



## **White paper for association of AOIP systems in a CFR 21 part 11 configuration**

AOIP system, association of a physical measuring device and LW1 or VISULOG software, provides a fully 21 CFR PART 11 compatible system. It creates one or/several audit trails, for all actions, events during a qualification. The user is authorised to access to the systems through a password and user ID given by the Administrator.

Access Rights are also decided by the administrator.

All the records are protected in a native format and can not be corrupted.



Questions pertaining to 21 CFR Part 11 and AOIP Control Systems	Answer	Comment
<b>11.1, 11.2, 11.3: Is the system regulated by 21 CFR Part 11?</b>		
Does the system store e-data to a hard drive, optical drive, and floppy disk, CD, or any other form of durable media?	Yes	Hard drive
Does the system store e-data with the intent of future retrieval or any purpose?	Yes	
Does this computerized system create, modify, maintain, archive, retrieve, or transmit any electronic record(s) that are required to demonstrate compliance with FDA regulations?	Yes	
Is this computerized system used exclusively to transmit paper records by electronic means, such as FAXs and scanned images?	No	
Do FDA regulations permit the use of electronic records for this required documentation?	Yes	
Is the computerized system an "Open System" or a "Closed System"?	Closed system	
Does the computerized system require electronic signatures on the electronic records?	Yes	
Are E-sigs are required when the: <ul style="list-style-type: none"> <li>records are printed out, would or do you need to sign them.</li> <li>person's name is saved as a field in the file/database and expect it to be right on the form, printout, and/or archive.</li> <li>person signing has attested that he did or saw something, or that he is authorizing some action.</li> </ul>	Yes  yes  Yes	
What type of electronic signature does this system use? <ul style="list-style-type: none"> <li>Handwritten signature executed to electronic record</li> <li>Biometric</li> </ul>	No	



<ul style="list-style-type: none"> <li>• Identification code/password</li> <li>• Token / password</li> </ul>	<p>No</p> <p>Yes</p> <p>No</p>	
<b>SUBPART B ELECTRONIC RECORDS 11.10: Controls for Closed Systems</b>		
Is sequence of execution of steps by operators key to proper execution of tasks?	Yes	
Does the system control such sequences?	yes	
<b>Validation</b> – Is the system validated in accordance with applicable regulatory requirements to ensure: <ul style="list-style-type: none"> <li><input type="checkbox"/> Accuracy. [11.10 (a)]</li> <li><input type="checkbox"/> Reliability. [11.10 (a)]</li> <li><input type="checkbox"/> Consistent intended performance. [11.10 (a)]</li> <li><input type="checkbox"/> Ability to discern invalid or altered records. [11 .10 (a)].</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>	<b>A Validation binder</b> containing quality test plans and test cases is available to customers
Can accurate and completed records be generated in human-readable and electronic form? (Includes associated metadata)	Yes	
<b>Inspectability</b> – Can the system: <ul style="list-style-type: none"> <li><input type="checkbox"/> Generate accurate and complete copies of records in both human and electronic form for inspection reviews and copying by the FDA. [11 .10 (b)]</li> <li><input type="checkbox"/> Protect records to enable their accurate and ready retrieval throughout the records retention period. [11.10 (c)]</li> </ul>	<p>Yes</p> <p>Yes</p>	
<b>Security-</b> Are security procedures and controls designed and implemented to include: <ul style="list-style-type: none"> <li><input type="checkbox"/> System access limited to authorized individuals. [11.10 (d)](Physical access)</li> <li><input type="checkbox"/> Operational system checks that enforce the proper sequencing of steps in a process (as appropriate). [11.10 (0)]</li> </ul>	N/A	Responsibility of the user and its Company Does not use physical access, only user ID and password.

<p>Authority checks to ensure only authorized individuals can:</p> <ul style="list-style-type: none"> <li>• Use the system. [11.10 (g)] (Logical access)</li> <li>• Electronically sign a record. [11.10 (g)]</li> <li>• Access the operation or computer system input or output device. [11.10 (g)]</li> <li>• Alter a record. [11 .10 (g)]</li> <li>• Perform the specified operation. [11.10 (g)]</li> <li>• Device or terminal checks shall determine validity of the source of input or operation (as appropriate). [11 .10 (h)]</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>	
Does the system maintain secure computer generated audit trails?	Yes	
Is the original data accessible from records that have been altered?	Yes	
Are there specific operations with privileges that should be keyed to individual users?	Yes	
Does the system employ authority checks to ensure that a given operation be executed only by authorized individuals?	Yes	
Are device check appropriate to ensure that input comes only from authorized sources?	Yes	
Does the system control such input?	Yes	
<p><b>Audit Trails</b> – Are procedures and controls designed and implemented for audit trails to:</p> <ul style="list-style-type: none"> <li>• Be secure. [11.10 (e)]</li> <li>• Be computer-generated. [11.10 (e)]</li> <li>• Be time- and date-stamped. [11.10 (e)]</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p>	
<p>Can the system independently record the date/time of operator entries and actions that:</p> <ul style="list-style-type: none"> <li>• Create electronic records. [11.10 (e)]</li> <li>• Modify electronic records. [11.10 (e)]</li> <li>• Maintain electronic records. [11.10 (e)]</li> <li>• Delete electronic records. [11.10 (e)]</li> </ul>	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>	

Does the system ensure that: <ul style="list-style-type: none"> <li>• Alterations to electronic records shall not obscure previously recorded information. [11.10 (e)]</li> <li>• Audit trail records shall be maintained for at least as long as the retention of the underlying records. [11 .10 (e)]</li> <li>• Audit trail records shall be available for FDA review and copying. [11.10 (e)]</li> </ul>	Yes Yes Yes	
Does the audit trail track who made an alteration and when it was made?	Yes	
Does the audit trail track why the alteration was made?	Yes	
<b>Personnel Qualifications</b> – Do persons have the education, training and experience to perform their assigned tasks <ul style="list-style-type: none"> <li>• Developer(s) of the computerized system. [11 .10 (i)]</li> <li>• Maintainer(s) of the computerized system. [11 .10 (i)]</li> <li>• User(s) of the computerized system. [11.10 (i)]</li> </ul>		Responsibility of the administrator The supplier should provide such training
<b>Accountability and Responsibility for Actions</b> Are there written policies and/or procedures that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. [11-10 g)]		Responsibility of the administrator
<b>Systems Documentation Controls</b> - Are there appropriate controls over systems documentation including - Adequate controls over the documentation for system operation and maintenance to include: <ul style="list-style-type: none"> <li>• distribution of documentation. [11.10 (k)(1)]</li> <li>• access to documentation. [11.10 (k)(1)]</li> <li>• use of documentation. [11.10 (k)(1)]</li> </ul>		Responsibility of the administrator
Revision and change control procedures to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation. [11.10 (k)(2)1]		Responsibility of the administrator

<b>11.50: SIGNATURE MANIFESTATIONS</b>		
<p><b>Signature Manifestations</b> Do signed electronic records contain information associated with the signing that clearly indicates the:</p> <ul style="list-style-type: none"> <li>• printed name of the signer. [11.50 (a)(1)]</li> <li>• date and time when the signature was executed. [11.50(a)(2)]</li> <li>• meaning of the signature. [11.50 (a)(3)]</li> </ul>	<p>Yes Yes Yes</p>	
<p>Are all items identified in 11.50 (a)(1) 11.50 (a)(2) and 11.50(a)(3) above subject to the same controls as for electronic records. [11.50 (b)]. Included as part of any human readable form of the electronic record (such as electronic display and/or printout or report). [11.50 (b)]</p>	<p>Yes</p>	
<p>Does the system use electronic signatures/authorizations?</p>	<p>Yes</p>	
<p>Does the system use biometric identification?</p>	<p>NO</p>	
<p>Does the system use dual component identification with at least ID and password one private to the user? (e.g. user ID and password or user ID and token?)</p>	<p>Yes</p>	<p>ID and password</p>
<p>Do all manifestations associated with an e-sig including screen displays, printouts, and other human-readable format clearly indicate the following:</p> <ul style="list-style-type: none"> <li>• The name of the signer</li> <li>• Date and time of the signing</li> <li>• Meaning of the signature (e.g. review approval authorship etc)</li> </ul>	<p>Yes Yes Yes</p>	
<b>11.70: SIGNATURE RECORD LINKING</b>		
<p><b>Signature/Record Linking –</b> Are the electronic signatures and handwritten signatures executed to electronic records linked to their respective electronic records to ensure</p>	<p>Yes</p>	

that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means? [11.70]		
<b>SUB-PART C: ELECTRONIC SIGNATURES</b> <b>11.100: General Requirements for Electronic Signatures</b>		
Is each electronic signature unique to one individual and can not be reused by, or reassigned to, anyone else? [11.100 (a)]	Yes	
Is the identity of the individual verified prior to the organization establishing, assigning, certifying, or otherwise sanctioning that administrator. individual's electronic signature? [11.100 (b)]		Responsibility of the administrator
The persons using electronic signatures, prior to or at the time of use should certify to the FDA that the electronic signatures used in the computerized system on or after August 20, 1997 are intended to be the legally binding equivalent of traditional handwritten signatures? [11.100 (c)]		Responsibility of the user
A certificate should be submitted in paper form and signed with traditional handwritten signature to the appropriate FDA Office specified in the Regulation? [11.100 (c)(1)]		Responsibility of the user
<b>11.200: ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS</b>		
<b>Electronic Signatures Not Based On Biometrics</b>		
Do the electronic signatures that are not based on biometrics <ul style="list-style-type: none"> <li>Employ at least 2 distinct identification components such as an identification code and password. [11.200 (a)(1)] 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. [11.200 (a)(1)(i)]. 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</li> </ul>	Yes	

<p>electronic signature components. [11.200 (a)(1)(ii)]</p> <ul style="list-style-type: none"> <li>• Be used only by their genuine owners. [11.200 (a)(2)]</li> <li>• 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. [11.200 (a)(351)]</li> </ul>	<p>Yes</p> <p>Yes</p>	
<p><b>11.300: CONTROLS FOR IDENTIFICATION CODES/PASSWORDS</b></p>		
<p><b>Controls for Identification Codes/Passwords</b></p>		
<p>Do persons employ controls to ensure their security and integrity when using electronic signatures based upon use of identification codes in combination with passwords?</p>		<p>Responsibility of the user</p>
<p>Do they have a unique combination of identification code password? [11.300 (a)]</p>	<p>Yes</p>	
<p>Are the identification code and password issuances periodically checked, recalled, or revised (e.g., to cover such events as password aging)? [11.300 (b)]</p>		<p>Responsibility of the administrator.</p>
<p>Are procedures and controls designed and implemented for devices which bear or generate identification code or or password information to:</p> <ul style="list-style-type: none"> <li>• Electronically deauthorize devices that have been lost, stolen or potentially compromised. [11.300 (c)]</li> <li>• Issue temporary or permanent replacements using suitable rigorous controls. [11.300 (c)]</li> </ul>	<p>N/A</p> <p>N/A</p>	<p>No device bears User ID or password</p>
<p>Are there transaction safeguards implemented to:</p> <ul style="list-style-type: none"> <li>• Prevent unauthorized use of identification codes and passwords.</li> </ul>	<p>No</p>	<p>Responsibility of the administrator</p>

<p>[11.300 (d)]</p> <ul style="list-style-type: none"> <li>• Detect any attempt at unauthorized use of identification codes and/or passwords. [11.300 (d)]</li> <li>• Report in an immediate and urgent manner any attempt at unauthorized use of identification codes and passwords to the system security unit, and management. [11.300 (d)]</li> <li>• Initial and periodic testing of devices that bear or generate identification code or password information? [11.300 (e)]</li> </ul>	<p>No</p> <p>No</p> <p>No</p>	
<b>OTHER QUESTIONS</b>		
Are the electronic signatures irrevocably linked to the records approved such that they are non-repudiatable?	Yes	
Does the system have a mechanism to terminate an idle session required for where e-sigs are possible?	Yes	
Is it possible for another individual to alter a signed record without an audit trail while leaving the e-sig intact?	N/A	Rendered unusable.
Is there a mechanism to ensure that passwords and/or ID tokens are aged?	Yes	
If tokens are used are there procedures to periodically test them for proper function and security?	N/A	No token used
If tokens are used, are there lost management procedures to de- activate lost or missing tokens?	N/A	No token used
Are there controls that ensure that ID/password combinations are unique?	Yes	
Are there detection procedures/alarms to detect and report attempted security breaches?	No	