

System Assessment Report
Relating to Electronic Records and Electronic Signatures;
Final Rule, 21 CFR Part 11

System: StabNet
(Software Version 1.0)

1 Procedures and Controls for Closed Systems

Runn o.	Ref.	Topic	Question	Yes	No	Comments
1.1	11.10 (a)	Validation, IQ, OQ	Is the system validated?	☒	☐	The operator is solely responsible for the validation of the system. The responsibility of the supplier lies in supplying systems which are capable of being validated. This is supported by the internal Metrohm quality control system which can be audited at any time. In this respect Metrohm offers a range of validation services: conformity certificates, prepared documentation for IQ and OQ, carrying out IQ and OQ at the operator's premises, ...

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.2	11.10 (a)	Audit Trail, Change	Is it possible to discern invalid or altered records?	X		All relevant operator entries are recorded in an automatically generated audit trail with date, time with difference to UTC Coordinated Universal Time) and user. This time is taken from the client's system time, which means that the administrator has to take care of the system time to be correct; for reproducibility all clients connected should be synchronized. In the report generator, the report can be defined in order to indicate any modified results data (results). Sample data modifications are recorded with the audit trail of the respective results. For method modifications all former versions are saved in the database and a comment has to be entered. Methods are subject to a version control. This means that modified data of a method leads to a new entry (version) in the database. If the results data are changed (recalculation), all former versions are saved in the database and a comment has to be entered. A version check is implemented for determinations. This means that modified data leads to a new entry in the database. Incomplete records of methods are identified by the fact that they cannot be saved. Invalid methods can be loaded but the associated analysis cannot be started. Invalid results can be recognized if limit values have been defined. In case of exceeding this limits it can be defined in the system whether a message is displayed on the screen or on the report or whether an E-mail is sent.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.3	11.10 (b)	Report, Printout, Electronic Record	Is the system able to produce accurate and complete copies of electronic records on paper?	X		Method parameters can be printed out as part of a configurable report. Configurable reports can be printed out for determinations (results data). Modifying the report configuration can be disabled for routine users. The automatic printout at the end of an analysis can be defined in the method. This way it can be ensured, that system operator can reliably follow any modifying, overwriting or deleting of the data of a determination. Each printout is accompanied by a time stamp giving information about the difference to UTC. To print out an old version of a method or determination, the respective record has to be changed to be current version.
1.4	11.10 (b)	Report, Electronic Record, FDA	Is the system able to produce accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?	X		All data can be stored as encrypted XML file (RDET format) and processed with StabNet. Data can be exported to XML, CSV, TXT and RDET format. Via the report generator all reports can be provided in PDF format. The automatic data export at the end of an analysis can be defined in the method. This way it can be ensured, that the system operator can reliably follow any modifying, overwriting or deleting of the data of a determination.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.5	11.10 (c)	Electronic Record, Retention Period, Archiving	Are the records readily retrievable throughout their retention period?	O		The operator is solely responsible for storage/archiving. <i>StabNet</i> can be installed as local server or client version. The system can store the data permanently either in the <i>StabNet</i> database or on the computer or on a network drive by using an archiving system or on paper. The database has an automatic backup function. The data on the storage device is encrypted and provided with a checksum. This way it is protected against accidental and improper modification. Modifications are recognized by the system. The content can be read by the <i>StabNet</i> software at any time. The method used for archiving data and which data are to be archived must be defined by the operator. Interfaces for archiving (XML files) are available in the system.
1.6	11.10 (d)	Login, Access Protection, Authorization User, Administrator	Is the system access limited to authorized individuals?	X		The system is provided with a login system with an unlimited number of editable profiles (access rights / user groups). The access rights for the single user groups can be arbitrarily defined by the administrator. The persons responsible for the system (administrators) must ensure that access rights are assigned to authorized persons only. All changes of access rights are recorded in the audit trail.
1.7	11.10 (e)	Audit Trail, Electronic Record, Operator Entries	Is there a secure, computer generated, time stamped audit trail, that logs the date and time of those user entries and actions which create, modify or delete electronic records?	X		The audit trail documents all user entries and actions on electronic records with date, time with difference to UTC and user. Additionally, all modifications of security settings, user administration or configuration data are recorded in the audit trail.
1.8	11.10 (e)	Electronic Record, Overwriting data, Change	If modifying electronic records, is previously recorded information still available in the system (i.e. is it not overwritten by the modification)?	X		A new version is automatically created, if methods or determination data are changed and saved.

Ru nn o.	Ref.	Topic	Question	Yes	No	Comments
1.9	11.10 (e)	Audit Trail, Retention Period	Is the audit trail of an electronic recording retrievable throughout the retention period of the record?	X		As long as the audit trail has not been deleted it is kept. The disk space is the limiting factor here. The audit trail can only be deleted after it has been archived before. The audit trail is being archived as a text file with a checksum. If configured, the system requires a double check before the audit trail can be deleted; this double check is available to specific user rights only. The operator is solely responsible for the safe storage of the archived audit trail.
1.10	11.10 (e)	Audit Trail, FDA, Inspection	Is the audit trail available for review and copying by the FDA?	X		The audit trail can be exported to a text file and is therefore available in electronic form. By means of the checksum, the data integrity of the audit trail can be verified. Additionally, a write protected PDF file of the audit trail can be created.
1.11	11.10 (f)	Sequence of steps, Sequence, Plausibility Check, Devices	If the sequence of system steps or events is important, is it enforced by the system (e.g. as it would be the case in a process control system)?	X		In the system, plausibility checks are already carried out when a determination is started, for example, a check is made whether a database is assigned to the selected method, or whether the device is present. The parameters of the determination are programmed in the method and must be strictly maintained.
1.12	11.10 (g)	Login, Access Protection, Authorization, User, Administrator	Does the system ensure that only authorized persons can use the system, electronically sign records, access the functions, the computer system input or output device, can modify a record or perform other operations?	X		The user can be identified by the login function. (The person responsible for the system (= administrator) must ensure that access rights are assigned to authorized persons only). The administrator function can be clearly separated from user roles, see also 11.10 (d), No. 1.6. Methods and determinations can be signed and therefore be released electronically. There are two signature levels. The system demands that the reviewing and the releasing person is not the same. Additionally the rights assigned to a group can be restricted, so that their members are able to use signed methods only.

Ru nn o.	Ref.	Topic	Question	Yes	No	Comments
1.13	11.10 (h)	Balance, Connection, Terminals, Input data, Devices	Does the system control the validity of connected devices? <i>If it is a system requirement that input data or instructions can only be received by certain input devices (e.g., terminals) does the system check the validity of the source of any data or instructions received?</i> <i>(Note: This applies where data or instructions can be received from more than one device, and therefore the system must verify the integrity of the source, such as a network of balances or remote controlled terminals).</i>	X		During the IQ all the devices connected are entered into the list of devices and are subsequently checked. Metrohm devices are recognized, their validity is being checked and they are automatically entered into the list of devices. Validation of the devices connected is carried out as part of the system validation (see also 11.10 (a), No. 1.1) by the operator.
1.14	11.10 (i)	Training, Support, User, Administrator	Is there documented training, including training on the job, for system users, developers, IT support staff?	X/O		The operator is responsible for training the users and administrators. Metrohm offers standard training courses for all application fields. Individual training courses can be arranged separately. Metrohm product developers and service personnel are trained on a regular basis.
1.15	11.10 (j)	Policy, Responsibility, Electronic Signature	Is there a written policy that makes individuals fully accountable and responsible for actions initiated by their electronic signatures?	O		If electronic signatures are used the operator must have a policy which defines the equality of handwritten and electronic signatures.
1.16	11.10 (k)	Documentation, Distribution of Documentation, Access to Documentation, System Documentation, Logbook, Manuals	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	O		The system has a comprehensive manual supporting the user and the service personnel. Additionally the content of the manual is available as Online Help. The operator is responsible for distributing paper-based documentation.

Run no.	Ref.	Topic	Question	Yes	No	Comments
1.17	11.10 (k)	SOP, Documentation, Manuals, System Documentation, Audit Trail , Logbook	Is there a formal change control procedure for system documentation maintaining an audit trail which records modifications with a time sequence?	X/O		The system documentation is unambiguously assigned to a system and a software version. Release notes are kept with each software version – except for the initial version 1.0. However, the operator must maintain a device logbook and note any changes in the documentation and the software. Templates of these documents are supplied by Metrohm.

2 Additional Procedures and Controls for Open Systems

Run no.	Ref.	Topic	Question	Yes	No	Comments
2.1	11.30	Data, Encryption, Data Transfer	Can methods and determinations be securely transferred from one system to another? Is the data encrypted on its way from the sender to the receiver?	N/A		StabNet is not designed to be accessed via the Internet. The data are stored as a file, encrypted and provided with a check-sum. This protects the data against unauthorized modification. In case of a modification the data become useless. Even if corrupted data are transferred to another system this is recognized.
2.2	11.30	Electronic Signature	Are electronic signatures used?	N/A		StabNet is not designed to be accessed via the Internet. Methods and determinations can be signed and therefore be released electronically. There are two signature levels. The system demands that the reviewing and the releasing person is not the same.

3 Signed Electronic Records

Run no.	Ref.	Topic	Question	Yes	No	Comments
3.1	11.50	Electronic Signature	Do the signed electronic records contain the following related information? - Full name of signer - Date and time of the signature - Meaning of the signature (as approval, review, responsibility)	X		In case of methods and determinations all signatures contain the full name of the signer, date and time of the signature and the meaning (out of a list box) for signing. Additionally, a comment on a signature can be entered, which is saved together with the electronic signature.
3.2	11.50	Electronic Signature	Is the information mentioned above shown on displayed and printed copies of the electronic record?	X		Full signature data can be shown on the display and on printouts.
3.3	11.70	Electronic Signature	Are signatures linked to their respective electronic records in order to ensure not being cut, copied or otherwise transferred by ordinary means for the purpose of forgery?	X		The signature is securely linked to the method or determination. Signature elements cannot be cut, copied or transferred by ordinary means.

4 Electronic Signature (General)

Run no.	Ref.	Topic	Question	Yes	No	Comments
4.1	11.100 (a)	Electronic Signature	Are electronic signatures unambiguously assigned to a person?	X		Each user gets a unique login name, which is displayed together with the signature data. The system ensures that this login name is unique system-wide. Once a login name is created it cannot be deleted any more – it can only be deactivated. It must be ensured by organizational means, that login names are used only once.
4.2	11.100 (a)	Electronic Signature	Are electronic signatures ever reused by, or reassigned to, anyone else?	O		A login name used is assigned to one person. It must operationally be ensured, that this login name is not assigned to another person. A reactivation is not affected by this.
4.3	11.100 (a)	Electronic Signature	Does the system allow transferring the authorization of electronic signatures (representatives)?	O		The secure and traceable user rights management is in the responsibility of the user. The assignment of representatives is part of the regular user management and has to be carried out by the administrator. A procedure has to be in place for this.
4.4	11.100 (b)	Electronic Signature	Is the identity of a person verified before an electronic signature is allocated?	O		With the initial signing rights assignment to a user, the identity of the respective person has to be verified against the user rights request..

5 Electronic Signatures (Non-biometric)

Run no.	Ref.	Topic	Question	Yes	No	Comments
5.1	11.200 (a) (1)(i)	Electronic Signature	Does the signature consist of at least two components, such as an identification code (e.g. user name) and a password, or an identification card and a password?	X		The signing functions is carried out with login name and password.
5.2	11.200 (a) (1)(ii)	Electronic Signature	When several signings are made during a continuous session, is the password requested for each signing? (Note: Both elements must be named when firstly signing a session).	X		The password has to be entered with each signature.
5.3	11.200 (a) (1)(iii)	Electronic Signature	If signings are not made during a continuous session, would still both elements of the electronic signature be requested?	X		The login name and the password have to be entered with each signature.
5.4	11.200 (a) (2)	Electronic Signature	Are non-biometric signatures used by their genuine owners only?	O		The operator has to ensure that a user only uses his/her own signature
5.5	11.200 (a) (3)	Electronic Signature, Falsify Electronic Signature	Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	X/O		The administrator defines an initial password that has to be changed with the first login. The operator is responsible to control that a login name is handed over to the designated user only. The data of the database are encoded in a format non-readable for humans.

6 Electronic Signatures (biometric)

Runn o.	Ref.		Question	Yes	No	Comments
6.1	11.200 (b)	Electronic Signature, Biometric Electronic Signature	Has it been proved that biometric electronic signatures can be used by their genuine owner only?	N/A		There is no use of biometric signatures with the system.

7 Control of Identification Code and Password

Runn o.	Ref.	Topic	Question	Yes	No	Comments
7.1	11.300 (a)	Identification Code, Uniqueness, Password, Identification, Login, Access Protection	Are there controls in order to maintain the uniqueness of each combination of identification code and password, such as no person can have the same combination of identification code and password?	X		The system ensures that every identification code (user name) is used only once within the system and therefore each combination of identification code and password can also only exist once. Modification of names has to be organizationally administered by the operator. The system can be run as client server system. This ensures that all identification codes are identical on all clients. It is recommended to use unambiguous identification codes (e.g. personnel number or initials) covering the entire organization. Generally it is recommended setting guidelines for the whole organization in which creating of user accounts and using passwords (length, period of validity, ...) are defined.
7.2	11.300 (b)	Identification Code, Password, Validity, Identification, Login, Access Protection	Are there procedures ensuring that the validity of identification codes are periodically checked?	O		The operator is responsible for checking the identification codes periodically.

Run no.	Ref.	Topic	Question	Yes	No	Comments
7.3	11.300 (b)	Password, Validity, Password Expiry, Identification, Login, Access Protection	Do passwords periodically expire and need to be revised?	X		The validity period of the password can be defined by the administrator. Values between 30 and 90 days are common. After this period is expired, the user is forced to change his/her password. A long validity period represents a security risk. A validity period which is too short means that the users have to remember a new password frequently and may write it down. The system saves the password history and therefore reusing passwords is impossible.
7.4	11.300 (b)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection	Is there a procedure for recalling or disabling identification codes and passwords if a person leaves or changes its workplace?	O		The procedure has to be set up by the operator. The corresponding user can be removed from the system by the administrator, but remains saved in the system as part of the group "removed users" without any access rights.
7.5	11.300 (c)	Identification Code, Password, Validity, Disable User Access, Identification, Login, Access Protection, Loss of ID card	Is there a procedure for electronically disabling an identification code or password if it is potentially insecure or has been lost?	O		The procedure has to be set up by the operator. The corresponding user can be removed from the system by the administrator, but remains saved in the system as part of the group "removed users" without any access rights.
7.6	11.300 (d)	Unauthorized Use, Login, Access Protection	Is there a procedure for recognizing attempts of misuse and for notifying the security authority?	X/O		After <i>n</i> incorrect attempts (number can be defined by the administrator) a message is displayed, saying that the maximum number of unsuccessful login attempts has been reached and the user is disabled. A corresponding message can be sent to the management by E-mail. All attempts to log-in to the system are recorded in the audit trail. The procedure to inform the security authority has to be implemented by the operator.
7.7	11.300 (d)	Unauthorized Use, Login, Access Protection	Is there a procedure for reporting repeated or serious attempts of misuse to the management?	O		A method for reporting to the management must be defined by the operator. After <i>n</i> incorrect attempts a message is displayed, saying that the maximum number of login attempts has been reached and the user is disabled. A corresponding message can be sent to the management by E-mail.

Ru nn o.	Ref.	Topic	Question	Yes	No	Comments
7.8	11.300 (c)	Loss of ID card, ID card, Unauthorized Use, Access Protection	Is there a loss management procedure if identification hardware (e.g. ID card) is lost or stolen?	N/A		There is no hardware device for user identification.
7.9	11.300 (c)	Loss of ID card, Electronically Disabling ID card, ID card, Unauthorized Use, Access Protection	Is there a procedure for electronically disabling such hardware if it is lost, stolen or potentially insecure?	N/A		There is no hardware device for user identification.
7.10	11.300 (c)	ID card, Access Protection	Are there controls for the issuing of temporary and permanent replacements of this hardware?	N/A		There is no hardware device for user identification.
7.11	11.300 (e)	Testing of ID cards, ID card, Access Protection	Is there initial and periodic checking of identification tokens and cards?	N/A		There is no hardware device for user identification.
7.12	11.300 (e)	Modification of ID cards, ID card, Unauthorized Use, Access Protection	Does this checking also control that there have been no unauthorized modifications?	N/A		There is no hardware device for user identification.

O = The operator is responsible.

N/A = Not applicable to the system

8 Indices

References to the page number:

A

Access Protection.....	5, 6, 12, 13, 14
Access to Documentation.....	7
Administrator	5, 6, 7
Archiving	5
Audit Trail	3, 5, 6, 8
Authorization	5, 6

B

Balance	7
Biometric Electronic Signature	12

C

Change.....	3, 5
Connection	7

D

Data.....	9
Data Transfer	9
Devices	6, 7
Disable User Access	13
Distribution of Documentation	7
Documentation	7, 8

E

Electronic Record	4, 5
Electronic Signature	7, 9, 10, 11, 12
Electronically Disabling ID card	14
Encryption	9

F

Falsify Electronic Signature	11
FDA	4, 6

I

ID card	14
Identification.....	12, 13
Identification Code	12, 13
Input data.....	7
Inspection	6
IQ	2

L

Logbook	7, 8
Login	5, 6, 12, 13
Loss of ID card	13, 14

M

Manuals	7, 8
Modification of ID cards	14

O

Operator Entries.....	5
OQ	2
Overwriting data.....	5

P

Password	12, 13
Password Expiry	13

Plausibility check	6
Policy	7
Printout	4

R

Report.....	4
Responsibility	7
Retention Period.....	5, 6

S

Sequence	6
Sequence of steps.....	6
SOP	8
Support.....	7
System Documentation.....	7, 8

T

Terminals.....	7
Testing of ID cards	14
Training.....	7

U

Unauthorized Use	13, 14
Uniqueness.....	12
User	5, 6, 7

V

Validation.....	2
Validity	12, 13

References to the run number of the entry:

A

Access Protection.... 7.12, 7.11, 7.10, 7.9, 7.8, 7.7, 7.6,
7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6
Access to Documentation..... 1.16
Administrator 1.14, 1.12, 1.6
Archiving 1.5
Audit Trail 1.17, 1.10, 1.9, 1.7, 1.2
Authorization 1.12, 1.6

B

Balance 1.13
Biometric Electronic Signature 6.1

C

Change..... 1.8, 1.2
Connection 1.13

D

Data..... 2.1
Data Transfer 2.1
Devices 1.13, 1.11
Disable User Access 7.5, 7.4
Distribution of Documentation 1.16
Documentation 1.17, 1.16

E

Electronic Record 1.8, 1.7, 1.5, 1.4, 1.3
Electronic Signature..... 6.1, 5.5, 5.4, 5.3, 5.2, 5.1, 4.4, 4.3,
4.2, 4.1, 3.3, 3.2, 3.1, 2.2, 1.15
Electronically Disabling ID card..... 7.9

Encryption 2.1

F

Falsify Electronic Signature 5.5
FDA..... 1.10, 1.4

I

ID card 7.12, 7.11, 7.10, 7.9, 7.8
Identification..... 7.5, 7.4, 7.3, 7.2, 7.1
Identification Code 7.5, 7.4, 7.2, 7.1
Input data..... 1.13
Inspection 1.10
IQ 1.1

L

Logbook 1.17, 1.16
Login 7.7, 7.6, 7.5, 7.4, 7.3, 7.2, 7.1, 1.12, 1.6
Loss of ID card 7.9, 7.8, 7.5

M

Manuals 1.17, 1.16
Modification of ID cards 7.12

O

Operator Entries..... 1.7
OQ 1.1
Overwriting data..... 1.8

P

Password 7.5, 7.4, 7.3, 7.2, 7.1
Password Expiry 7.3

Plausibility Check 1.11
Policy 1.15
Printout 1.3

R

Report..... 1.4, 1.3
Responsibility 1.15
Retention Period..... 1.9, 1.5

S

Sequence 1.11
Sequence of steps..... 1.11
SOP 1.17
Support..... 1.14
System Documentation..... 1.17, 1.16

T

Terminals..... 1.13
Testing of ID cards 7.11
Training..... 1.14

U

Unauthorized Use 7.12, 7.9, 7.8, 7.7, 7.6
Uniqueness..... 7.1
User..... 1.14, 1.12, 1.6

V

Validation..... 1.1
Validity 7.5, 7.4, 7.3, 7.2