

Validation Checklist
DicksonWare™ Secure and 21 CFR 11 Requirements

<u>21 CFR Part 11 Requirements</u>	<i>Dicksonware™ Secure complies with associated 21 CFR 11 requirement?</i>	<i>Requires Customer Action prior to use to comply?</i>	<u>Comments on compliance or requirements</u>
Procedures and Controls for Closed Systems	(check = yes)	(check = yes)	<i>Customers may devise their own validation protocols that may or may not be compliant with 21 CFR 11.</i>
Is the system validated?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	To comply, customer must purchase validation certificate (N520) with each Dickson calibrated data logger that is to be used with DicksonWare™ Secure(*).
Is it possible to discern invalid or altered records?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Invalid or altered records will not open at all with Dicksonware™ Secure.
Is the system capable of producing accurate and complete copies of electronic records on paper?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Using the print function in DicksonWare™ Secure, the graph and/or datafile can be printed complete with all 21 CFR 11 requirements.
Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review, and copying by the FDA?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Unaltered valid datafiles and/or graphs can be emailed/transferred to another user of DicksonWare™ Secure.
Are the records readily retrievable throughout their retention period?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Records can be saved to any designated location/directory the customer designates. The default is for all records to be saved to "C:/Dickson/dwSecure".
Is system access limited to authorized individuals?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Only users with valid user ID and Password can access system.
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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Audit trail is secure, encrypted and contains date, time, operator, and action taken when using a validated Dickson data logger.
Upon making a change to an electronic record, is previously recorded information still available (i.e., not obscured by the change)?	<input type="checkbox"/> (Not Applicable)	<input type="checkbox"/>	Not Applicable. Datafiles cannot be modified by the customer/user. Attempts to do so render the datafile invalid.
Is an electronic record's audit trail retrievable throughout the record's retention period?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Audit trails are automatically generated and cannot be "turned off". Audit trails can be saved and retrieved indefinitely.
Is the audit trail available for review and copying by the FDA?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Like the datafiles, audit trails can be printed and/or electronically transferred/emailed to another user of DicksonWare™ Secure.
If the sequence of system steps or events is important, is this enforced by the system (e.g., as would be the case in a process control system)?	<input type="checkbox"/> (Not Applicable)	<input type="checkbox"/>	Not Applicable. There is no specific sequence of steps nor any order specific operations within DicksonWare™ Secure.

Validation Checklist
DicksonWare™ Secure and 21 CFR 11 Requirements

<u>21 CFR Part 11 Requirements</u>	<i>Dicksonware™ Secure complies with associated 21 CFR 11 requirement?</i>	<i>Requires Customer Action prior to use to comply?</i>	<u>Comments on compliance or requirements</u>
Does the system ensure that only authorized individuals can use the system, electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DicksonWare™ Secure has a mandatory User ID and Password login system with two levels of operational/system access, administrator and user levels, ensuring that only authorized individuals can access the system and use the various features according to their level of access.
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 or 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 weigh scales, or remote, radio controlled terminals.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The software will accept data only from validated data loggers designed and manufactured by Dickson specifically for use with DicksonWare™ Secure using Dickson's proprietary communications protocols. Each specific unit capable of working with DicksonWare™ Secure is uniquely identified by the software for further system checks.
Is there documented training, including on the job training for system users, developers, IT support staff?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Users may arrange/purchase system training from Dickson or provide their own training through testing and the DicksonWare™ Secure help files and documentation. DicksonWare™ Secure is user-friendly and safeguards against user error to limit the amount of training required.
Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Customer must create a written policy explaining to DicksonWare™ Secure users that they are responsible for actions done under their login.
Is the distribution of, access to, and use of systems operation and maintenance documentation controlled?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Our software controls access and use of itself. Customer is responsible for obeying the licensing terms and distribution of the software, and the computer hardware and software DicksonWare™ Secure application runs on.
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?	<input type="checkbox"/> (Not Applicable)	<input type="checkbox"/>	Not Applicable. Audit trails are not changeable. They are encrypted and can't be modified.

Validation Checklist
DicksonWare™ Secure and 21 CFR 11 Requirements

<u>21 CFR Part 11 Requirements</u>	<i>Dicksonware™ Secure complies with associated 21 CFR 11 requirement?</i>	<i>Requires Customer Action prior to use to comply?</i>	<u>Comments on compliance or requirements</u>
Additional Procedures and Controls for Open Systems			
Is data encrypted?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The data is encrypted.
Are digital signatures used?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Digital signatures are used.
Signed Electronic Records			
Do signed electronic records contain the following related information? - The printed name of the signer - The date and time of signing The meaning of the signing (such as approval, review, responsibility)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Electronic records do contain the name, date/time stamp, and action.
Is the above information shown on displayed and printed copies of the electronic record?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Related information is displayed on the electronic record and on printed copies.
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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	The signatures cannot be copied, cut or transferred and are linked to the original record in an encrypted audit trail.
Are electronic signatures unique to an individual?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	The software will not let you use duplicate digital signatures. Recommend customer include a statement in their written procedures that only one person is linked to each user ID.
Are electronic signatures ever reused by, or reassigned to, anyone else?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Recommend customer include a SOP statement that user IDs are not to be reused or reassigned to anyone else.
Is the identity of an individual verified before an electronic signature is allocated?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Unique User ID and Password ensure individual verification.
Electronic Signatures (Non-biometrics)			
Is the signature made up of at least two components, such as an identification code and password, or an id card and password?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User ID and Password
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.)	<input type="checkbox"/>	<input type="checkbox"/>	Not Applicable. The session ends when one signs off. Multiple signings on the same session does not apply.
If signings are not done in a continuous session, are both components of the electronic signature executed with each signing?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User ID and Password, everytime
Are non-biometrics signatures only used by their genuine owners?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	User ID and Password

Validation Checklist
DicksonWare™ Secure and 21 CFR 11 Requirements

<u>21 CFR Part 11 Requirements</u>	<i>Dicksonware™ Secure complies with associated 21 CFR 11 requirement?</i>	<i>Requires Customer Action prior to use to comply?</i>	<u>Comments on compliance or requirements</u>
Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
Has it been shown that biometrics electronic signatures can be used only by their genuine owner?	(Not Applicable) <input type="checkbox"/>	<input type="checkbox"/>	Not Applicable.
Controls for Identification Codes and Passwords			
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?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DicksonWare™ Secure will not allow duplicate User IDs or Passwords.
Are procedures in place to ensure that the validity of identification codes is periodically checked?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Identification validity is checked each and every time used.
Do passwords periodically expire and need to be revised?	<input type="checkbox"/>	<input type="checkbox"/>	Expiration of passwords, if necessary, is determined by the customer's system administrator and the company's SOP (Standard Operating Procedures) regarding password policies.
Is there a procedure for recalling identification codes and passwords if a person leaves or is transferred?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	DicksonWare™ Secure, under administrator logging, is capable of administering other User IDs and Passwords if necessary.
Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Sytem Administrator may disable other users' accounts. Customers may document their own SOP for handling the disabling of accounts.
Is there a procedure for detecting attempts at unauthorized use and for informing security?	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	An audit trail provides detection of unauthroized use. The review and use of that data is the customer's responsibility.
Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The customer should have an internal procedure for reporting unauthorized use to management.
Is there a loss management procedure to be followed if a device is lost or stolen?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The customer should have an internal procedure if a Dickson data logger is potentially compromised. Dickson can repair, replace or recalibrate the loggers used with DicksonWare™ Secure.
Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	The customer should have an internal procedure if a Dickson data logger is potentially compromised. Dickson can repair, replace or recalibrate the loggers used with DicksonWare™ Secure.

Validation Checklist
DicksonWare™ Secure and 21 CFR 11 Requirements

<u>21 CFR Part 11 Requirements</u>	<i>Dicksonware™ Secure complies with associated 21 CFR 11 requirement?</i>	<i>Requires Customer Action prior to use to comply?</i>	<u>Comments on compliance or requirements</u>
Are there controls over the issuance of temporary and permanent replacements?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Replaced, repaired or recalibrated units should be "Validated" prior to use, whether they are to be used as temporary or permanent replacements.
Is there initial and periodic testing of tokens and cards?	(Not Applicable) <input type="checkbox"/>	<input type="checkbox"/>	Not Applicable. No tokens/cards used with this system.
Does this testing check that there have been no unauthorized alterations?	(Not Applicable) <input type="checkbox"/>	<input type="checkbox"/>	Not Applicable. No tokens/cards used with this system.