

Self-assessment of Serstech 100 Indicator & Serstech ChemDash Pharma regarding compliance with FDA 21 CFR Part 11 e-records;e-signatures

Document ID

Statement compliance v1.1

Revision date

June 2020

General status

Approved



Serstech AB

info@serstech.com

Phone: +46 46 255 112

Åldermansgatan 13



SE-227 64 Lund

Sweden

Approvals

Revision	Date	Written by	Reviewed by	Approved by
Version 1.1	June 2020	Evangelia Mitsou (<i>Senior Applications&Quality Specialist</i>)	Peter Billsten (Technical Sales Director)	Peter Billsten (Technical Sales Director)

Modifications

Version no.	Date	Change details	Page(s) No.
1.1	22/06/2020		

Index

1.Purpose 4

2.Documents of Reference 5

3. Status of the whole system (Serstech 100 Indicator & ChemDash Pharma)..... 6

4.Analytical report of 21 CFR Part 11 compliance 7

4.1 Introduction to software's User Management concept and User Hierarchy levels 7

4.2 Creating the Audit and Authentications logs (Audit Trail) 9

4.3 Database backup and restore (Data retrieval)..... 10

5.Third part 21 CFR Part 11 Compliance Checklist (Qualio.com)..... 12

Appendix 1 13

Appendix 2 16

1. Purpose

This document describes the Serstech 100 firmware and PC software compliance with the US Food and Drugs Administration's Code of Federal Regulations, Chapter 21, part 11 (FDA 21 CFR Part 11). The Serstech 100 Indicator provides processed measurement data and results according to its function (analytical hand-held Raman spectrometer). The Serstech ChemDash Pharma PC software provides data and user management.

The design and development of the applications respect the FDA initial requirements. FDA compliance embraces complete systems including hardware, software, documentation, file and user management, user rules of conduct, company security standards, etc...

2.Documents of Reference

TITLE 21
FOOD AND DRUGS
CHAPTER I

FOOD AND DRUG ADMINISTRATION,
DEPARTMENT OF HEALTH AND HUMAN SERVICES
PART 11
GENERAL PROVISION
ELECTRONIC RECORDS
ELECTRONIC SIGNATURES

Contents:

Subpart A: General Provisions

11.1 Scope.

11.2 Implementation.

11.3 Definitions.

Subpart B: Electronic Records

11.10 Controls for closed systems.

11.50 Signature manifestations.

11.70 Signature/record linking.

Subpart C: Electronic Signatures

11.100 General requirements.

11.200 Electronic signature components and controls.

3. Status of the whole system (Serstech 100 Indicator & ChemDash Pharma)

According to gap analysis made for the firmware(embedded software on the device) and PC software development standards towards the fulfillment of the requirements for the 21 CFR Part 11, "Serstech 100 Indicator and Serstech ChemDash Pharma are considered as a Closed system, characterized as Computerized System category C.

4. Analytical report of 21 CFR Part 11 compliance

4.1 Introduction to software's User Management concept and User Hierarchy levels

As required by FDA CFR11.200.1, Serstech's ChemDash Pharma software employs the identification of the operating system (Windows 7,8 and 10 versions 32 or 64 bits). General access limitation can be achieved using Microsoft's integrated User Management. It remains the sole responsibility of the customer's IT department to configure, manage and maintain these settings.

ChemDash Pharma is using user hierarchy levels such as Super Admin/Admin/Active/Disabled. Please find all user levels in ChemDash Pharma and their privileges described in the Table 1 below:

Table 1: User Hierarchy levels in ChemDash Pharma

User Hierarchy levels in ChemDash Pharma application	Privileges
Super Admin	<p>The Super Admin has the right to all functions in the application:</p> <ol style="list-style-type: none"> 1.Import user accounts to the system 2.Set other accounts as Admins and Active/Disable them 3.Create instrument Admin/Users and correlate them to a ChemDash user account 4.Manage their Indicators, monitor their status and manage instrument Users 5.Manage all measurements made with the Serstech 100 Indicator 6.Create database backups and restore the whole database in case of need 7.Set PIN-codes and their expiration date for the Instrument
Admin	<p>Admin is a privileged user and can perform most of the actions with restriction in the administrative rights that are listed above for Super Admins</p>
Active	<p>A user account that is set to Active can only view reports, measurements, and libraries. An Active role can also export measurements but is absolutely restricted from any administrative function</p>

Disabled	This is for a person who leaves the company but still its credentials remain to the system. This user's account can be set to Disabled from the system
-----------------	--

After the User has successfully gone through the ChemDash Pharma Installation process, the Admin of the PC where the ChemDash Pharma application is installed will be automatically the Super Admin of the application. Image 1 below shows the preview of the front page in the application. As we can see, on the top right there is the username (email or name) of the Super Admin in the application (name@server.com).

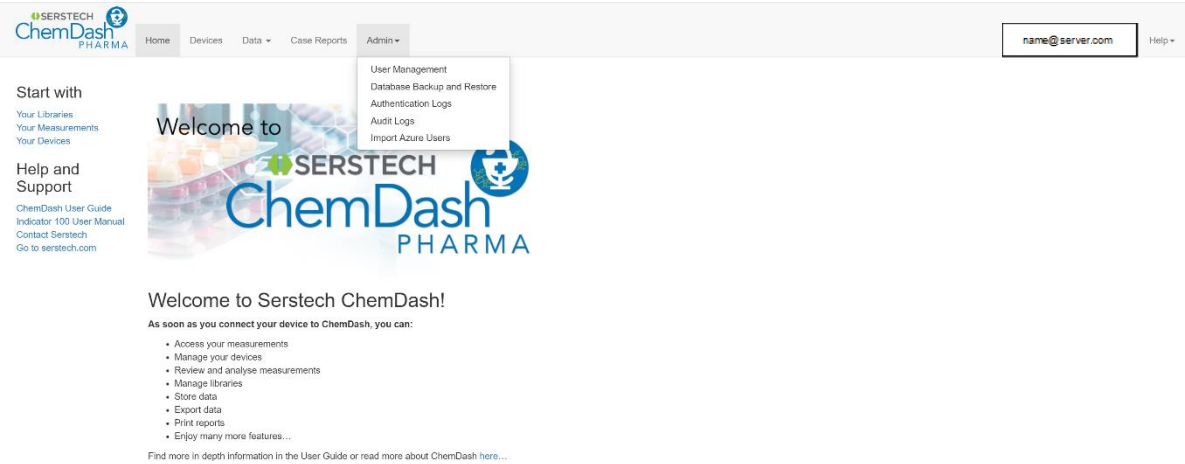


Image 1:Preview of the frontpage in ChemDash Pharma

The implementation of the access rights in the application Instrument's measurement software provides the module in which the software functionalities are available and recorded in a secured log file if they have a direct influence on the reliability and validity of the measurements. The Super Admin in the ChemDash Pharma installation is the one who has the right to access the User Management field, import and edit the hierarchy level in other users within the same domain (Image 2).

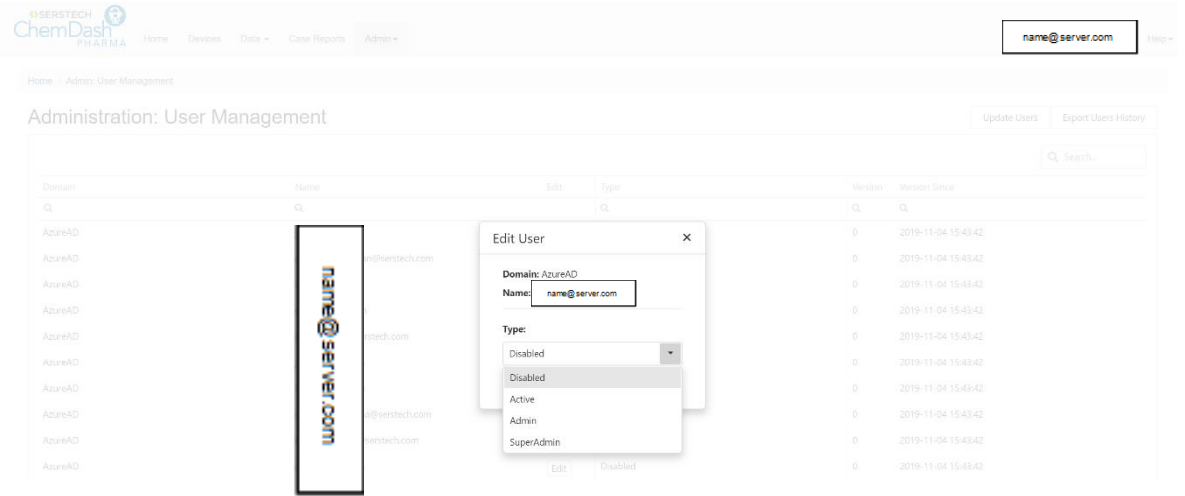
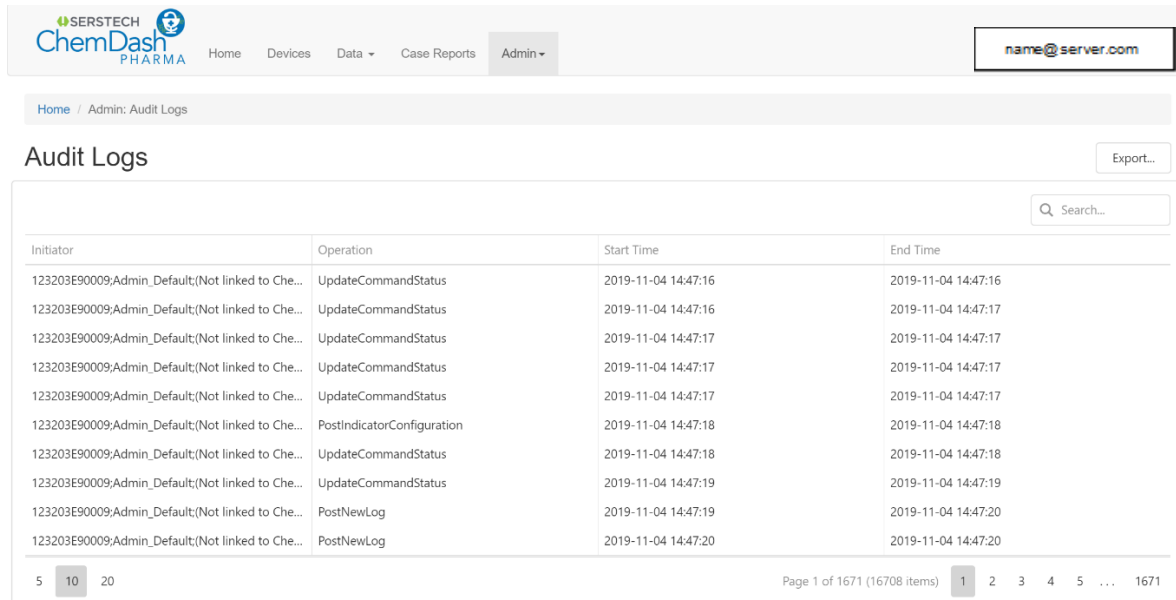


Image 2:User Management Administration section

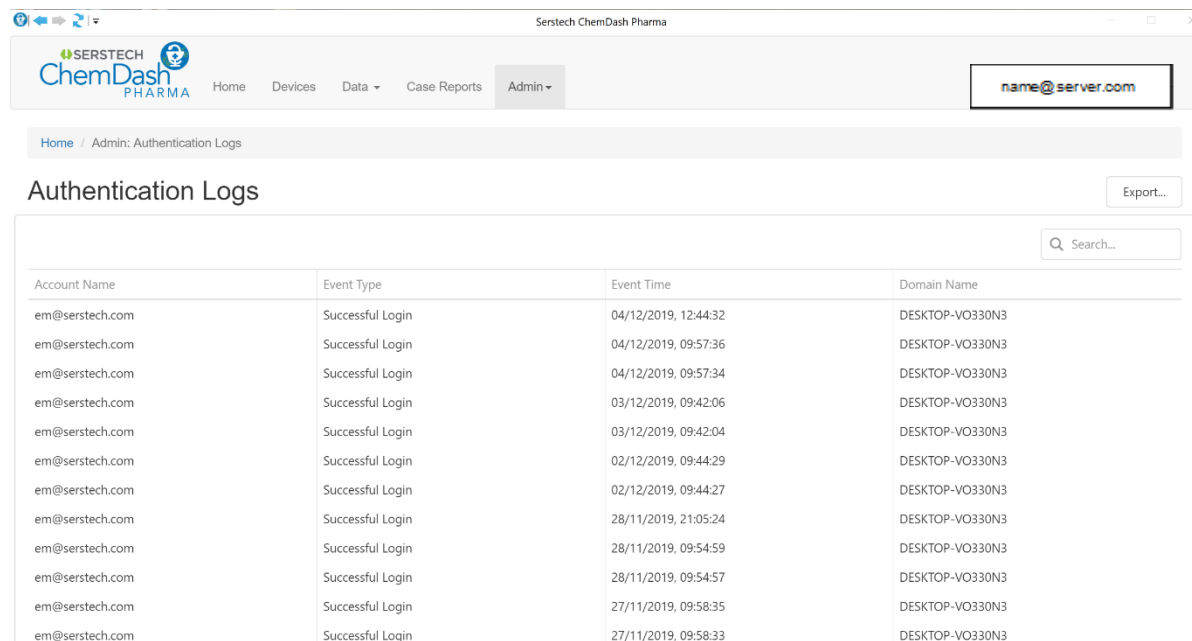
4.2 Creating the Audit and Authentications logs (Audit Trail)

The logs are created automatically the first time that the Audit trail feature is selected. Audit and Authentication logs can be also exported in the Windows log format (.csv) and stored with the operating system files. Logs can be used for external audits (such as FDA audit). In the Super Administration mode, the following dialogue boxes appears (Image 3 and 4).



Initiator	Operation	Start Time	End Time
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:16	2019-11-04 14:47:16
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:16	2019-11-04 14:47:17
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:17	2019-11-04 14:47:17
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:17	2019-11-04 14:47:17
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:17	2019-11-04 14:47:17
123203E90009;Admin_Default;(Not linked to Che...	PostIndicatorConfiguration	2019-11-04 14:47:18	2019-11-04 14:47:18
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:18	2019-11-04 14:47:18
123203E90009;Admin_Default;(Not linked to Che...	UpdateCommandStatus	2019-11-04 14:47:19	2019-11-04 14:47:19
123203E90009;Admin_Default;(Not linked to Che...	PostNewLog	2019-11-04 14:47:19	2019-11-04 14:47:20
123203E90009;Admin_Default;(Not linked to Che...	PostNewLog	2019-11-04 14:47:20	2019-11-04 14:47:20

Image 3: Audit logs accessible only through the Super Administration mode



Account Name	Event Type	Event Time	Domain Name
em@serstech.com	Successful Login	04/12/2019, 12:44:32	DESKTOP-VO330N3
em@serstech.com	Successful Login	04/12/2019, 09:57:36	DESKTOP-VO330N3
em@serstech.com	Successful Login	04/12/2019, 09:57:34	DESKTOP-VO330N3
em@serstech.com	Successful Login	03/12/2019, 09:42:06	DESKTOP-VO330N3
em@serstech.com	Successful Login	03/12/2019, 09:42:04	DESKTOP-VO330N3
em@serstech.com	Successful Login	02/12/2019, 09:44:29	DESKTOP-VO330N3
em@serstech.com	Successful Login	02/12/2019, 09:44:27	DESKTOP-VO330N3
em@serstech.com	Successful Login	28/11/2019, 21:05:24	DESKTOP-VO330N3
em@serstech.com	Successful Login	28/11/2019, 09:54:59	DESKTOP-VO330N3
em@serstech.com	Successful Login	28/11/2019, 09:54:57	DESKTOP-VO330N3
em@serstech.com	Successful Login	27/11/2019, 09:58:35	DESKTOP-VO330N3
em@serstech.com	Successful Login	27/11/2019, 09:58:33	DESKTOP-VO330N3

Image 4: Authentication logs accessible only through the Super Administration mode

Actions recorded in the event log (Audit-trail) showing who logged into the device, the date and timestamp of their logging in and from where they logged in. The Authentication

logs are regarding the PC ChemDash Pharma software status and as mentioned above, are accessible in human readable form both electronically and printable.

4.3 Database backup and restore (Data retrieval)

The Database backup and restore function can be accessed only under the Super Administration mode and allows only the Super Admin to schedule when and where the database backup will be created and stored. The Super Admin can decide if the database will create backups on a daily or weekly basis. The Super Admin can also trigger a backup if needed. The import of a backup will allow the database to restore itself in case of failure on the local PC where the ChemDash Pharma application is installed, please see image 5 below.

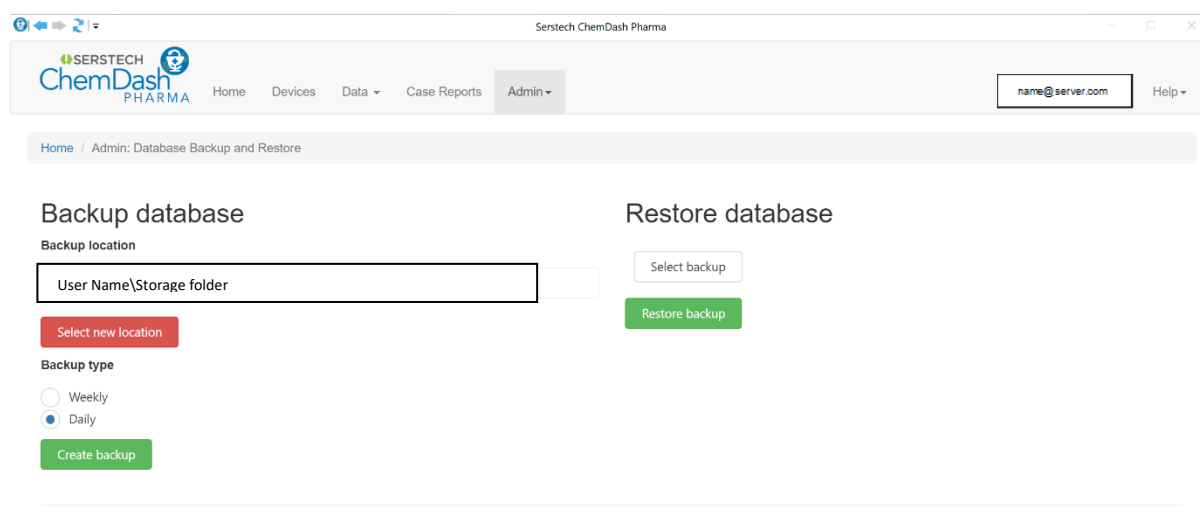


Image 5:Database backup and restore

The Table 2 below presents the key features of both the ChemDash Pharma and the Serstech Indicator 100's compliance with 21 CFR part 11. On the Appendix 2 (pages 17-29), it can be found the analytical compliance with 21 CFR Part 11 for both the Serstech 100 Indicator and the computer software ChemDash Pharma.

Table 2:Key features of 21CFR Part 11 compliance

21 CFR part 11 requirement	Compliance	Comment
System should be able to generate complete copies of electronics records in human readable and electronic form for audit trail	YES	All electronic records including audit trail can readily be produced in both electronic and human readable form.
Users not able to modify records. Access to records only through the application.	YES	Measurements cannot be edited once created; information can only be added in free text fields. Incorporating measurements in libraries

Record modifications reserved for admins		allow editing of sample information Access control to edit functionality is accomplished through a combination of integration with windows user rights system – Chemdash users and admins are selected from windows users and data directories are protected by windows file rights and encryption.
System should be able to generate a list of authorized admins and users with their individual rights	YES	Utilizing windows user rights – ChemDash Pharma is able to read out the Windows User list and establish who of these that are Chemdash users and their right levels – These data can be exported & viewed.
System should be able to create a backup for electronic records. Backup functionality should be integrated into the system	YES	A ChemDash Pharma administrator can configure automatic backups of the database. Both full backups and incremental backups are available. Windows Task Scheduler runs the database backup as a service in the background.
System should be able to import backups from earlier software versions. Backup and restore actions should be documented in the system audit trail	YES	This functionality is tested as working processes are clearly defined to prevent incompatible future implementations causing issues to the system. All backup/restore functions are included in the audit-trail log.
All electronic records are stored in the database in one location. The user can only access the database through application	YES	As mentioned earlier, it is solved through a combination of Windows User Rights Directory and encryption.
Data is to be recreated after a computer system failure prevention of data corruption needs to be in place	YES	All saved (electronically signed) data is retained into the database backup files and can be restored into the system.
The system should have different user- access control levels	YES	The system is automatically importing Windows Users on the PC.According to their Windows Active Directory Rights, these Users are mapped to an internal database (ChemDash Pharma) user hierarchy.
The system should be able to create a list of current and previous operators showing their credentials in pdf form	YES	Implemented

5. Third part 21 CFR Part 11 Compliance Checklist (Qualio.com)

An external source for the 21 CFR Part 11 compliance was used as an extra step to assure Serstech products compliance. The 21 CFR Part 11 compliance checklist was used from Qualio.com, can be found on the Appendix 1 (pages 13-15). This list is also used to improve our whole system's processes. Qualio's checklist is divided into four parts: Part 1: Validation, Part 2: Audit Trail, Part 3: Copies of Records, and, Part 4: Record Retention.

Appendix 1

3rd Part validation-QUALIO.COM

Part 1:Validation

- I. Is the system validated? YES: Serstech has validated the whole system, however, the procedure which the instrument is used has to be validated by the end user.
- II. Is it possible to discern invalid or altered records? NO
- III. Are the records readily retrievable throughout their retention period? YES
- IV. Is system access limited to authorized individuals? YES
- V. If the sequence of system steps or events is important, is this enforced by the system (process control system)? YES
- VI. Does the system ensure that only authorized individuals can use it, electronically sign records, alter a record, or perform other operations? YES
- VII. If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals) does the system check the validity of the source of any data instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weight scales, or remote, radio controlled terminals). YES
- VIII. Is there documented training, including on the job training for system users, developers, IT support staff? YES: Employees at Serstech get a proper training during their introduction period about the whole system plus company policies. Regarding our partners we supply training material and physical or online training to them. We believe that our partners provide sufficient training to the end customer.
- IX. Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures? YES
- X. Is the distribution of, access to, and use of systems operation and maintenance documentation controlled? YES
- XI. Is data encrypted? YES: Both device and PC application require user credentials to login. The data when transferred from the device to the PC application and vice versa are in a format that cannot be accessed by any unauthorised users.
- XII. Are digital signatures used? E-signatures are used for the log-in action.

Part 2. An Audit Trail For Every Document

- I. Is there a secure, computer-generated, time-stamped audit trail that records the date and time of operator entries and actions that create, modify, or delete electronic records? YES
- II. Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)? YES: For example, for basic electronic records such as measurements, the core information cannot be altered, only text information can be added. Measurements can be used to build user defined libraries where information can be edited. However, core information e.g. spectral information

date & time stamp, serial no. of instrument cannot be altered for traceability issues. In addition, the library function is limited to authorized users.

- III. Is an electronic records audit trail retrievable throughout the record's retention period? YES
- IV. Is the audit trail available for review and copying by the FDA? YES
- V. Does the audit trail include the User ID, sequence of events (in particular scenarios or instances), original and new values (Backups of any modified or deleted records), a change log, and revision and change controls? YES
- VI. Do signed electronic records contain: The printed name of the signer YES
- VII. The date and time of signing YES
- VIII. The meaning of the signing (such as approval, review, etc.) YES: approval signing required.
- IX. Is the above information shown on displayed and printed copies of the electronic record? YES: For example, basic data such as analyst ID, serial number of the device and a date & time stamp always follow the data and can be displayed. However, some information has to be extracted from the Audit trail log.
- X. Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification? YES: only electronic signatures for login.
- XI. Is there a formal change control procedure for system documentation that maintains a time-sequenced audit trail for those changes made by the pharmaceutical organization? The Audit trail of instrument and ChemDash gives tools to end user to comply with this. However, it is ultimately the end user responsibility to comply with this.
- XII. Are electronic signatures unique to an individual? Since the log in is based on the Active Directory system, this is an end user's responsibility.
- XIII. Are electronic signatures ever reused by or reassigned to anyone else? Since the log in is based on the Windows Active Directory system, this is an end user's responsibility.
- XIV. Is the identity of an individual verified before an electronic signature is allocated? Since the log in is based on the Windows Active Directory system, this is an end user's responsibility.
- XV. Is the signature made up of at least two components, such as an identification code and password, or an id card and password? YES
- XVI. Has it been shown that biometric electronic signatures can be used only by their genuine owner? No-Does not apply in our case.
- XVII. When several signings are made during a continuous session, is the password executed at each signing? (Note: Both components must be executed at the first signing of a session.): Not applicable (electronic signatures only for login)
- XVIII. If signings are not done in a continuous session, are both components of the electronic signature executed with each signing? Not applicable see XVII
- XIX. Are non-biometric signatures only used by their genuine owners? Since the log in is based on the Windows Active Directory system, this is an end user's responsibility.
- XX. Would an attempt to falsify an electronic signature require the collaboration of at least two individuals? YES

Part 3. Copies of Records

- I. Is the system capable of producing accurate and complete copies of electronic records on paper? YES
- II. Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA? YES
- III. Is the system using established automated conversion or export methods (PDF, XML, or SGML)? YES in PDF

Part 4. Record Retention

- I. Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password? YES: Since the user ID is based on the Windows Active Directory system, this is an end user's responsibility that user names are not reused.
- II. Are procedures in place to ensure that the validity of identification codes is periodically checked? YES :User ID is based upon windows active directory and thus it is an end-user responsibility that identification codes are periodically checked.
- III. Do passwords periodically expire and need to be revised? YES: User ID is based upon windows active directory and thus it is an end-user responsibility that identification codes periodically expire.
- IV. Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred? YES: Super Administrator can inactivate a user and thus deny access to the system. Recalling passwords is an end-user responsibility since the windows active directory is used for identifying users.
- V. Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost? YES
- VI. Is there a procedure for detecting attempts at unauthorized use and for informing security? YES
- VII. Is there a procedure for reporting repeated or serious attempts at unauthorized use to management? YES
- VIII. Is there a loss management procedure to be followed if a device is lost or stolen? YES
- IX. Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised? YES
- X. Are there controls over the issuance of temporary and permanent replacements? YES
- XI. Is there initial and periodic testing of tokens and cards? YES
- XII. Does this testing check that there have been no unauthorized alterations? YES

Appendix 2

Electronic Code of Federal Regulations		
e-CFR data is current as of October 24, 2019		
21 CFR Part 11 requirements	YES/NOT APPLICABLE	COMMENTS
Subpart A—General Provisions		
Sec.11.1 Scope.		
(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.		The 21 CFR Part 11 scope applies to the <i>ChemDash Pharma</i> software
(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.		
(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.		

<p>(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with §11.2, unless paper records are specifically required.</p>	
<p>(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.</p>	
<p>(f) This part does not apply to records required to be established or maintained by §§1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(g) This part does not apply to electronic signatures obtained under §101.11(d) of this chapter.</p>	
<p>(h) This part does not apply to electronic signatures obtained under §101.8(d) of this chapter.</p>	
<p>(i) This part does not apply to records required to be established or maintained by part 117 of this chapter. Records that satisfy the requirements of part 117 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(j) This part does not apply to records required to be established or maintained by part 507 of this chapter. Records that satisfy the requirements of part 507 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	

<p>(k) This part does not apply to records required to be established or maintained by part 112 of this chapter. Records that satisfy the requirements of part 112 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(l) This part does not apply to records required to be established or maintained by subpart L of part 1 of this chapter. Records that satisfy the requirements of subpart L of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(m) This part does not apply to records required to be established or maintained by subpart M of part 1 of this chapter. Records that satisfy the requirements of subpart M of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(n) This part does not apply to records required to be established or maintained by subpart O of part 1 of this chapter. Records that satisfy the requirements of subpart O of part 1 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	
<p>(o) This part does not apply to records required to be established or maintained by part 121 of this chapter. Records that satisfy the requirements of part 121 of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.</p>	

Sec.11.2 Implementation.	
(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.	<p>The ChemDash Pharma software provides electronic records, for example: processed data,audit trail,configuration settings etc. Audit trail report in PDF format, Data export in JCAMP, CSV and Text format, etc. The ChemDash Pharma software also provides paper records like:Audit trail reports, configuration reports. The final & complete implementation of 21 CFR Part 11 processes is the partner’s/customer’s responsibility.</p>
(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:	
(1) The requirements of this part are met; and	
(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.	
Sec.11.3 Definitions.	
(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.	<p>The ChemDash Pharma software is a closed system and uses username and password credentials to authenticate each user.</p>
(b) The following definitions of terms also apply to this part:	

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).
(2) Agency means the Food and Drug Administration.
(3) Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.
(4) 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.
(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.
(6) Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.
(7) Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

<p>(8) Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.</p>	
<p>(9) 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.</p>	
<p>Subpart B--Electronic Records</p>	
<p>Sec. 11.10 Controls for closed systems.</p>	
<p>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:</p>	

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	YES	Through audit trails for user and quality relevant data changes to your data are always tracked.
(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.	YES	All quality relevant data is available both electronically and in human readable format by FDA or any other inspection body.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	YES	All electronic records, including audit trails, are backed up and are retrievable during the retention period.
(d) Limiting system access to authorized individuals.	YES	The access to data is limited for unauthorized users and is given only to authorized persons with individual usernames and passwords.
(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.	YES	All quality relevant data have an audit trail. The audit trails track changes user specific and timestamped. The audit trails cannot be modified and are available in both electronic and human readable form PDF.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.		All operations/actions that are performed in a specific sequence the system enforces this sequence and therefore prevents accidental changes to data.
(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.	YES	Regarding the authority checks, ChemDash Pharma has an elaborate role-based authority concept which meets the requirements of the 21 CFR Part 11.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.		The ChemDash Pharma system has validated input and output interfaces. The data that can the system accept come from the Serstech 100 Pharma Indicator and can be uploaded to ChemDash Pharma and later exported as JCAMP, CSV or Text files.
(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.	YES	Serstech employees that worked for the 21 CFR Part 11 implementation have adequate training about the requirements. Furthermore, special training and documentation are given to Serstech partners.
(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 is an end-user responsibility
(k) Use of appropriate controls over systems documentation including:	YES	This is ultimately an end-user responsibility. However, user hierarchy together, audit trail logs, user manuals and give tools to assist end user in complying with this.
(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.		
(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.		

Sec. 11.30 Controls 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.		NOT APPLICABLE
Sec. 11.50 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;	YES	
(2) The date and time when the signature was executed; and	YES	
(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	YES	
(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).	YES	
Sec. 11.70 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.	YES	Not handwritten signatures as are not applicable for our system

Subpart C--Electronic Signatures		
Sec. 11.100 General requirements.		
(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	YES	
(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.		
(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.	YES	
Sec. 11.200 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.	YES	
(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.	YES	
(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.	YES	
(2) Be used only by their genuine owners; and	YES	
(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.	YES	
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	NOT APPLICABLE	

Sec. 11.300 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.	YES	The system ensures that the login credentials are always unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	YES	The system enforces passwords to be changed after a certain period. Furthermore, in order to lock/unlock users one needs to be authorized.
(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.	YES	Users are locked out of the system if their passwords were entered wrongly 3 times in a row. Unlocking users is only possible through authorized users. Furthermore, each locking and unlocking event is tracked in an audit trail.
(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.	YES	
(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.	YES	

Self-assessment of Serstech 100 Indicator & Serstech ChemDash Pharma regarding compliance with FDA 21CFR Part 11 e-records;e-signatures

Document ID

Revision date

General status

Statement compliance v1.1

June 2020

Approved

Serstech AB
info@serstech.com
Phone: +46 46 255 112
Åldermansgatan 13
SE-227 64 Lund
Sweden