Setra CEMS™ Software
Electronic Records and Signatures
Compliance Statement

Support of compliance with FDA 21 CFR Part 11

Document #	SS-CEMS-ElectronicCompliance-Rev B
Created By	Samantha S
Reviewed By	Patrick M

Setra Systems, Inc

159 Swanson Road, Boxborough, MA 01719
800.257.3872 • www.setra.com

1 Content

This document describes how the requirements of 21 CFR Part 11 can be satisfied by Setra's Continuous Environment Monitoring System ("CEMS") and the appropriate organizational measures to ensure that the system users operate the system in conformance with the regulation.

2 Terminology

2.1 Electronic Records

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 system.

2.2 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.

2.3 Closed System

A closed system is an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

2.4 Open System

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

2.5 Handwritten Signature

The scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing 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.

3 Why 21 CFR Part 11

The 21 code of Federal Regulations (CFR) Part 11 was implemented in 1997 to let the FDA accept electronic records and signatures in place of paper records and handwritten signatures for compliance. The regulation outlines controls for ensuring that electronic records and signatures are trustworthy, reliable, and compatible with FDA procedures and are as verifiable and traceable as their paper counterparts.

3.1 The 21 CFR Part 11 Regulation

The 21 Code of Federal Regulations (CFR), Part 11 title contains the legal regulations of the FDA (US authority for supervising food and medicinal products) concerning the use of

electronic records and electronic signatures. Definitions for the electronic record and electronic signature terms are contained in sections 11.3 (6) and (7) of the regulation.

3.2 Purpose of the regulation

Part 11 was originally issued on July 21, 1992 as preannouncement of a draft law. The purpose of this initiative was to accelerate the approval process for medicinal products. However, the other consequences, namely the acceptance of both information and signatures for the approval in electronic form, were apparent immediately. After six years of cooperation between various authorities and the pharmaceutical industry, the final regulation took effect on August 20, 1997.

3.3 Content of the regulation

Part 11 specifies the legal prerequisites under which electronic records and signatures are accepted as being equivalent to records on paper and handwritten signatures. Part 11 assumes that the danger of manipulation and non-traceable changes to electronic records and signatures is greater than for paper form and additional measures must be adopted.

4 CEMS Conformance with 21 CFR Part 11

The following table maps the requirements identified with the regulation to CEMS capabilities.

21 CFR PART 11 Requirement	Setra CEMS™ Software Capabilities
§11.10.a Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Validation of CEMS is the responsibility of customers. Setra can assist in the process, in the form of IQ/OQ protocols. CEMS database is password protected and not accessible by end users, hence it's not possible to alter records stored in CEMS. CEMS provides an audit trail for updates to records which have been created or modified providing visibility to all data changes.
§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	Standard reports are available for the output of the recorded data and the associated meta data (e.g., record audit trail). These reports can be printed to paper form or exported to both computer and human consumable formats (such as PDF, Excel, CSV, or Word).

and copying of the electronic records.	
§11.10.c Protection of records to enable their accurate and ready retrieval throughout the records retention period.	CEMS data is protected during its retention period in a secure database with controlled access. Data can be retrieved only through CEMS web portal and only by authorized users. Data can be exported in readable form and may also be exported in industry standard formats.
§11.10.d Limiting system access to authorized individuals.	Access to CEMS is through unique username and passwords. Accounts are administered with the user management functions in CEMS. Customers are expected to assign access according to their own procedures and practices.
§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.	CEMS generates an audit trail for every user action with information such as - date/time, username and action performed. Audit trails cannot be altered or deleted. Actions can be annotated at the time the action is performed and this annotation is included in the audit trail.
§11.10.f Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Modification of electronic records cannot be performed under any circumstances or sequence of actions taken by the user.

§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.	User credentials control which users can access the system to perform tasks. Alterations of records are not permitted by any user.
§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.	SetraEDGE is pre-programmed with a unique key, which ensures that only valid devices can communicate with CEMS. Additionally, communication between SetraEDGE and CEMS is encrypted by means of TLS V1.2
§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.	The CEMS customer is responsible for ensuring that their employees and other authorized users of the system have the necessary training & education. Setra will provide initial training to the end user.
§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 CEMS customer is responsible for the organization and the provision of appropriate quality procedures.
§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.	The CEMS customer is responsible for the organization and the provision of appropriate quality procedures.
2. Revision and change control procedures to maintain an audit trail that documents time- sequenced development and modification of systems documentation.	The CEMS customer is responsible for the organization and the provision of appropriate quality procedures.

§11.30 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.	Customer Data is encrypted at rest through storage level encryptions in all hosting locations, and within the application context for the mobile client. Data in transit is protected with industry-recognized TLS protocols (HTTPS or MQTT)
§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;	The name of the signing person identified within the systems user management must be unambiguous and in plain language. CEMS maintains the system-authenticated and time- stamped details of each electronic signature in the audit trail, including the user's full name as entered into the system by the CEMS customer.
2. The date and time when the signature was executed;	All signatures are stored with the date and time the signature was executed. CEMS maintains the system-authenticated and time- stamped details of each electronic signature in the audit trail.

3. The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The signee can enter the meaning of the signature either via comment or selecting a meaning from a list of choices.
§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).	All signature information in the system can be dis- played or printed appropriately.
§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.	The name and checksum of the generated file are listed in the audit trail. The user can upload a report which was generated from the system and check for falsification/ manipulation. Upon validation, a message is displayed indicating the success or failure of that action.
§11.100.a Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	This is guaranteed using system-internal unique user IDs. A user ID can occur only once in CEMS.
§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.	The CEMS customer is responsible for the organization and the provision of appropriate quality procedures that confirm the identity of individuals prior to granting system access.
§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	The CEMS customer is responsible for the organization and the provision of appropriate quality procedures.

equivalent of traditional handwritten signatures.	
§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.	CEMS electronic signatures consist of a user ID and the associated password.
1.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.	The initial signing is based on the user id and password; subsequent signings during that session require entering the user password to ensure the signee is the authorized user. There is an automatic logout after a period of inactivity after which the user is required to login using their credentials and executing the subsequent signature after this period.
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.	CEMS electronic signatures always consist of a user ID and the associated password. The user logged on to a session will be entered as default user for the electronic signature and only needs to enter their password at the time of signing. A user that is not logged in must login using their user credentials in order to sign.
2. Be used only by their genuine users	The CEMS customer is responsible for the organization and the provision of appropriate quality procedures that confirm the identity of individuals prior to granting system access.
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	The electronic signature entries in the system are protected cryptographically and cannot be forged.

or more individuals.	Passwords can only be changed by the user or reset by an authorized person. Attempts made to login with invalid credentials are logged in audit trail.
§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.	CEMS does not offer any electronic signatures based on biometric characteristics in the system.
§11.300 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.	CEMS login is based on a unique username, which would ensure two individuals don't have same credentials. A username can occur only once.
§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).	User passwords expire every 90 days. Passwords are enforced to contain a minimum of 1 upper case, 1 lower case, 1 numeric and 1 special character.
§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	The CEMS customer is responsible for the organization and the provision of appropriate employee identity management procedures. CEMS provides the ability to disable user accounts and reset user passwords by the user and/or an authorized administrator user.

or permanent replacements using suitable, rigorous controls.	
§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.	Users are required to change their passwords after 90 days. Unauthorized login attempts are logged in the audit trail. If the number of failed logins exceeds the predefined number of failed logins, the user credentials are locked out until re-enabled by an authorized administrator user.
§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.	The CEMS customer is responsible for the organization and the provision of appropriate employee identity management procedures.