US FDA 21 CFR Part 11 Support

ID7000™ software supports functions relevant to 21 CFR Part 11. The software in the following table refers to the ID7000 software.

Section	Requirement	Compliance
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:	
11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	The software is released following validation and verification testing conducted by Sony. IQ and OQ procedures and QC functions are available for system validation.
11.10(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.	The software provides both electronic and human-readable formats of the records (e.g., worksheets, reports, audit trails, user logs). Once exported outside the system, the user must take needed steps to ensure protection of data and records.
11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Records are secured within a hidden folder structure controlled by an indexing database. All records are retained until the user with appropriate privileges decides to delete records. Records that are exported from the software must be managed by the user according to prevailing policies and processes to ensure data protection.
11.10(d)	Limiting system access to authorized individuals.	The software requires a password for all users when logging in. Each user has a defined role, including access privileges. Users and their roles must be managed by administrators.
11.10(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.	The software automatically generates a secure, computer-generated, time-stamped audit trail of all user actions that affect the record. Once turned on, users cannot modify, deactivate, or delete the audit trail. The audit trail is maintained with the record through the lifetime of said record.
11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	The device restricts what users can do based on the state of the system and the permissions associated with the account which is logged in.
11.10(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 software is accessed using a valid username and password. Based on the role and privileges associated with the account, the software provides users with the authority to carry out particular functions. These privileges include tasks such as electronic signature application to a record, deletion of a record, or export of records.

Section	Requirement	Compliance
11.10(h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	The software has been designed to require specific inputs for given fields of information—and it includes error messaging capability that informs the user when invalid information is input into a software field. The software also confirms the validity of the record by attaching a checksum value to the record when it is exported. Before a record can be imported, the software checks the value and restricts the import if the value has changed since export.
11.10(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.	Sony can provide user training and documentation for operation of the system and software. It is the responsibility of the user's organization to ensure training of staff and provide needed information on the record/ electronic signature operating procedure based on their own policies and procedures.
11.10(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.	This is the responsibility of the user's organization. Written policies and procedures should be defined that outline the importance of electronic signatures with respect to individual responsibility and the consequences of tampering for both the company and the individual.
11.10(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 software has a built-in help function that displays user manuals and is available to all users. The user manuals incorporated in the help function will be updated appropriately with system software updates. All updates are made available to end users to ensure optimal system operation through the field support organization.
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.	The software is designed to operate as a closed system and therefore this does not apply.
11.50	**Signature Manifestations**	
11.50(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.	All signed records (electronic and human readable forms) within the software contain the username of the signer, the date and time of the signing and the authorship.
11.50(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).	

Section	Requirement	Compliance
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.	Records are created in PDF format, and electronic signatures are applied via PDF functionality. The PDF function ensures that electronic signatures cannot be reused.
11.100	**General Requirements**	
11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	The software ensures that every combination of username and password is unique to the user. If the username is disabled, it cannot be reused for other users. It is the responsibility of the user's organization to verify the identity of all users who use the software.
11.100(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.	This is the responsibility of the user's organization.
11.100(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.	This is the responsibility of the user's organization.
11.200	**Electronic Signature Components and Controls**	
11.200(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. (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.	A software requires a unique username and password to apply an electronic signature. Both components are necessary for each signing, separately from login.
11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	The software does not support biometric signatures.

Section	Requirement	Compliance
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:	
11.300(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.	No two individuals can have the same combination of username and password. The combinations of username and password must be unique.
11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Passwords are set to expire when they are first created or reset. The password expiration can be set by the administrator.
11.300(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.	Administrators can delete accounts or change compromised passwords as needed. The user must reset their password on the first login after the change to ensure that the administrator does not own the password.
11.300(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.	After a specified number of consecutive failed login attempts, the software locks out the problematic user. The specified number of attempts can be set by the administrator to suit the operation of the user's organization.
11.300(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.	Periodic checks are the responsibility of the user. Administrators are encouraged to periodically check for access restrictions and unauthorized data manipulation.

9.13.120122.0