FlowCam®

Frequently Asked Questions about 21 CFR Part 11 Compliance in VisualSpreadsheet 6

Name/Version of Software:	VisualSpreadsheet® 6
Description of Software:	VisualSpreadsheet is FlowCam's paired, proprietary software that aquires, sorts, and filters digital particle images and enables the user to analyze the data obtained by FlowCam.

21 CFR Part / Subpart and Associated Question	Answer as it pertains to VisualSpreadsheet Software
11.10 (a) Has the system been validated to ensure accuracy, reliability, and consistent intended performance?	Yes. Software and instrument validation occur during manufacturing and QC testing. IQOQ can also be performed on site. Instrument validation is based on sizing and counting with NIST certified bead standards.
11.10 (a) Does the validation documentation show that 21 CFR Part 11 audit trail and methodological control requirements are functioning?	Yes.
11.10 (a) Is the hardware and software documentation related to the system readily available to inspecting authorities?	Yes.
11.10 (a) Is the system able to detect invalid or altered records where applicable (e.g. invalid field entries, fields left blank that should contain data, values outside of limits)?	Yes. The audit trail contains this information and cannot be altered.
11.10 (b and c) Is it possible to view and print accurate and complete copies of the electronic records throughout the records retention period?	Yes.
11.10 (b and c) When electronic records are displayed, printed, or copied, is their meaning and content preserved?	Yes. The audit trail contains this information and cannot be altered.
11.10 (c) Are the electronic records protected via the application against intentional or accidental modification or deletion?	Yes.

11.10 (c) Is the retention period formally defined?	Not a function of the software. Determined by the user’s Information Technology department.
11.10 (c) Are electronic records archived off the system?	Not a function of the software. Determined by the user’s Information Technology department.
11.10 (d) Is there a controlled, documented process for granting access to a new user, for changing privileges for an existing user, and for deletion or deactivation of user accounts?	Yes.
11.10 (d and g) Does the software use authority checks to ensure that only authorized individuals can use the system?	Yes.
11.10 (d and g) Are there different levels of access based on user responsibilities?	Yes. There are 4 levels of access: 1. Administrator- creates and manages other users 2. Supervisor- authorizes user changes to data runs 3. User- collects data runs, performs data analysis 4. Lab Technician- only performs data analysis
11.10 (d and g) Do user access level changes need approval by Supervisor level accounts?	Yes.
11.10 (e) Does the software use 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?	Yes. The audit trail contains this information and cannot be altered.
11.10 (e) Can the audit trail be disabled?	No.
11.10 (e) Does the audit trail have the ability to record the “Who”, “When”, “What”, and “Why”?	Yes.
11.10 (e) Can selected portions of the audit trail be viewed and printed by inspectors (available for agency review and copying)?	Yes.
11.10 (f) Does the software use operational system checks to enforce permitted sequencing of steps and events, as appropriate?	The system requires supervisor input to determine correct procedure/sequencing.
11.10 (g) Does the software verify that an individual has the authority to electronically sign an electronic record before allowing them to do so?	Yes.

11.10 (h) Is a secondary device used to collect source data or operation instruction?	No. The FlowCam is the source of generated data and operation instruction. Original data runs are preserved and changes are marked in the audit trail.
11.50 (a) Do signed electronic records contain the full printed name of the signer, the date and time when the signature was executed; and the meaning (such as review, approval, responsibility, or authorship) associated with the signature?	Yes.
11.50 (a) Are dates and time stamps automatically applied by the system?	Yes.
11.50 (a) Are the source and format of the system date and time defined, controlled, unambiguous, and protected from unauthorized change?	Yes.
11.50 (b) Are the items identified in 11.50 (a) subject to the same controls as for electronic records and included as part of any human readable form of the electronic record (such as electronic display or printout)?	Yes.
11.70 Are users required to provide an electronic signature?	Yes. A user ID and password are required to gain access to the application.
11.70 Are electronic signatures 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.
11.100 (a) Is each electronic signature unique to one individual?	Yes.
11.100 (a) Are electronic signatures ever reused by, or reassigned to, anyone other than the original owner?	No.
11.100 (a) Does the system prevent unauthorized individuals from signing electronically on behalf of another?	Yes.

11.100 (b) Before assigning an individual's electronic signature, is the identify of the individual verified?	Not a function of the software.
11.100 (c) Do persons using electronic signatures certify/understand that said electronic signatures are intended to be the legally binding equivalent of traditional handwritten signatures?	Not a function of the software. This would be covered during training and/or by the Supervisor.
11.200 (a)(1) Do electronic signatures employ at least two distinct identification components such as an identification code (or User ID) and password?	Yes.
11.200 (a) Are passwords required to be of a minimum length?	Yes.
11.200 (a) Must passwords comply with certain complexity requirements?	The administrator can set password requirements.
11.200 (a)(1) Is the individual required to sign in using all of the electronic signature components for each period of controlled system access?	Yes.
11.200 (a)(2) Are electronic signatures only used by their genuine owners (e.g. do procedures reinforce that signatures are not "loaned" to co-workers)	Not a function of the software.
11.200 (a)(3) Are electronic signatures 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?	Not a function of the software.
11.200 (b) Are electronic signatures based upon biometrics designed to ensure that they cannot be used by anyone other than their genuine owners?	Software does not currently support biometric electronic signatures.
11.300 (a) Are controls in place to maintain the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password?	Yes.

11.300 (b) Are identification codes and password issuances periodically checked, recalled, or revised (e.g. to cover such events as password aging)?	Not a function of the software.
11.300 Is there a procedure to reset a forgotten password that verifies the requestor's identity?	Yes.
11.300 Is the Administrator the only one with access to reset a password?	Yes.
11.300 Does the application lock out a user after consecutive failed login attempts?	Yes. After 3 failed attempts, the user will be asked to contact the Administrator.
11.300 Is the Administrator the only one with the ability to unlock users?	Yes.
11.300 (c and e) Does the system use tokens, cards, or other devices that bear or generate identification code or password information?	No.
11.300 (d) Does the software use transaction safeguards to prevent unauthorized use of passwords and/or identification codes?	Yes. The password file is encrypted so that passwords cannot be read by ordinary means.