



---

## Support for 21 CFR part 11 Compliance

21 CFR part 11, titled “Electronic Records and Electronic Signatures,” went into effect August 20, 1997 to enable state-of-the-art technology to be used in accordance with existing regulations; namely, to prevent falsification, abuse or inadvertent corruption of electronic data and electronic signatures.

21 CFR part 11 sets forth the requirements that computerized systems must fulfill to allow electronic signatures and records in lieu of handwritten signatures on paper records. Full 21 CFR part 11 compliance requires both administrative/procedural controls as well as technical/system controls. Thus, full compliance goes beyond the capability of a single technology or software package; however, component technologies should be conducive to 21 CFR part 11 compliance. As a brief overview, 21 CFR part 11 describes general requirements pertaining to:

- Computerized system validation, where a computerized system encompasses both hardware and software
- Users, policies and procedures applying to such a system
- Controlled access to the computerized system
- Audit trails for all records/signatures
- Use of electronic signatures for authentication of electronic documents
- Proper storage of electronic records

The sections that follow provide a summary of the relevant sections of 21 CFR part 11, and Ahura Scientific’s interpretation of and solutions addressing these core requirements for TruScan.

### *Requirements Assessment*

**Definition: § 11.3 (4)** *Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*

- ✓ **TruScan Capability:** In order to use the TruScan system, users must first be granted a user profile with appropriate administrative access as determined by the system administrator. As such, Ahura Scientific’s understanding is that the TruScan device is a closed system under this definition.

**Requirement: § 11.10 (a)** *Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*

- ✓ **TruScan Capability:** Ahura Scientific’s understanding is that validation encompasses a structured and documented plan of system adoption and implementation containing, but extending well beyond the TruScan system itself. Ahura Scientific’s services include documentation to support and assist with Installation and Operational Qualification.

**Requirement: § 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.*

- ✓ **TruScan Capability:** TruScan generates self-describing and self-contained electronic records which include all data and security features necessary to demonstrate compliance. These records are available in a number of human-readable formats including ASCII, PDF, JPEG and SPC (open binary standard spectroscopy format).

**Requirement: § 11.10 (c)** *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*

- ✓ **TruScan Capability:** TruScan records can not be altered on the device when generated at run-time. TruScan is a transient device meaning that it is not intended for permanent on-board storage of electronic records, and has no capacity to do so. Completed electronic records are delivered to a secure location (designated by the system administrator in the device configuration) via a TCP/IP 'sync' process which relies on the secure asset delivery features of TCP.

**Requirement: § 11.10 (d)** *Limiting system access to authorized individuals.*

- ✓ **TruScan Capability:** As discussed above, user profiles must be granted by the system administrator before access to the TruScan system can be accomplished. User access is restricted by usernames and passwords on the device itself. Pertinent administrative/procedural controls should also be in place to restrict physical access to the system when not in use. Administrators can manage user profiles, reset passwords, and execute other access restriction elements via the TruScan WebAdmin tools.

**Requirement: § 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.*

- ✓ **TruScan Capability:** TruScan automatically generates audit trails containing all referenced information. Audit trails are delivered to a secure location (identified by the system administrator in the device configuration) for permanent storage. Electronic records can not be changed once created.

**Requirement: § 11.10 (f)** *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.*

- ✓ **TruScan Capability:** TruScan has a strictly enforced workflow and will not allow operation outside of the permitted sequencing of steps. For a detailed description of the permitted workflow, please see the TruScan user manual.

**Requirement: § 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.*

- ✓ **TruScan Capability:** TruScan has three authority levels: user, developer, and administrator. The user level for each user profile is set by the system administrator during creation of the corresponding user profile.

**Requirement: § 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.*

- ✓ **TruScan Capability:** TruScan records the data input in the electronic record; the validity of that input should be procedurally assured by external measures.

**Requirement: § 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.*

- ✓ **TruScan Capability:** Enforcement of this requirement should be assured through appropriate administrative control of user system access; however, Ahura Scientific offers documented TruScan training for all user levels including system administrators, developers and users.

**Requirement: § 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.*

- ✓ **TruScan Capability:** The establishment and adherence to such policies should be assured by external measures.

**Requirement: § 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.*

- ✓ **TruScan Capability:** The establishment and adherence to such controls should be assured by external measures. TruScan maintains a system configuration audit trail that documents changes made to the system configuration by developers and administrators.

**Requirement: § 11.30** *Controls for open systems.*

- ✓ **TruScan Capability:** As discussed above (**§ 11.3 (4)**), TruScan is a closed system. As such, controls for open systems do not apply.

**Requirement: § 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.*

- ✓ **TruScan Capability:** The electronic records generated by TruScan contain the specified information.

**Requirement: § 11.50 (b)** *The items identified in (§ 11.50 (a)) 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).*

- ✓ **TruScan Capability:** TruScan maintains signature manifestations as described in **§ 11.50 (a)** in the same fashion as for electronic records. Additionally, all signature information is included in human-readable forms of the electronic record.

**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 to falsify an electronic record by ordinary means.*

- ✓ **TruScan Capability:** TruScan's electronic signatures are embedded in the electronic record, and can not be excised or copied.

**Requirement: § 11.100 (a)** *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.*

- ✓ **TruScan Capability:** TruScan does not allow duplicate usernames to be in use on the same device. User accounts can be disabled or deleted from the system (an action which is audited in the system logs), and external documentation and policies should be used to ensure that the same username is not later assigned to a different individual.

**Requirement: § 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.*

- ✓ **TruScan Capability:** The establishment and adherence to such controls should be assured by external measures.

**Requirement: § 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 legally binding equivalent of traditional handwritten signatures*

- ✓ **TruScan Capability:** The establishment and adherence to such controls should be assured by external measures.

**Requirement: § 11.200 (a)(1) (a)(1)(i)** *Electronic signatures that are not based upon biometrics shall (1) employ at least two distinct ID component such as 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*

- ✓ **TruScan Capability:** TruScan requires a username and password as ID components for the initial system logon. {We then derive electronic signatures for all tests within a session according to 21 CFR 211.194(a)(7)}

**Requirement: § 11.200 (a)(1)(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.*

- ✓ **TruScan Capability:** As described above, TruScan requires a username and password for the initial system logon. Additionally, timeouts based on system inactivity (frequency of which are set by the system administrator) are used to logoff users that have not accessed the system for a continuous period of time. In order to create new electronic signatures after automatic logoff, the user must log back on with all electronic signature components (username and password).

**Requirement: § 11.200 (a)(2-3)** *Electronic signatures that are not based upon biometrics shall be used only by their genuine owners. Electronic signatures that are not based upon biometrics shall be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than it's genuine owner requires collaboration of two or more individuals.*

- ✓ **TruScan Capability:** TruScan allows electronic signatures for a user to be generated though only a single username and password combination. System access is restricted unless an appropriate username/password combination is selected. Should a user forget their password, the system administrator can re-set it for them.

**Requirement: § 11.200 (b)** *Electronic signatures based on biometrics shall be designed to ensure that they can not be used by anyone other than their genuine owners.*

- ✓ **TruScan Capability:** TruScan does not use electronic signatures based on biometrics.

**Requirement: § 11.300** *Persons who use electronic signatures based upon the 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. b) Ensuring that identification and password issuances are periodically checked, recalled, or revised. 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. 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. 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.*

- ✓ **TruScan Capability:** a) TruScan does not allow duplicate usernames (identification code) for different individuals. b,d-e) The establishment and adherence to such controls should be assured by external measures. c) The system administrator has the ability to deactivate user profiles as necessary. d) TruScan records failed login attempts in the audit logs, and if the number of failed login attempts exceeds the administratively set limit, the user account will be locked pending release by an administrator. e) TruScan has no reliance on tokens or cards.



---

Ahura Scientific, Inc.  
46 Jonspin Road  
Wilmington, MA 01887  
+1 978 657 5555 voice  
+1 978 657 5821 fax  
truscan@ahurascientific.com