Date	17 Aug 2016	Service Note #	OPT-DISS-3007	Updated	NA
Product	Opt-Diss Software		Created By	J. Yangco	
Description	Opt-Diss Software Compliance with 21 CFR Part 11 Requirements				

Release	☒	Internal	☒	Distributors	☒	Customers

Parts Required	Serial Numbers Affected
None	All

Software Compliance with 21 CFR Part 11

The following table describes Opt-Diss software functionality and services that support customer deployment of the system to meet applicable requirements of Federal Regulations 21 CFR Part 11 for a closed system used to store electronic records. The customer is responsible for providing any written procedural controls, beyond the scope of vendor responsibilities, required for full 21 CFR Part 11 compliance. These procedural controls must address system and documentation changes for customer prepared documents, user and administrator training, physical and software security, system data backup and archiving, and the management of user identification codes and passwords.

21 CFR Part 11 Requirement:	Opt-Diss Functionality and Services:
Subpart B -- Electronic Records	
§ 11.10 (a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Internal validation and validations conducted at customer sites have demonstrated that system performance is accurate, reliable, and consistent and that the system recognizes and refuses to open data files edited from an external application. Validation consists of the following activities: Distek-conducted hardware and software validation testing; On-site hardware IQ/OQ, software IQ, on-site system OQ/PQ or UAT (User Acceptance Testing). Hardware IQ/OQ and software IQ are performed by a Distek Trained Validation Specialist. The system OQ/PQ testing protocol may be purchased and executed by the customer or the customer may contract with Distek to have the protocol executed on-site by a Distek Trained Validation Specialist.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

§ 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.	Opt-Diss provides the means for opening record files and viewing raw data, calculated results, and metadata (audit trail event log, instrument settings, run conditions, and sample and standard information). Reports can be printed that contain the identical items and values viewed on the workstation screen. To ensure that data and corresponding metadata are inexorably linked, metadata are saved in the same file as the corresponding raw data. To ensure that printed reports accurately reflect their corresponding record contents, the system automatically saves files containing unsaved changes when a report for that file is printed.
§ 11.10 (c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Opt-Diss records are saved in user-defined categories within an administratively-defined data folder that can reside on a secured network file server. Once the Opt-Diss data folder is defined by the administrator, records cannot be saved to other locations. Outside of the Opt-Diss program, users have "Read Only" privileges for the data folder and do not have change privileges. The customer is responsible for ensuring that the data folder security settings are maintained as described in the Opt-Diss Installation Guide, and that the data folder contents are backed up and archived to ensure protection throughout the retention period.
§ 11.10 (d) Limiting system access to authorized individuals.	Opt-Diss security is integrated with the Windows Operating System. To gain access to the Opt-Diss workstation, users must be authenticated through the operating system. To access the Opt-Diss application, logged-on users must be members of one of the Opt-Diss Groups configured and populated by an operating system administrator. Logged-on users are forced to re-enter their ID/password after 5 minutes of inactivity. Outside of the Opt-Diss program, users have "Read Only" privileges for the administratively defined data folder and do not have change privileges.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

§ 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.	Changes to records are audited and maintained in an audit trail event log stored in the data file which contains the raw data and metadata for a dissolution run. Each entry includes the local date/time of the action, the ID of the logged-on user, a description of the action, the original value of the changed record, and the new value of the record. For each change event, the audit trail event log records the previous record value and the new value. The system does not allow audit trail information to be deleted. The information can only be viewed and printed. The customer is responsible for ensuring that the data folder security settings are maintained as described in the Opt-Diss Installation Guide, and that records within the folder are secured, backed up, and archived to ensure protection throughout the retention period.
§ 11.10 (f) Use of operational checks to enforce permitted sequencing of steps and events, as appropriate.	There are no system events or processing steps that require external approval/sign-off before proceeding to another step. Thus this requirement may not be applicable. The system performs checks to ensure that open files with unsaved changes cannot be inadvertently closed without saving the changes, that calibration events are performed in sequence, and that percent dissolved results are not calculated until a sample reference blank and standards data have been acquired.
§ 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.	Workstation access and application use are restricted to authorized accounts managed by a system administrator. Access to specific functions within the application can be further restricted by administrative assignment of authorized workstation users to one of the four Opt-Diss Groups (Administrators, Developer, Operator, and Reviewer).

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

§ 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.	This is not applicable. The Opt-Diss system consists of a single computer directly connected to a single instrument.
§ 11.10 (i) Determination that persons who develop, maintain, or use electronic record/signature systems have the education, training, and experience to perform their assigned tasks.	Training records are available for Opt-Diss system developers. The customer is responsible for maintaining training records for system users.
§ 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.	The customer is responsible for establishing procedural controls governing assignment and use of electronic signatures.
§ 11.10 (k) Use of appropriate controls over systems documentation. (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 document time-sequenced development and modifications of system documentation.	(1) The customer is responsible for establishing procedural controls governing distribution, access, and use of Opt-Diss system operation and maintenance documentation held at their sites. Distek, Inc. includes, with each installed system, a user manual, installation guide, hardware IQ/OQ protocols, a software IQ protocol, and optionally a system OQ/PQ or UAT protocol. The hardware OQ protocol can be used as a periodic performance verification or calibration procedure. (2) The customer is responsible for establishing procedural controls governing their in-house development of Opt-Diss system documentation. Distek, Inc. maintains each version of any system document pertaining to Opt-Diss development.
§ 11.30 Controls for open systems.	Should Opt-Diss be deployed as an open system, the customer is responsible for establishing procedures and controls to address these requirements.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

§ 11.50 Signature manifestation. (1) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (a) The printed name of the signer; (b) The date and time when the signature was executed; (c) The meaning (such as review, approval, responsibility, or authorship) associated with the signature. (2) The items identified in paragraphs (1)(a), (1)(b), and (1)(c) 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).	(1) For all signings Opt-Diss automatically includes the date and time of a signing and the logged on user's ID which is uniquely associated with the signer's printed name. For signing events ("ready for review", "review", and "approval") other than parameter changes, the signer must enter the meaning of the signature into the data file Note field. (2) Signing events are logged in the associated data file audit trail event log which can be viewed and printed. See responses for § 11.10 (e) (Audit Trails).
§ 11.70 Signature/record linking. Electronic signatures and handwritten signatures 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.	Opt-Diss electronic signatures are embedded into the record data files to which they apply and cannot be copied, excised, or transferred by ordinary means.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

21 CFR Part 11 Requirement:	Opt-Diss Functionality and Services:
Subpart C -- Electronic Signatures	
§ 11.100 General Requirements.	The customer is responsible for meeting the General Requirements which address electronic signature uniqueness, verification of users' identities, and certification of the customer's intent to use electronic signatures as the legally binding equivalent of handwritten signatures.
§ 11.200 Electronic signature components and controls. (1) Electronic signatures that are not based upon biometrics shall: (a) 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. (b) Be used only by their genuine owners; and (c) Be administrated and executed to ensure that attempted use of an individual's electronic signature by anyone other than its	(1)(a) Opt-Diss employs a non-biometric electronic signature consisting of a user ID (identification code) and a password. (1)(a)(i) Opt-Diss requires potential signers who are not the logged-on workstation user to logon to the workstation and the Opt-Diss application. The logged-on user is required to re-enter their password signature component for all change and signing events. (1)(b) and (c) The customer is responsible for ensuring that users adhere to procedural controls that govern management of workstation accounts, password assignment, ID/password usage, and password confidentiality.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835

genuine owner requires collaboration of two or more individuals.	
§ 11.300 Controls for identification codes/passwords.	The customer is responsible for establishing controls to ensure the security and integrity of identification code and password combinations.

121 North Center Drive
North Brunswick, NJ 08902 USA
P: 732-422-7585 F: 732-422-7310 TOLL FREE: 888-234-7835