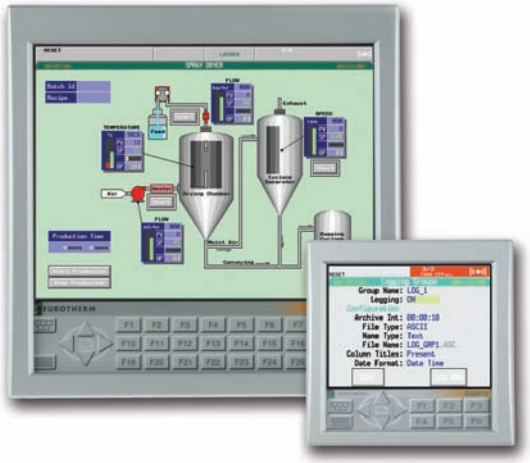
Eycon™ SERIES Visual Supervisor



Eycon™ Series Visual Supervisor and 21 CFR Part 11

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	Validation is clearly intended to be on a project basis. Eurotherm® has a long history of projects successfully validated to GAMP standards. Eurotherm offer assistance in validating products to GAMP guidelines. Log files which include logged process data, report data, and audit trail (alarms and events, operator notes, recipe actions, batch actions, etc) are in binary, compressed and checksumed format proprietary to Eurotherm. Details are not published. Invalid data records are rejected by Review. Review does not offer the facility to modify such records.
(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.	Complete and accurate copies of logged process data, report data, and embedded audit trail are available on screen or printed out through the use of the Review package. Complete and accurate electronic copies of logged process data, report data and embedded audit trail are available by copying the raw data files, by importing to Excel, 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 is Logged to removable media, via a USB port. Once removed archiving of files and backup strategy is the responsibility of the user.
(d) Limiting system access to authorized individuals.	User based security allows individuals to be granted access according to their authority level.

SUB PART B – ELECTRONIC RECORDS (continued)

11.10 Controls for closed systems (continued)	
(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.	Secure (embedded in the binary history file), computer generated, time-stamped runtime audit trail of batch stop/start, alarm acknowledgments, logins, recipe download, parameter changes. Record changes do not obscure previous data. Audit trail is embedded in the history file so guaranteeing retention alongside the records and availability for review / copying.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Sequencing of steps can be enforced via sequence function charts, operator messages/prompts and interlocks. The specifics are down to configuration.
(g) Use of authority checks to ensure that only 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.	Individual password protected user accounts. Each user account is allocated to a user group which determines the levels of authority within the system.
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	System errors and input channel status can be configured to be alarmed and logged automatically. Various methods to ensure a valid format of operator entered data are available.
(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 deter record and signature falsification.	Procedural
(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

11.30 Controls for open systems	Not Applicable
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 product is targeted at use in closed systems.

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; and **(3)** The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Signed records contain unique user ID, date and time, meaning. Meaning includes signed / authorised plus an operator entered note plus automatically generated action type (eg recipe download, alarm ack, message text responded to).
(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 (ID), timestamp and meaning are all embedded in the binary format history file.

SUB PART B – ELECTRONIC RECORDS (continued)

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, prints created via review for handwritten signature will always contain timestamp details which permit re-creation from the original data.

SUB PART C – ELECTRONIC SIGNATURES

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.	The product ensures that no two user accounts have the same username. Deleted user ID's cannot be re-created.
(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	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 control	
(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. **(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; and	Users can change their own passwords and no read access to 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.
(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 change their own passwords and no read access to passwords is provided. So, unless one user tells another their password, it is impossible to commit fraud without an audit trail of that fraud being left.
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Not applicable.

SUB PART C – ELECTRONIC SIGNATURES (continued)

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 names are forced to be unique provided that the retired accounts doesn't exceed the maximum.
(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 retired and the user ID will remain within the uniqueness checks.
(c) Following loss management procedures to electronically deauthorize 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 loss of password, the administrator may set a new password for an account which the account holder should then immediately replace by a password of their own.
(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational 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. Failed logins that disable accounts are detailed in the Audit Trail within the instrument.
(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.	Procedural