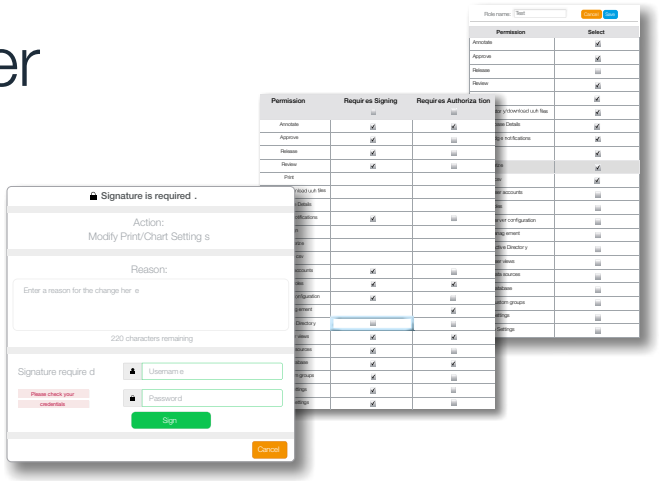
Eurotherm Data Reviewer FDA 21 CFR Part 11

(Auditor Option)

Eurotherm®



Optimize Operational Efficiency with Advanced Data Management Solutions

Regulatory Compliance Considerations

As part of an ongoing commitment to aid compliance to the US Code of Federal Regulations from the Foodand Drug Administration (FDA) and specifically FDA 21 CFR Part 11 requirements, this data sheet demonstrates how Eurotherm domain expertise helps customers meet the various requirements of FDA 21 CFR Part 11.

Each subsection considered is listed in the header of the tables below, and the statements within each table are accompanied by a commentary demonstrating how the Eurotherm solution aids compliance.

Sub Part B - Electronic Records

11.10 Controls for Closed Systems	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Eurotherm® offer assistance in validating products to Good Automated Manufacturing Process (GAMP) guidelines. Original data that is recorded in files that are in a binary, compressed and checksummed format proprietary to Eurotherm. Details are not published. The viewing tool rejects invalid/altered (i.e. incorrectly checksummed) records. Extensive testing is carried out by Eurotherm Ltd, an ISO 9001 certified company. Validation (and maintenance of the validated state) is further supported by automatic incrementing of configuration/security version numbers each time a change is saved. These numbers are stored in the audit trail.
(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.	True, accurate and complete copies on screen or printouts are available through the use of Eurotherm Data Reviewer. True, accurate and complete electronic copies are available by copying the raw data files or by setting up a 'PDF printer' (requires Adobe Acrobat or similar) in order to export graphs in PDF format.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Data can also be periodically pulled from the product using Eurotherm Data Reviewer. Once data has left the recorder, the strategy for security and backup of data remains the responsibility of the user.
(d) Limiting system access to authorized individuals.	Individual password protected user accounts.
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 at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Tamper-resistant (embedded in the binary history file), computer-generated, time-stamped audit trail including notification acknowledgment, logins, signature details and configuration changes.

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	If required a second authorization signature may be applied, which is also recorded in the audit trail.
g) Use of authority checks to ensure that only authorised 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.	Individual password protected user accounts. Each user can have their own set of access permissions or privileges to customize what they can do to the application.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Events are logged. Access to Data Reviewer configuration is controlled, and changes made are recorded in the audit trail.
(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.	Procedural.
(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to detect record and signature falsification.	Procedural. However, Microsoft® Active Directory can be used to manage logins and password procedures. alternatively, you can define your login and password procedure within Data Reviewer.
(k) Use of appropriate controls over systems documentation including: (1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance. (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Procedural in accordance with ISPE Gamp© 5 guidelines and file configuration checksum management during change control.

11.30 Controls for open systems	
Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in Sec. 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	The application is targeted for use within closed systems. With appropriate external systems/procedures the application may be used in an open system.

11.50 Signature Manifestations	
(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The signed records, containing the printed name (user ID), date, time and meaning are attributable to an individual. Meaning includes signed/authorized together with an automatically generated type (e.g. 'config' for a configuration change), plus an Operator entered note (designated as either: annotation, approval, review, release).
(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).	Name (user ID), timestamp and meaning are all embedded in the binary format history 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, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Signature manifestation is embedded in the binary format history file. For hybrid systems, printouts created via Euortherm Data Reviewer for handwritten signatures will always contain the timestamp details which permit re-creation from the original data.

Sub Part C- Electronic Records

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. (b) Before an organisation establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organisation shall verify the identity of the individual.	Eurotherm Data Reviewer complies with this requirement, as user accounts cannot have the same user name. Expired accounts remain in the system and are set to 'retired'. The number of user accounts is not limited within the software. Procedural.
(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. **(1)** The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. **(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 signer's handwritten signature.	Procedural.

11.200 Electronic signature components and controls	
(1) Employ at least two distinct identification components such as an identification code and password. **(i)** 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. **(ii)** 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.	Requires re-entry of user ID and password during a signing. Both components will be required for all signings.
(2) Be used only by their genuine owners.	Users can only change their own passwords and no read access to other users passwords is provided. It is also possible to have logins time out after a set period of inactivity; to limit the number of login retries before an account is disabled; to set a minimum length for passwords; and to force password expiry after a set number of days, prevent password re-use and force use of non-alphanumeric characters. Eurotherm Data Reviewer can also utilize Microsoft Active Directory to manage user authentication.
(3) 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.	Users can only change their own passwords and no read access to other users passwords is provided. Unless a user has shared their password, a full audit trail will be left. With the Auditor option enabled, it is further possible to force system administrator changes for user accounts to be authorized by a second individual.

Eurotherm Data Reviewer FDA 21 CFR Part 11

11.300 Controls for identification codes / passwords	
Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:	
(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	User accounts are retired. All user names are forced to be unique.
(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g. to cover such events as password aging).	It is possible to force password expiry after a set number of days. If a user leaves, their account can be marked as retired.
(c) Following loss management procedures to electronically deauthorise lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.	Procedural. Compromised accounts can be disabled. On the loss of password, the administrator may set a new password for an account which the account holder should then immediately replace with a password of their own.
(d) Use of transaction safeguards to prevent unauthorised use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorised use to the system security unit, and, as appropriate, to organisational management.	It is possible to have logins time out after a set period of inactivity; to limit the number of login retries before an account is disabled; to set a minimum length for passwords; and to force password expiry after a set number of days. Unsuccessful logins that disable accounts are detailed in the audit trail within Eurotherm Data Reviewer.

Eurotherm

Faraday Close, Worthing,
West Sussex BN13 3PL
United Kingdom
Phone: +44 (0) 1903 268500
Fax: +44 (0) 1903 265982

www.eurotherm.com

Published April 2023

Document Number HA033530 Issue 2