

EmpowerTM 2 Software

21 CFR PART 11 COMPLIANCE ASSESSMENT

Note: Information presented in this document assumes that the appropriate Empower 2 System Policies have been configured for Electronic Record (ER) and Electronic Signature (ES) support.

Overview	Yes/No/NA
Is the system a Closed System, where system access is controlled by the persons who are responsible for the content of the electronic records that are on the system?	Yes
Is the system an Open System, where system access is <u>not</u> controlled by the persons who are responsible for the content of the electronic records that are on the system? (e.g. A service provider controls and maintains access of the contents of the system, etc.).	No
Does the system use an ID/ password combination?	Yes
Does the system use tokens?	No
Does the system use biometrics?	No

Ref.		Yes/No/NA	Explanation
<p>Subpart B – Electronic Records 11.10 Controls for Closed Systems</p>			
1.	11.10 (a)	Is the system validated?	<p>Yes</p> <p>Waters Corporation has structurally validated Empower 2 software and supplies a certificate of structural validation with the Empower 2 software.</p>
2.	11.10 (a)	Does the validation documentation show that Part 11 requirements have been met and are functioning correctly?	<p>Yes</p> <p>Empower 2 software allows users to be compliant with 21 CFR Part 11, but complete compliance can only occur within a validated electronic records environment. Validation documentation is available for examination during an audit of the Waters quality system for data products development.</p>
3.	11.10 (a)	Is the system able to detect invalid records where applicable (e.g. invalid field entries, fields left blank that should contain data, values outside of limits)?	<p>Yes</p>
4.	11.10 (b)	Is it possible to view the entire contents of the records?	<p>Yes</p>
5.	11.10 (b)	Is it possible to print the entire contents of the records?	<p>Yes</p>
6.	11.10 (b)	Is it possible to generate all the records electronically in a format that can be put on a portable medium (e.g. diskette or CD) or transferred electronically?	<p>Yes</p>

Ref.			Yes/No/NA	Explanation
7.	11.10 (c)	Are records protected against intentional or accidental modification or deletion?	Yes	The abilities to modify or delete data within the Empower 2 software application are specifically assigned privileges. All actions involving a creation, deletion or modification of data is audit trailed and requires user confirmation before changes are committed to the database.
8.	11.10 (c)	Is data archived off the system? If so, is the meta data (including the audit trail) archived as well? Can all the archived data be accurately retrieved after system upgrades?	Yes	Meta data can be archived off the system and includes all information that is part of the electronic record, including audit trails. Archived data can be retrieved after system upgrades and procedures for this are defined in the documentation for each software release.
9.	11.10 (d)	Are there different levels of access based on user responsibilities (e.g. user, administrator) (if appropriate)? Is this documented and controlled?	Yes	User access is based on the concept of "User Types". A user type defines a specific level of access based on allowed activities/responsibilities. Changes to user types are documented in the system audit trail. The ability to create, modify or delete user types are discrete privileges that may be assigned to specific individuals.
10.	11.10 (d)	Are user access levels approved by management or the system owner before assignment to a user?	Yes	User access levels are set and approved during the process of creating a user. Only an individual who has explicitly been given the privilege to create or alter a user account can change the access level for a particular user.
11.	11.10 (d)	Is there is a controlled, documented process for granting access to a new user, for changing privileges for an existing user and for deleting user accounts?	Yes	User creation, modification and deletion are controlled through a software wizard, and is only accessible to appropriately privileged users. In addition, Empower 2 System Policies can be used to predefine specific aspects of the user creation process to ensure compliance with Part 11.

Ref.			Yes/No/NA	Explanation
12.	11.10 (d)	Is there physical security and procedures to protect the server, database and system components from unauthorized access?	NA	Each organization must develop a controlled, documented procedure for managing system security and protection.
13.	11.10 (e)	Is an electronic audit trail function automatically generated for all operator entries?	Yes	A designated system administrator may configure audit trail settings on a per project basis. All activities for all users in projects with full audit trail turned on will be audit trailed, with no user types or activities treated differently.
14.	11.10 (e)	Is the audit trail completely outside the control and access of users (except for read-only access of the audit trail file)?	Yes	A designated system administrator may configure audit trail settings, no other users will have control over audit trails.
15.	11.10 (e)	Is it impossible to disable the audit trail function?	Yes	The system audit trail cannot be disabled. Empower 2 data is stored in Projects and it is impossible to disable or modify audit trail settings for a project after its creation. A designated system administrator may configure audit trail settings.
16.	11.10 (e)	Is the system date and time protected from unauthorized change?	NA	The system date and time are taken from the server. The ability to change the system date and time is a privilege that is controlled through the computer operating system and not through the Empower 2 software.
17.	11.10 (e)	When data is changed or deleted, are all previous values still electronically available?	Yes	All previous values are stored in the embedded database. When data is changed, new values are added to the database, and previous information is not overwritten or obscured. The privileges to change or delete data may be assigned only to specific users.

Ref.			Yes/No/NA	Explanation
18.	11.10 (e)	Is the audit trail data protected from accidental or intentional modification or deletion (read-only access)?	Yes	Project audit trails cannot be modified or deleted. The system audit trail can be archived and removed – and requires the active collaboration of 2 system administrators to sign off on this archival and removal before the process can begin. A binary archived system audit trail can be retrieved into the Empower 2 “Offline System Audit Trail” view for review and analysis.
19.	11.10 (e)	Are the electronic audit trails maintained and retrievable for at least as long as its respective electronic records?	Yes	Audit trail are maintained either as part of project archives and database backups. In addition, the system audit trail may be specifically archived in either ASCII or binary format. Binary archives may be restored into the software at a later date for review.
20.	11.10 (e)	Are the electronic audit trails readily available for inspections and audits?	Yes	Audit trails are available both online in Empower 2 and can be archived for storage or offsite inspection. A binary archived system audit trail can be retrieved into the Empower 2 “Offline System Audit Trail” view for review and analysis.
21.	11.10 (e)	Can selected portions of the audit trail be viewed and printed by inspectors?	Yes	Full searching and filtering capabilities are available with the Empower 2 audit trails.
22.	11.10 (e)	Can selected portions of the audit trail be extracted in a transportable electronic format that can be read by regulatory agencies?	Yes	The audit trail can be backed up to an ASCII file (.txt) or to a binary file. The ASCII file can be viewed in any file viewer, while the binary file can be restored into another Empower 2 system for searching and analysis in the Empower 2 “Offline System Audit Trail” view.

Ref.			Yes/No/NA	Explanation
23.	11.10 (e)	If no audit trail is available, can the system detect that a record was altered since its last approval?	NA	Audit trails are available in the database. Alteration of information creates new values that are stored in the database. Records are not overwritten and full audit trails are available to document changes. This will require calling Waters and help from the Waters development team.
24.	11.10 (e)	Are operator name, date, time, and indication of record (or file) creation, modification or deletion recorded in audit trail?	Yes	
25.	11.10 (e)	If the predicate regulation requires it, is the reason for a change included in the audit trail?	Yes	Assuming the Empower 2 System Policies have been appropriately configured.
26.	11.10 (f)	If the system requires sequenced steps, does it ensure that the actions are performed in the correct sequence?	Yes	Empower 2 software uses Wizards to ensure proper sequencing.
27.	11.10 (g)	Does the system ensure that only authorized individuals can use the system?	Yes	In order to access the Empower 2 system, individuals must have a user account. This account will define the capabilities that user will have on the system. Without an account, no access to the system is allowed.
28.	11.10 (g)	Does the system (or procedure) verify that an individual has the authority to electronically sign a record before allowing them to do so?	Yes	The right to sign-off is a specifically assigned privilege. Users who have not been assigned this privilege may not electronically sign a record.
29.	11.10 (h)	If it is a requirement of the system that data input or instructions can only come from specific input devices (e.g. instruments, terminals); does the system check for the correct device?	NA	Empower 2 designates appropriate input based on user authentication, and not device authentication. Raw data may only come from a device on which Empower 2 acquisition software has been configured. Other instructions may only come from devices on which Empower 2 database access has been configured and enabled.

Ref.			Yes/No/NA	Explanation
30.	11.10 (i)	Is there documentation to show that persons who <i>develop</i> the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	Yes	Full documentation is available as part of an audit of Waters software development process.
31.	11.10 (i)	Is there documentation to show that persons who <i>maintain</i> or use the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
32.	11.10 (i)	Is there documentation to show that persons who <i>use</i> the system have the education, training and experience to perform their assigned tasks (including temporary and contract staff)?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
33.	11.10 (j)	Is there a written policy in place and enforced that holds individuals fully accountable and responsible for actions initiated under their electronic signatures?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
34.	11.10 (k)(1)	Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
35.	11.10 (k)(1)	Is access to "sensitive" systems documentation restricted e.g., network security documentation, system access documentation?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
36.	11.10 (k)(2)	Is there a Change Control (or equivalent) SOP governing revisions to system documentation?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
11.30 Controls for Open Systems				
37.	11.30	What controls ensure record authenticity, integrity, and confidentiality?	NA	Empower 2 software is a closed system
38.	11.30	Is data encrypted?	NA	Empower 2 software is a closed system

Ref.			Yes/No/NA	Explanation
39.	11.30	Are digital signatures used?	NA	Empower 2 software is a closed system
11.50 Signature Manifestations				
40.	11.50 (a)(1)	Do all electronically signed records contain the following information associated with the signing: <i>Full printed name of the signer</i>	Yes	The user must configure the full name of the signer for it to appear on the report.
41.	11.50 (a)(2)	Do all electronically signed records contain the following information associated with the signing: <i>Date and time of signing</i>	Yes	
42.	11.50 (a)(3)	Do all electronically signed records contain the following information associated with the signing: <i>Meaning of signature (e.g. review, approval)?</i>	Yes	Default meanings in the Empower 2 software include: review, approval, responsibility and authorship. Other signature meanings may be added to accommodate corporate requirements.
43.	11.50 (a)	Are the date and time stamps applied automatically (vs. being keyed in by the user)?	Yes	
44.	11.50 (a)	Are date and time stamps derived in a consistent way in order to be able to reconstruct the sequence of events?	Yes	Date and time stamps are the local date and time at the location where the signature was executed.
45.	11.50 (b)	Is the above information subject to the same controls as electronic records? (audit trail, access control etc.)	Yes	The user must turn on Full audit Trail in the project for this to occur.
46.	11.50 (b)	Are changes to signatures included in the audit trail?	Yes	Signatures may not be altered; new signatures may be added to a record and are fully audit trailed.
47.	11.50 (b)	Do the printed name, date, time, and signature meaning appear in every human readable form of the electronic record? (e.g. all screens and printed reports)	Yes	Electronic records are shown in human readable form in the Preview section of Empower 2 and in printed reports. A table of electronic signatures can be placed on reports that are used to view electronic records.

Ref.		Yes/No/NA	Explanation	
11.70 Signature/Record Linking				
48.	11.70	If handwritten signatures are executed to electronic records, are the handwritten signatures linked to the electronic record(s)?	NA	Handwritten signatures are not executed to electronic records. Handwritten signatures may be executed to a printed report, and such a report may include information identifying (and providing a link to) the original electronic record.
49.	11.70	If the electronic record is changed, is the signer prompted to re-sign (via either manual procedures (SOP) or technical means)?	Yes	All changes to an electronic record are audit trailed in the Empower 2 project in which the record is stored. The audit trail will include information on the user making the change, the date and time of the change, what was changed and the reason for the change. If electronic record information is modified, the electronic record can be re-signed in the Preview section of Empower 2. Each organization must develop a controlled, documented procedure to determine when a re-signing is required.
50.	11.70	Are the E-signatures linked (via technology, not procedures) to their corresponding electronic records to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means?	Yes	
Subpart C – Electronic Signatures				
11.100 General Requirements				
51.	11.100 (a)	Is each E-signature unique to one individual?	Yes	
52.	11.100 (a)	Are E-signatures ever reused by, or reassigned to, anyone other than the original owner?	No	
53.	11.100(b)	Is the individual identified adequately verified prior to issuance of an electronic signature?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.

Ref.			Yes/No/NA	Explanation
54.	11.100(b)	Is there a procedure for reissuing forgotten passwords that verifies the requestor's identity?	NA	Each organization must develop controlled, documented procedures for compliance with this requirement.
55.	11.100(c)(1)	Has certification of the intent to use electronic signatures been submitted to the agency in paper form with a traditional handwritten signature?	NA	Each organization must submit their written intent for compliance with this requirement.
56.	11.100(c)(2)	Can additional certification or testimony be supplied to show that an electronic signature is the legally binding equivalent of the signers handwritten signature?	NA	Each organization must develop their controlled, documented procedure for compliance with this requirement.
11.200 Electronic Signature Components and Controls				
57.	11.200 (a)(1)	Is the signature made up of at least two distinct identification components, such as an identification code and password?	Yes	A signature comprises a user name and a password.
58.	11.200 (a)(1)(i)	If continuous signing sessions are used, are two (or more) E-signature components required for the initial signing?	Yes	The user name and password are required for the initial signing.

Ref.	Ref.	Yes/No/NA	Explanation
59.	11.200 (a)(1)(i)	<p>If only one E-signature component is required for subsequent signings:</p> <ul style="list-style-type: none"> • Is the private component, known to and only useable by its owner, used for each subsequent signing? • Is the user required to stay in close proximity to the workstation for the entire session? • Is there an automatic logoff, or password protected screen saver that launches, after a short period of inactivity (with the password known only by one user)? 	<p>Yes</p> <p>The account password is the private component</p> <p>Yes</p> <p>Empower 2 software automatically ends the session after a period of time specified in Empower 2 System Policies Other Polices Section.</p> <p>Yes</p> <p>An inactivity period can be set in the Empower 2 system policies. If this period is exceeded, the signoff session is terminated and the signoff window is closed.</p>
60.	11.200 (a)(1)(i)	<p>If a user leaves the workstation, do procedures and/or automatic controls ensure that it is treated as a non-continuous session?</p>	<p>Yes</p> <p>Empower 2 software automatically ends the signing session after a period of time specified in Empower 2 System Policies.</p>
61.	11.200 (a)(1)(ii)	<p>Are two (or more) E-signature components required for each signing during a non-continuous signing session?</p>	<p>Yes</p> <p>The user name and password are required for each signature during a non-contiguous signing session.</p>
62.	11.200 (a)(2)	<p>Are non-biometric signatures only used by their genuine owners (e.g. by procedures or training reinforcing that non-biometric E-signatures are not "loaned" to co-workers or supervisors for overrides)?</p>	<p>NA</p> <p>Each organization must develop its own controlled, documented procedure for compliance with this requirement.</p>
63.	11.200 (a)(3)	<p>Are non-biometric signatures administered and executed so that unauthorized use requires the collaboration of two or more individuals?</p>	<p>NA</p> <p>Each organization must develop their controlled, documented procedure for compliance with this requirement. Individual users cannot view any information on other user accounts unless they are explicitly given the "Alter User" privilege. Under no circumstances is access to another user's password available to any user.</p>

Ref.			Yes/No/NA	Explanation
64.	11.200(b)	Are biometric E-signatures designed to ensure that they can be used only by their genuine owners?	NA	Empower 2 software does not use biometric E-signatures
11.300 Controls for Identification Codes/Passwords				
65.	11.300 (a)	Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals can have the same combination of identification code and password?	Yes	Empower 2 System Policies can be set to ensure that there must be unique combination of user names and passwords used on the system.
66.	11.300 (a)	Are controls (procedural or technical) in place to prevent the re-use of identification codes?	Yes	Empower 2 System Policies can be used to ensure that passwords may not be reused for individual user accounts, and that user names cannot be reused for multiple users.
67.	11.300(b)	Is the issuance of identification codes and passwords periodically checked, recalled, or revised (e.g. to cover such events as password aging)?	Yes	Empower 2 System Policies can be used to set password aging based on corporate policies.
68.	11.300(b)	Do passwords periodically expire and need to be revised?	Yes	Empower 2 System Policies can be used to set password aging based on corporate policies.
69.	11.300(b)	Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	Yes	Empower 2 allows a user account to be removed from active use. Each organization must develop controlled, documented procedures to ensure proper notification of user status changes.
70.	11.300(c)	Is a SOP in place directing action to be taken to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices used to carry or generate e-signature components?	NA	Empower 2 does not use tokens, cards or other devices to carry E-signature components.

Ref.			Yes/No/NA	Explanation
71.	11.300(c)	Does this SOP contain procedures for managing and controlling temporary or permanent token/ card replacements?	NA	Empower 2 does not use tokens, cards or other devices to carry e-signature components.
72.	11.300(d)	Are any attempts to unauthorized use detected and reported immediately to the system "security unit" (e.g. a system administrator is notified automatically by console message or paper) and, as appropriate, to organizational management?	Yes	When an invalid login attempt is made, an immediate notification is displayed on the consoles of all system administrators currently logged into the system. In addition, all system administrators not currently logged in will be informed when they next access the Empower 2 system. This information is also stored in the software message log and System Audit Trail.
73.	11.300(e)	Are there procedures covering the initial and periodic testing of devices, such as tokens or cards that bear or generate identification code or password information?	NA	Empower 2 does not use tokens, cards or other devices to carry e-signature components.
74.	11.300(e)	Does the testing include checks for proper functioning, performance degradation, and possible unauthorized alteration?	NA	Empower 2 does not use tokens, cards or other devices to carry e-signature components.