PROCESSVIEW 21 CFR PART 11 COMPLIANCE FOR THE WATLOW F4T CONTROLLER

Abstract

ProcessView has been designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. In the 21 CFR Part 11 requirements below, each section of the clause is specifically addressed by the ProcessView software.

ProcessView 21 CFR Part 11 Compliance

	5.2 Electronic Records (Subpart B)			
Section #	**Requirement**	**Yes**	**No**	**ProcessView Capability**
	11.10 Controls for closed systems.			
	Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity , and when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine, Such procedures and controls shall include the following:			ProcessView and the Watlow F4T must be configured as a closed system for the purpose of limiting access and maintaining the integrity of electronic records. The Watlow F4T controller must have its front touch screen "locked out" in order for all operational changes to go thru the ProcessView software so a user cannot make changes directly to the Process without an audit trial record being recorded. Secure methods for operator, engineer and supervisor access to the major operations (process operation, process data datalogging and profile creation and editing) are designed in accordance with Part 11.
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	YES		• Completed data files by the software are closed by the system and permanently linked to an encrypted signature file • Additional encrypted digital signatures can be added to any closed data file if the user has the appropriate security rights • System checks integrity of closed data files and any change to a closed data file results in an integrity failure notification • View digital signatures for any file • Check integrity of file, digital signatures and provide real-time results
(b)	The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspections, review, and copying by the agency.	YES		• Automatically data log process parameters via secure, digitally signed data files • View the data log as it is being recorded real-time • Data can also be converted to Excel spreadsheets in a CSV format for FDA inspection without altering the original encrypted data file • Data files that have been altered will fail digital signature validation when viewing has been attempted
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	YES		• Data log files can be exported to remote network locations, Cloud databases, local hard drive or FTP sites. • Data log files and Audit Trial files that validates file integrity and allows viewing without altering the original data file
(d)	Limiting system access to authorized individuals.	YES		• Select the "type", or level, for a user and assign a unique username and password for each use • Assign user rights, or privileges, for each user type • Optionally enable re-authentication to enforce security even if a user forgets to log-off. Re-authentication prompts the user for their username and password before changing any process control variable
(e)	Use of 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. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period for at least as long as that required for the subject electronic records and shall be available for agency review and copying.	YES		• By default, the stem automatically maintains a history of operator entries and cations. Audit trail entries contain information answering: Who, When, Where, What, Why and Ho whenever the data is available and applicable. Audit trail entries also contains the new and previous value to prevent previously recorded information from being obscured. • Continuously generate a detailed audit trail that includes time/date stamps of operator access, operator actions, system changes, setup changes, and other critical functions • The audit trial is an integral part of the electronic archive record and remains as long as the records are retained • The encrypted audit trail file is viewable with the Audit Trail viewer
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	YES		• Configurable user rights/multi-security level-based enforcement with re-authentication option provides a dual check of operator authentication before process changes can be made at the system level • All operator actions are recorded in a secure encrypted audit trail

(g)	Use of authority checks to ensure that any authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand	YES		• Each user is assigned to one of four user groups or types. Each of the four groups can represent a different level of privileges and security • Permissions for each user group can be individual enabled and disabled for every major function of the system • All operator actions are recorded in a secure Audit Trail file • Signed files are used to verify the integrity of the files • Optionally enable re-authentication to enforce security if a user forgets to log-off. Re-authentication prompts the user for their username and password before changing any process parameter
(h)	Use of device (e.g., terminal) checks to determine, as appropriate the validity of the source of data input or operational instruction.	YES		• All the audit trail entries recording operations performed from operator consoles are stamped with the username used to perform the operation, along with a timestamp documenting when the audit trail entry was recorded
(i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	N/A		• Users are responsible for developing implementing, and maintaining their own training programs and establishing criteria for the determination of qualifications for person who develop, maintain, and /or use ProcessView and 21 CFR Part 11 • A proper education program according to the work assignment of each individual is required. The execution of the education program should be recorded
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under the electronic signatures, in order to deter record and signature falsification.	N/A		• Users are responsible for developing, implementing, maintaining and enforcing their own written policies and procedures. Strict adherence to effective and practical policies and procedures ultimately affects the quality of the final product.
	11.50 Signature Manifestations			
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	YES		
(1)	The printed name of the signer	YES		• The user name is authenticated in real-time by checking the username against the registered user names in the system • The name can also be put in the comments column of the audit trail • Audit trail entries contain the username and the full name of the user
(2)	The data and time when the signature was executed; and	YES		• Each record int eh audit trail is time stamped with year, month, day, hour, minute, second and time zone offset
(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	YES		• Each record requiring electronic signature confirmation in the audit trail can contain a meaning/reason field for entry by the user at the time of confirmation
(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).	YES		• The electronic signatures of users are included in the audit trail containing information (a)(1), (a)(2), and (a)(3). It is available in human readable form as a CSV file. • Only users with appropriate security rights can digitally sign a closed data file.
	11.70 Signature/record linking			
	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, coped, or otherwise transferred to falsify an electronic record by ordinary means.	YES		• Digital signatures are automatically linked to each data file when the file is completed • Any data file with a missing signature file will automatically fail during viewing of the data file with the viewer • Usernames linked to person full names are automatically included in the Audit Trail by the software with the relevant electronic records

ProcessView 21 CFR Part 11 Compliance

	11.100 General requirements			
(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	YES		• The system administrator maintains the Usernames and sets the initial password. Each user should change their own password to make it confidential. A second authentication factor using personal identification number (PIN) can optionally be linked to each user. • Once a Username becomes invalid (retire, transfer), as set by the administrator, the Username cannot be used again.
(b)	Before an organization establishes, assigns certify, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall very the identity of the individual.	N/A		• Users are responsible for administration of user accounts. Policies and procedures have to be implemented to meet this requirement.
(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	N/A		• Users are responsible to certify to the agency that the electronic signatures in their system are intended to be legally binding. This should be done prior to utilizing electronic signatures in their system and only aft the agency recognizes that the certification sis complete.
(1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, t0 the Office of regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857	N/A		• Users are responsible to ensure that this certification is forwarded as specified by the agency.
(2)	Persons using electronic signatures shall upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the sign's handwritten signature.	N/A		• Users are responsible to provide any additional evidence and testimony, as requested by the agency, that a specific electronic signature is legally binding. The agency should be convinced of the testimony prior to utilizing the electronic system.
	11.200 Electronic signature components and controls			
(a)	Electronic signatures that are not based upon biometrics shall:			
(1)	Employ at least two distinct identification components such as an identification code and password.	YES		• ProcessView electronic signatures require a username and password as well as an option 3rd factor (PIN) for authentication of individuals. • The username is a unique string of up to 15 alphanumeric characters assigned by the system administrator. • The password is a user (system administrator) defend string of a minimum of eight and maximum of 12 characters. Each password is a strongly typed password, requiring an uppercase letter, a lower-case letter, a number and a special character • The re-authentication option requires that all users log in each time a system process change is made, even if the user is already logged in the system. • All login operation (and re-authentication login) requires the unique Username and password during each login
(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 electronic signature components.	YES		• ProcessView requires both username and password to be entered when first logging into the system • If a series of actions requiring an electronic signature are taken, both components of the signature are required initially (i.e. both the username and the user's password). Only the User's Password need to be entered for subsequent signings. • If a user is inactive for a configurable period of time, the current user will automatically be logged out
(ii)	When an individual executes one or more signings not performed during a sing, contiguous period of controller	YES		• If the user is logged out either manually or automatically, further operations cannot be performed until the user logs in again. After the log in the system behavior is the same as for (a)(1)(i). The first

	system access, each signing shall be executed using all of the electronic signature components.			electronic signature in the new period requires the username and password
(2)	Be used only by their genuine owners. Be administered and executed too ensure that attempted use of an individual's electronic signature by anyone other than is genuine owner requires collaboration of two or more individuals.	YES		• Users are responsible for administration of user accounts. The password of a user is set the first time that a user logs onto the system. The password should not be disclosed to anyone, not even the system administrator. Policies and procedures must be also be implemented to meet this requirement • All successful and failed login attempts are written to the secure, encrypted audit trail • Only 3 attempts are permitted for user login. When the user login data does not match an authorized user in the system If the user attempts fail the user will be locked out for a configurable time period from the system • All login operation (and re-authentication login) requires the unique Username and password during each login
	11.300 Controls for identification codes/passwords			
	Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ control to ensure that security and integrity. Such controls shall include: Maintaining the uniqueness of each combined identification code and password, such that no tow individuals have the same combination of identification code and password. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). Following loss management procedures to electronically deauthorize lost, stolen, missing , or otherwise potentially compromised tokens, card, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable rigorous controls Use of transition safeguards to prevent unauthorized use of password and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at unauthorized us to the system security unit, and as appropriate, to organization management. Initial and period testing of devices, such as tokens or cards, that bear or generate identification cod or password information to ensure that they function properly and have not been altered in an unauthorized manner	YES		• Users of ProcessView must employ controls to ensure the security and integrity of users and user data entered into the system • System can be configured to password expiration based on a configurable number of days. A new password will then be required, having provide the old one, before accessing any other functions • The system will not allow more than one user with the same Username to be entered into the system. Each user entered in to the system must have a unique Username. The administrator will be prompted during user entry if the username already exists. • The secure, encrypted audit trails stores all modifications made to user data.