Compliance Matrix for 21 CFR Part 11: Electronic Records

S3500 / Bluewave / SYNC / Nanotrac

General

This document explains how Microtrac FLEX software has been designed to satisfy and comply with regulations in 21 CFR Part 11 for electronic records and electronic signatures.

As part of the Title 21 covering Food and Drugs of the Code of Federal Regulations, Part 11, the United States Food and Drug Administration provides guidelines that describe requirements for transmitting and accepting electronic records and signatures. These regulations became effective on August 20, 1997 and must be followed by all companies that use electronic record keeping system and are regulated by the USFDA.

The guideline is an outgrowth of discussion between representatives of the FDA and pharmaceutical industry to create paperless records. Of special concern was the integrity and reliability of paperless records while assuring that they were equivalent to paper or hard-copy records. The primary purpose was to eliminate or prevent fraudulent signing of the records. Microtrac FLEX software addresses these issues as compiled by the USFDA in 21 CFR Part 11. The following provides information on the security of data obtained and stored on Microtrac instruments using FLEX software and subsequent compliance to 21 CFR Part 11 Electronic Signatures.

Definitions of 21 CFR Part 11

Electronic record: Any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained archived, retrieved, or distributed by a computer.

Electronic signature: A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

Handwritten signature: The scripted name or legal mark of an individual handwritten by the individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of writing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

Digital signature: An electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

Biometrics: A method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and /or actions are both unique to that individual and measurable.

Closed system: An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Open system: An environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B – Electronic Records

Subpart B – Electronic Records		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.10 **Closed Systems**	Persons who employ closed systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity … of electronic records.	**YES:** Microtrac operates as a closed system. Microtrac provides software that allows activation of security features to protect data records and to ensure authenticity and integrity of electronic records.
11.10 (a)	Validation of systems to ensure accuracy, reliability consistent intended performance and the ability to discern invalid or altered records	**YES:** As part of Microtrac validation service, software security features are verified. When FLEX software is enabled, stored data cannot be altered even if security system is disabled. Alterations of stored data can only be saved as a new record for which as audit trail is provided to track alterations.
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	**YES:** Data records and history can be viewed, printed and displayed
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period	**YES:** Data records are saved to an encrypted and password protected database that can be located locally or on a user computer network. Client shall implement computer and file backup and archiving procedures to provide a second layer protection of data throughout retention period. Original data records cannot be overwritten. Modifications are saved as new records with audit trail. No application other than Microtrac FLEX can open or view data records.
11.10 (d)	Protection of records to enable their accurate and ready retrieval throughout the records retention period	**YES:** Client is responsible for establishing usernames, passwords, authorizations and privileges. Operator's manual describes procedure. Once the security system is enabled by the client, it controls access to the software

Subpart B – Electronic Records		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.10 (e)	Use secure computer-generated, time-stamped audit trails to independently record the date and time of operator entries and action that create, modify or delete electronics 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.	**YES:** FLEX software automatically records all measurement parameters, time, date. Original data cannot be overwritten. New calculation of saved data must be saved as a new audit-trailed record. Audit trail information report is automatically generated from FLEX software upon user request. Audit Trail reports the date and user identification of all changes made to parameters that would affect measurement results.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	**YES:** Microtrac FLEX provides an "Auto-Sequence" option. Activation of this option along with SOP can be used to specify steps of measurement. Administrators can restrict access to the setup parameters that define an Auto-Sequence via the FLEX security system. Administrators can also enforce setzero (background) measurements prior to all manually performed data collections via the FLEX security system.
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.	**YES:** Two administrators are required for establishing access criteria, passwords and user names. Log-in failures include lock-out of user accounts and/or software application. Only designated administrators can unlock the software. Reasons for a lockout are provided by the security system to the administrator. Automatic lock-out from software occurs after an administrator-defined non-use period. Access is controlled user authentication (User Id and Password). Unique combinations of user id and passwords are enforced by the FLEX security system. Passwords can be set to expire after a period of time defined by a FLEX security system administrator.

Subpart B – Electronic Records		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of data input or operational instruction.	**YES:** Client can perform periodic checks with traceable standards. Microtrac trained service personnel are available for verification and/or validation evaluation.
11.10 (i)	Determination that persons who develop, maintain, use electronic record/electronic signature systems have education, training and experience to perform their assigned tasks.	**YES:** Client is responsible for SOPs to comply with this control. Microtrac provides in-house and other courses for instrument operation training. The Microtrac FLEX security manual provides all information needed by designated client administrators to setup the FLEX security system.
11.10 (j)	The establishment of and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronics signatures, in order to deter record and signature falsification.	**Not applicable:** Client must establish SOPs and other written policies to deter falsification or fraudulent uses.
11.10 (k1)	Use of appropriate controls over systems documentation including adequate controls over the distribution of, access to and use of documentation for system operation and maintenance.	**YES:** Software is supplied with on-line and printed manuals that can be used to establish SOPs. It is the responsibility of client to control system documentation and procedures.
11.10 (k2)	Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	**YES:** Software contains version information that can be incorporated into the client's documentation.
11.30 **Open Systems**	Persons who employ open systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity… of electronic records from the point of their control to the point of their receipt. Such procedures and controls shall include those identified in 11.10 . . . and use appropriate digital signature standards to ensure . . . record authenticity, integrity and confidentiality.	**Not Applicable:** Microtrac FLEX is a **"Closed" System**. Microtrac FLEX electronic data records **cannot** be viewed or altered by any other application program than Microtrac FLEX.

Subpart B – Electronic Records		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: Printed name of signer; Date and time when signature was executed; and the meaning (such as review, approval, responsibility or authorship) associated with the signature.	**YES:** Microtrac FLEX software allows configuration using two administrations who are responsible for establishing these criteria. Operation manual provides directions. The Microtrac FLEX security system provides for enforcement of Electronic Signatures to all data records and data altering operations. Microtrac FLEX Electronic Signatures consist of an enforced unique Password and PID (Personal ID code) for signing. Provision is also made for an approver electronic signature to be attached to each electronic record.
11.50 (b)	(b) The items identified in 11.50 (a) 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 display or printout)	**YES:** Digital signatures are embedded within the electronic record and is included as part of the human-readable, on-screen and printed forms of the electronic record.
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 be transferred to falsify an electronic record by ordinary means.	**YES:** Digital signature is stored with each data record that is signed. Microtrac data records that are stored while the Microtrac security system is active cannot be altered.

Subpart C – Electronic Signatures

Subpart C – Electronic Signatures		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.100 **General requirements for electronic signatures**	(a) Each electronic signature shall be unique to one individual and shall not be reused, or reassigned to anyone else (b) Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such signature the organization shall verify the identity of the individual. (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	**YES:** It is required by client to establish a unique user name and password and privileges in Microtrac FLEX software. The Microtrac FLEX security system setup procedure enforces unique user ID and password combinations. Client is responsible to comply with Parts (b) and (c).
11.200 (a1) **Electronic signature components and controls**	a) Electronic signatures 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.	1) **YES:** The Microtrac FLEX security system setup procedure enforces unique user ID, password and user PID (personal ID code) combinations for each user account. An electronic signature in Microtrac FLEX consists of the user ID and Password when signing and the user ID and PID when displayed with the associated data record. i) **YES** ii) **YES**
11.200 (a2)	2) Be used only by their genuine owner	**Not applicable:** Client is responsible for training, establishing SOPs and other written policies to deter falsification or fraudulent uses to comply with this control

Subpart C – Electronic Signatures		
Section Number 21 CFR Part 11	**Text from 21 CFR Part 11**	**Microtrac Flex Software Implementation**
11.200 (a3)	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.	**Not applicable:** Client is responsible for training, establishing SOPs and other written policies to deter falsification or fraudulent uses to comply with this control.
11.200 (b)	b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used anyone other than their genuine owners.	**Not applicable**
11.300 (a) **Controls for identification codes/passwords**	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.	**YES:** FLEX software does not allow duplicate user names and/or passwords.
11.300 (b)	b) Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g., to cover events as password aging)	**YES:** User passwords can be set to expire after a defined period of time.
11.300 (c)	c) Following loss management procedures to electronically de-authorize 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.	**Not applicable**
11.300 (d)	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.	**YES:** Unsuccessful attempts to login with a user account will cause the account to lock-out until intervention by administrator.
11.300 (e)	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.	**Not applicable**

For further information please contact us at:

www.microtrac.com