each software update. Additionally, the software includes "about" section that displays the current software version. The system owner is responsible for maintaining the documents of any other further changes made at site.

Control for open systems

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.

SCHMIDT + HAENSCH instruments operate as closed systems hence these regulations are outside their scope. As mentioned in the comment to point b) all data exported from the instruments data base is only a mirror image of the original data.

Signature Manifestations

a. Signed electronic records shall contain information associated with the signing that clearly indicates all of 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.

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

All electronic and printed records contain the data needed to comply with regulations. The data includes date, time, action taken by user (Signed as removed, rejected, signed), role of the user and comment given by the user. On printed records even the date, time and user who printed this is mentioned.

Signature/record linking

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.

Electronic signatures are unique to individual users and an integral component of electronic records. Printed records can be linked to the original data according to the user information printed.

SUB-PART C: (ELECTRONIC SIGNATURES)

General Requirements

a. Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

A unique electronic signature is assigned to individual user in the form of unique username and is not reused or reassigned to anyone else. Once set the username can no longer be changed or deleted to guarantee traceability.

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 requirement is beyond the scope of AQUISYS 3 however system owner must take appropriate measures to verify the identity of individual users.

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.

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.

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.

This requirement is beyond the scope of AQUISYS 3 however the system owner must submit a certification to agency that electronic signatures used in their system are intended to be legally binding and equivalent to traditional signed documents.

b. Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

This requirement is beyond the scope of AQUISYS 3 since we use digital signatures based on user name and password and not biometrics.

Electronic signature components and controls

a. 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 individual has unique user ID and has to set a unique password before accessing the system. When signing a record at least one of these unique components must be re-entered.

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.

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.

AQUISYS 3 is operated in closed environment therefore it does not require subsequent signing and is thus out of scope for software. Still the feature can be enabled for additional data integrity.

2. Be used only by their genuine owners; and

This requirement is to be followed by customers to ensure that only genuine and qualified users be granted access to system and software.

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.

This requirement is beyond the scope of AQUISYS 3 since only individual users can have an access to system and software. The instrument administrator has the ability to deactivate a user or change passwords in case of misuse.

b. Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

This requirement is beyond the scope of AQUISYS 3 since we use digital signatures based on user name and password and not biometrics.

Controls for identification codes/passwords

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.

Each individual user has unique username and password. The client IT and system administrator should ensure that no two individuals have same username and password combination. AQUISYS 3 checks password history and user name duplicates.

b. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

AQUISYS 3 software system supports password aging and there is provision for password expiry and renewal which can be adjusted (never, monthly, annually) as per customer requirements.

c. Following loss management procedures to electronically deauthorize 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.

The customer is responsible on how to handle lost or forgotten passwords. In particular, the administrator is in charge of regenerating forgotten passwords; however, in the event that the administrator is restricted from access due to three incorrect log-in attempts, the client must contact SCHMIDT + HAENSCH for assistance. Please adhere to the manual‘s retrieval procedure.

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.

A number of unsuccessful login attempts before the user is blocked can be determined by the administrator. Passwords can be generated by the administrator, and each unsuccessful login is noted in the audit trail.

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 requirement is beyond the scope of AQUISYS 3 since it does not require any tokens or cards to generate code or password.

Please report any missing points to us. We do not take liability for the completeness of this comparison or the valid phrasing in this document. This is under no circumstances be understood as a legal advice on 21 CFR part 11 compliance management.

All the mentioned points are taken from: https://www.ecfr.gov/current/title-21/chapter-I/subchapter-A/part-11 Any liability is transferred back to the original creator of the above-mentioned document.