

Rule Number	Regulation	<i>ensur</i> Document Control Software
11.10a	Validation of systems to <i>ensure</i> accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	<p>Validation manuals are available from Mystic Management Systems to <i>ensure</i> the accuracy, reliability and consistent intended performance of each module in the system. It is the responsibility of the client to execute the Validation testing to assure compliance.</p> <p>Read-only content Audit Trails track the creation, modification, review, approval and deletion of records along with computer generated date and time stamps and user identification.</p> <p>In addition <i>ensur</i> prevents alteration of all content that has been Approved in the system.</p>
11.10b	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.	<i>Ensurr</i> provides electronic copies of documents in their native form and a PDF form suitable for inspection, review, and copying. <i>Ensurr</i> allows the export of document content and document meta data by users that have been granted the permission to do so.
11.10c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	<p><i>Ensurr</i> locks down content and meta data on all approved content in the system to prevent any alteration.</p> <p><i>Ensurr</i> content is fully indexed and provides extensive search and retrieval tools.</p> <p>All content and electronic records are retained throughout the retention period even when they have been marked as obsolete.</p>
11.10d	Limiting system access to authorized individuals.	<p>Access to the system is controlled by username and password login and each user's actions can be restricted by rights.</p> <p><i>ensurr</i> supports Windows and Active Directory authentication.</p> <p>Accounts will be locked after a configurable number of unsuccessful login attempts. These accounts must be unlocked by an <i>ensurr</i> system administrator to allow that account access to the system.</p> <p>Electronic Signatures are also required after logging into the system in order to check in content, or perform a review, approval, or rejection.</p>

Rule Number	Regulation	<i>ensur</i> Document Control Software
11.10e	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	<p>The <i>ensur</i> system uses database generated time-stamps, secure log in, and electronic signatures to create a comprehensive read-only audit trail.</p> <p>In addition, <i>ensur</i> maintains all content (native format and PDF format) and audit trails in its database throughout the life of the content.</p> <p>This audit trail information can be retrieved at any time for review.</p>
11.10f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	<p>Incorporated into <i>ensur</i> is a six phase, rules-based Life Cycle: Draft, Submitted for Approval, Approved, Current, Historic and Archived.</p> <p>Business rules prevent inappropriate actions in each phase of the lifecycle. The system also enforces dependency links among content. This forces supporting content to become current prior to the content which relies upon it. Change Order links allow a collection of content to proceed synchronously for review and approval.</p>
11.10g	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.	<p>Windows Domain or Active Directory authentication can be used to access the system. This authentication is utilized to verify each user's electronic signature once they have gained access to the system.</p> <p>Each user account can be controlled to limit which actions may be performed within the system. This includes importing and exporting content and data.</p> <p>PDF overlays are used to further control the security on specific content which can suppress printing, copying, and altering data.</p> <p>All alterations are recorded in a read-only audit trail with date-time stamps. Alterations are prohibited to content which has been approved.</p>
11.10h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	<i>ensur</i> challenges the user for their identity whenever data is altered or content status is modified. User rights are granted by group membership in accordance with organizational structure.
11.10i	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	<i>ensur</i> provides a training module that can capture all training that users have completed and preserves a read-only record of all completed training and assessments that have been rendered.

Rule Number	Regulation	<i>ensur</i> Document Control Software
11.10j	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.	<i>ensur</i> provides for users to record, via electronic signature, the fact that they have read and understood any policy or procedure stored in the <i>ensur</i> repository. Quizzes can be developed and managed within <i>ensur</i> to assess user comprehension.
11.10k	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.	All documentation can be automatically distributed in PDF format with security controls to prevent alteration, copy or printing of the content. Distribution is controlled by <i>ensur</i> group membership that prevents distribution to unauthorized individuals. Access to the system is strictly controlled by username and password authentication and by rights granted within the system. Revision and change control are built into the document lifecycle business rules and controlled by the security model in <i>ensur</i> . Each document maintains a full read-only, unalterable, time sequenced audit trail that records all actions taken on a given document.
11.50a	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.	<i>ensur</i> records the full name of the user at the moment each electronic signature is collected. This signature is also date-time stamped. The signature and date are written to the audit trail along with a human readable description of the action taken.
11.50b	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).	The user interface and printed reports all include the full name of the user, the date-time stamp, and an human readable description of the nature of each electronic record in a document's audit trail. The full audit trail of every document is available for printout in accordance with this requirement.
11.70	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 so as to falsify an electronic record by ordinary means.	The <i>ensur</i> system provides database linkages from each electronic signature to the respective documents and provides no means whatsoever to alter, erase, copy, or transfer these signatures and electronic records to other content for any purpose.

FDA 21 CFR Part 11



Rule Number	Regulation	<i>ensur</i> Document Control Software
11.100a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	<p>Each electronic signature in <i>ensur</i> is tied to an account that is a unique based on the combination of domain, and username. The system enforces that every username within a domain is unique.</p> <p>A unique user identifier is assigned by the database each time a user account is added to the <i>ensur</i> system. This guarantees the unique identification of every account. Once a user has taken any action in <i>ensur</i>, (for example, signing a document) that unique user record may never be deleted and will remain a permanent electronic record in the database. User accounts may be inactivated, but may never be reused by another individual.</p>
11.100b	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.	<p>This is primarily the responsibility of individuals within the company to establish via its standard operating policies and procedures.</p> <p><i>ensur</i> can record that personnel have read and understood the policies and procedures contained in <i>ensur</i>. <i>ensur</i> can even prevent such documents from becoming current until users tasked with marking the document as read and understood have done so within <i>ensur</i> by providing their electronic signature to signify they have read and understood the document.</p>
11.200a	<p>Electronic signatures that are not based upon biometrics shall:</p> <ol style="list-style-type: none"> (1) Employ at least two distinct identification components such as an identification code and password. (2) Be used only by their genuine owners; and (3) Be administered and executed to <i>ensure</i> that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals 	<p>The electronic signature implementation within <i>ensur</i> requires the user to provide two distinct identification components:</p> <ul style="list-style-type: none"> - Username - Password <p>The username is stored in the <i>ensur</i> system. The password is not stored in plain-text within <i>ensur</i>. It is stored using a one-way hashing algorithm. Reverse hashing the password is not possible, even with the involvement of technical support. Therefore, the password must be supplied by the genuine owner.</p>

Reference

U.S. Food and Drug Administration, "Part 11 - Electronic Records; Electronic Signatures (Final)".
http://www.fda.gov/ora/compliance_ref/Part11/FRs/background/pt11pxf.htm