21 CFR Part 11 Compliance Table

EasyMatch® Essentials L2-ER and Vista L2

The world's true measure of color
HunterLab

Hunter Associates Laboratory
11491 Sunset Hills Road
Reston, Virginia 20190 USA
www.hunterlab.com

For Vista with Essentials 2025.3 and above

21 CFR Part 11 Compliance Table

Subpart	Requirement	Solution	Procedural or Technical?
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:		
(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Vista ER can be used as stand-alone instrument with the build-in android system. A system validation checklist, installation qualification (IQ) checklist, and operation qualification (OQ) checklist are provided with the system in the Validation and Compliance Notebook to assist you in validating your Vista. Performance qualification (PQ) advice, HunterLab's ISO 9001:2008 certificate (www.hunterlab.com/certifications.html)and HunterLab's software validation statement for Vista Essentials (see User's Manual) are also included as part of the system documentation. Vista Essentials-Electronic Records displays an error message when any job file is opened that has been tampered with from outside the software.	Procedural/ Technical
(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.	Permanent records are stored in Essentials database that can be viewed, printed and exported (to a flash drive) through Vista Essentials-Electronic Records. Exporting job to an .csv/.xlsx file and sending data out to any available ports are available software functions.	Technical
(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	The job files will be autosaved. And the user can backup the database to an external thumb drive. The period of backup will be established in company SOPs.	Procedural/Technical

Subpart	Requirement	Solution	Type
(d)	Limiting system access to authorized individuals.	Vista Essentials-Electronic Records limit access to authorized users with their correct passwords. The administrator must assign and maintain the user accounts.	Technical/ Procedural
(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 required for the subject electronic records and shall be available for agency review and copying.	Audit logs are maintained for each job and for the Vista Essentials-Electronic Records application. Users can view and expor tthe audit log to a flash drive. The system time can be synchronized with the network server. Record retention SOPs will be established using guidance given in the Validation and Compliance Notebook.	Technical/ Procedural
(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Vista Essentials-Electronic Records prompts for standardization at intervals set by the administrator/Lab Manager. Other sequencing requirements will be covered by company SOPs.	Technical/ Procedural
(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.	The User/Role information can be created and configured with Security Settings in Vista Essentials-ER. Functions available to each role is restricted as desired. Users have a unique login that Vista Essentials-ER enforces, and User ID is recorded with the measurement.	Technical
(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Vista Essentials-Electronic Records does not allow measurements if standardization is not successfully completed or has expired.	Technical
(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.	Training needs will be determined and undertaken by the user company. Training is available through HunterLab on a fee-paid basis.	Procedural
(j)	The establishment of, and adherence to, written policies that hold individuals accountable and	Policies will be written and maintained by each user company. Guidance is given in the Validation	Procedural

	responsible for actions initiated under their electronic signatures, to deter record and signature falsification.	and Compliance Notebook	
Subpart	**Requirement**	**Solution**	**Procedural or Technical?**
(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.	The Vista Essentials ER User's Manual is provided in Adobe Reader format on the thumb drive. These files may not be modified. Control and distribution of this manual, the Validation and Compliance Notebook, as well as company SOPs and maintenance records are the responsibility of the user company.	Procedural/ Technical
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 §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.	HunterLab is addressing closed systems only.	N/A
11.50	**Signature manifestations.**		
(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all 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	Electronic signatures are applied according to company SOPs and include the signer's name, the date and time of signing, and the purpose of the signature (e.g., creation, approval). Operators may electronically sign individual measurements only. Administrators and Lab Managers may electronically sign both	Technical /Procedural

	signature.	measurements and jobs. Once a job is electronically signed, no additional measurements can be added. Job e-signature details (user name, timestamp, and comments) will appear in the job PDF report.	
(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 export).	An electronic signature, once applied by signing a job file, is always available . It may not be altered or deleted.	Technical
Subpart	**Requirement**	**Solution**	**Procedural or Technical?**
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.	An electronic signature, once applied to a job file, is permanently linked to that job and may not be altered or deleted.	Technical
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.	Vista Essentials ER does not allow a single user name/password combination to be used more than once.	Technical
(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.	The user company will establish a SOP for identity verification using guidance given in the Validation and Compliance Notebook.	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	The user company will make this certification to FDA. A reminder and sample certificate are provided in your Validation and Compliance Notebook.	Procedural

	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.		
11.200	**Electronic signature components and controls.**		
Subpart	**Requirement**	**Solution**	**Type**
(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. 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. 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 the electronic signature components. (2) Be used only by their genuine owners; and (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.	Signing of a Vista Essentials-Electronic Records job file requires initial login to Vista Essentials plus entry of the ID and password on each signing. An auto log-off will be activated to eliminate the risks involved with walking away from the system. After log-off, user re-enters name/password to login to Vista Essentials ER. A user account will also be disabled if login fails more than a certain number of times.	Technical
(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by	HunterLab is not addressing biometric means of applying signatures now.	N/A

	anyone other than their genuine owners.		
Subpart	**Requirement**	**Solution**	**Type**
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.	Vista Essentials does not allow a single user name/password combination to be used more than once.	Technical
(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Following the instructions given in the Validation and Compliance Notebook, the operating system will be set up to require that a new password be entered at intervals chosen by the administrator.	Technical
(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 replacement using suitable, rigorous controls.	HunterLab is not addressing biometric means of applying signatures now. The user company will have a data backup procedure in place in case of catastrophic system failure. User IDs and passwords would likely be reassigned if a new software installation were required for recovery.	Procedural
(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.	In accordance with the Validation and Compliance Notebook, the system will lock a user account after a defined number of failed login attempts. An Administrator must then verify the user's identity and either unlock the account or create a new one before the user can regain access.	Technical/ Procedural
(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.	HunterLab is not addressing biometric means of applying signatures now.	N/A

Disclaimer

While HunterLab has attempted to consider all parts of the 21 CFR Part 11 rule (hereafter called “Part 11”) in developing its color measurement systems and the instructions and advice contained in this notebook, this system has not been approved or mandated by the United States Food and Drug Administration (FDA) or any other government agency. HunterLab makes no claims that completion of all steps described will disqualify companies or individuals from FDA sanction. Compliance responsibility lies with the user company, not HunterLab.