zenon
by COPA-DATA

zenon in regulated industries

FDA 21 CFR part 11

www.COPA-DATA.com
pharmaceutical@COPA-DATA.com

Content

Revision History

Rev.	Date	Author	Description
1.0	Jan-2000		First issue
2.0	Jan-2006	Markus Helbok	Review zenon 6.20
3.0	Jan-2012	Robert Harrison	Review zenon 7.0
4.0	Mar-2020	Giuseppe Menin	Review zenon 8.20 and Analyzer 3.40
5.0	Oct-2022	Giuseppe Menin	Review zenon software platform 11
6.0	June-2023	Bernhard Korten	Review zenon software platform 12

1. Executive summary

The Part 11 regulation concerns all electronic records that are created, modified, maintained, archived, retrieved or distributed for regulatory purposes. It establishes the criteria for the use of electronic records and signatures, under which they will be considered equivalent to conventional paper records and handwritten signatures.

COPA-DATA and its zenon Software Platform provide solutions that ensure compliance in FDA-regulated environments. A strict internal company quality management system provides development procedures that ensure high-quality and reliable products. We aim to provide solutions which adhere to the Part 11 regulation and also provide the most efficient platform to develop regulated projects, giving efficiently engineered solutions that reduce the validation effort needed. This document describes the FDA 21 CFR Part 11 regulation and how the zenon Software Platform is in full accordance with it, promoting innovation through the development of validation processes as efficiently as possible.

2. Introduction

This document details the information on how zenon is in full accordance with the FDA 21 CFR Part 11 regulation.

The FDA 21 CFR Part 11 regulation (from now on referenced as "Part 11 regulation") establishes the criteria for the use of electronic records and signatures under which they will be considered equivalent to conventional paper records and handwritten signatures.

Part 11 regulation concerns all electronic records that are created, modified, maintained, archived, retrieved or distributed for regulatory purposes.

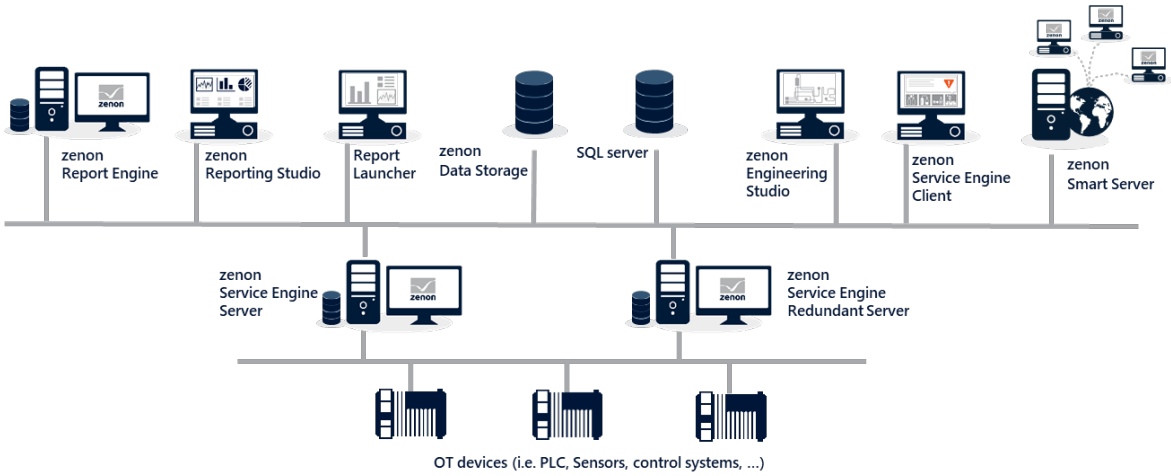
This requires related computerized systems to employ procedures and controls designed to ensure the authenticity, security, and confidentiality of electronic records.

Moreover, the zenon Software Platform offers functionalities, workflows and security measures that enable the customer to create compliant projects. However, the ultimate responsibility for the software validation belongs to the regulated company since the software compliance depends on the operational environment in which it is used.

COPA-DATA is available to assist with receive both postal and on-site audits to provide evidence that the zenon Software Platform operates in compliance with the applicable regulatory rules and with the reference guidelines for the life-science industries.

2.1. Scope – System Architecture

This document applies to the zenon Software Platform consisting of the following modules:



- zenon Engineering Studio → This is an administration module used to configure projects, i.e. HMI screens, recipes, audit trail, user levels, etc.

- zenon Service Engine → This is a module used by end users to execute projects designed using the zenon Engineering Studio.

- zenon Reporting Studio → This is an application used by administrators to configure reports and layouts using report templates.

- zenon Report Engine: This is the application generating reports based on predefined templates, using real time and historical data produced within zenon platform and linked external databases.

- Report Launcher → This is a web client where configured reports are made available to end users who can then launch, display, print and export the reports.

- zenon Data Storage -> This is a zenon service, based on MongoDB technology, where historical data produced in zenon software platform are stored (e.g. Time series process values, Alarm history, Audit Trail).

- zenon Smart Server -> This service offers access to zenon application via Web Clients.

3. Part 11 compliance with zenon

For automated projects operating in regulated areas, compliance with Part 11 regulation is mandatory.

zenon provides the technical features needed to satisfy the requirements for regulated environments, such as audit trail, alarm management, user administration, security, data storage, and reporting, either as a standalone system or as part of an integrated system.

With zenon, all projects are able to comply with Part 11 regulation. The zenon philosophy of parameterization instead of programming follows the "use by many" library concept to fulfill the functional aims and provide automation, HMI, and SCADA operational functionalities. Parameters can be easily set to enable the required functionality in a manner that satisfies the Part 11 regulation.

The validation process has the highest efficiency possible thanks to the system parametrizations, which enable full integral functionality and native communication with industrial systems and networks. "Native communication" means that connection to systems and networks is achieved without the need to involve another system because any possible interface is an integral component of the zenon Software Platform. Interfaces do not need to be validated separately. Consequently, validation covers the whole zenon project including the interfaces.

Moreover, the fact that native communication doesn't need any design or configuration on the third-party system means that zenon simply connects with full bi-directional data exchange. The use of integral functionality and parametrizations instead of programming allows full control over the system behavior. Over the entire project, risk is reduced since, in this way, the software is simply configured. Therefore, compliance with Part 11 regulation is entirely possible for all projects at each development stage.

zenon development has always been driven by the need to ensure quality and compliance with Part 11 and other international regulations in a GMP environment. The zenon basic design is always maintained, while the configuration of individual modules and components can be set and reset to meet specific requirements without affecting the validation status of the overall project.

4. FDA 21 CFR Part 11 regulation

The Part 11 regulation is separated into three sections. Firstly, "Subpart A" gives the general purpose of the regulation, and it provides the definitions of the terms used.

The detailed criteria are laid out in "Subpart B" for Electronic Records, and in "Subpart C" for Electronic Signatures. This document contains Part 11 Compliance statements for Section B and C requirements and explains how they are dealt with by the zenon Software Platform.

An extract of Subpart A is reported here, below, in order to illustrate the scope of this document and the terminology used.

4.1. Subpart A – General Provisions

§ 11.1 Scope

(a) The regulations set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full hand-written signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with § 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

§11.2 Implementation

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S–0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g. method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

§ 11.3 Definitions

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) Act means the Federal Food, Drug, and Cosmetic Act (secs. 201–903 (21 U.S.C. 321–393)).

(2) Agency means the Food and Drug Administration.

(3) Biometrics means 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.

(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.

(5) Digital signature means 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.

(6) Electronic record means 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.

(7) Electronic signature means 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.

(8) Handwritten signature means 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.

(9) Open system means 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.

5. 21 CFR Part 11 compliance statements

5.1. Subpart B – Electronic Records

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 regulated company is ultimately responsible for the system validation. However, zenon provides several tools to assist in the validation process.

zenon Service Engine
zenon offers a documentation tool that provides a hardcopy of the project content as well as a comparison wizard that can identify differences in projects, highlighting changes and the situations that require verification. zenon Engineering Studio includes also a "history of changes" functionality that tracks all the modifications to the configuration of the zenon project. This information is available to support the configuration management process.

zenon Report Engine
In order to support the configuration management process, we recommend users manage report template versioning manually, adding a version number and an explanatory comment (e.g. in the Report Launcher comment and in the Reporting Studio comment fields) in case of changes to the report template.

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.

zenon Service Engine

Data in zenon software platform is saved in its own proprietary file formats or in a SQL database or in a MongoDB data storage. The individual data can be accessed in many ways:

- zenon has reporting capabilities, proving combined or individual documents for audit trail, alarm lists, historical and online values. The data is provided as a screen report, hardcopy, or electronic .PDF format, allowing reading and archiving of the data.
- zenon integrated tools include: audit trail, alarm management, and archive revision screens for reading, listing and commenting. Data can be stored in the proprietary formats and accessed via the zenon tools afterwards.
- Data can be exported into different formats (dBase, ASCII/CSV, XML, SQL) and then displayed and archived in external systems.
- Historical data can be stored in a relational SQL database. External programs can access data there via authorized access.

Specific reports can be configured using the zenon Report Viewer, which can generate reports when manually requested by a user; automatically on process events, such as "batch complete"; on a timed basis; or when instructed by an external system, such as the ERP or MES.

zenon Report Engine

zenon Report Engine is used to design and generate reports to visualize, print and export data acquired by zenon Service Engine. It can access data from any linked database, even third-party databases.

Reports can be exported in .PDF, .XML, .CSV, Word, Excel, PowerPoint, .MHTML formats.

Reports can be sent by email or stored in a central file share.

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

zenon Service Engine

Data is stored in zenon-specific binary files, which can be secured by the security system of the Windows file system, or in a SQL database or in a MongoDB data storage. In all cases, customers should establish policies and procedures to ensure that records are retained for an appropriate retention period.

The location of the data can be specified by the user. Therefore, data can be placed on a secure server with its own protection and security measures.

zenon Report Engine

zenon Report Engine is provided with its own SQL database where report (RDL files) and configuration data are saved. This database also contains the procedures used by the system to populate and optimize report generation.

The zenon Report Engine database is protected by means of access control measures.

Dynamic data that is used to populate the reports is not saved in the tool database but is read on the interfaced databases on request.
Exported or saved reports fall under the responsibility of the regulated company, since their protection depends on where they are archived.

11.10 (d) Limiting system access to authorized individuals.

zenon Service Engine
Access to both zenon Service Engine and zenon Engineering Studio can be limited to authorized users who have active credentials (username and password).

zenon has local internal User Administration features and supports the use of Active Directory accounts. Both systems can be used concurrently.
Biometric and external security identification devices that bear or generate identification codes or password information can be accommodated too. They can be activated upon request.

The system detects failed login attempts with incorrect passwords or ID and it locks out the user after a certain (configurable) number of attempts. All successful and unsuccessful login attempts are recorded. zenon also offers password aging, length, complexity and history functionalities.

Each zenon project should utilize the automatic user logout function which logs out a user after a defined period of time.

In order to prevent concurrent access to the same record in client-server architectures, it is possible to set an option that allows only one person to access the record at a time.
When accessing the system remotely, specific functionality is available to allow only one person to access the system at a time, and protocols are in place to request access and log out other users.

Customers must have procedures in place to define who is authorized to access the system and at which access level. Moreover, the customer's procedures should be in place at the operating system level to restrict user access across the PC operating system.

zenon Report Engine
Access to zenon Report Engine is limited to authorized users, i.e. users who have been enabled by the Administrator to access the Report Launcher.

Users/user groups can be given access rights to one or more folders that contain report(s). In addition, different user roles with different privileges can be configured, e.g. administrator can delete/rename report templates while standard users can only run reports.
zenon Report Engine can use both Windows local accounts and Active Directory accounts.

Only administrators can access to the SQL database using the standard login functionality of the database itself.

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.

zenon Service Engine
All events managed through the user interface (i.e. in the Service Engine module) can be included in the audit trail.
The fields that are recorded in the audit trail can be configured at project level (i.e. in the zenon Engineering Studio).

The audit trail records: timestamp (date and time of the event), variable name, user name, inserted and modified values (in this case, the audit trail should register both the old value and the new one). In addition, it is possible to configure the audit trail to display further information, such as: variable identification, full user name, computer or system name, project/application name, variable status, alarm text, alarm area and alarm class, etc.
The system can be configured to allow users to add comments alongside all captured information.
Furthermore, automated events and system events can be recorded in the audit trail.

zenon has built-in clock synchronization with the (server) operating system date and time to ensure that all date and time stamps are accurately recorded in the audit trail.
It is the responsibility of the customer to synchronize the operating system date and time with a reference one and to inhibit the change of date, time and time zone.

The audit trail is automatically recorded and maintained as a binary file in a specific folder. This data is accessible, filterable and available to query through the user interface; both the audit trail of the entire project and a view of the audit trail for any critical field can be visualized.

Audit trail data can be exported in several formats (i.e. CSV, XML, SQL, etc.) and printed in .PDF and paper format.
The customer is responsible for activating the audit trail and configuring the appropriate backups for it.

zenon Report Engine
The audit trail is not applicable to zenon Report Engine since while end users can launch a report they cannot modify the data contained within it.
If the audit trail recorded by zenon Service Engine is included in a report created with zenon Report Engine, it is the responsibility of the report designer to properly configure the report in order to include all the required audit trail information (i.e. username of the operator, date and time of the operation, value before and after the change).

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

zenon Service Engine
The sequencing of user steps, automatic steps and operational checks can be configured using the integral zenon functionality to force a user to follow a workflow at certain phases of process execution (e.g. configuration of recipes).

zenon Report Engine
Operational checks are not applicable to zenon Report Engine since the tool does not manage workflows.
However, it is important to note here that end users can launch only released reports, i.e. reports that have been uploaded by an administrator on the Report Launcher at the end of the design stage.

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.

zenon Service Engine
Access to both zenon Engineering Studio and zenon Service Engine can be limited to authorized users who have active credentials (username and password).
Utilizing zenon's authorization levels, different layers of security can be applied to different users or user groups.

Each dynamic element accessible to a user can have an authorization level attributed to it. As a result, the logged-in user must hold the specific authorization level in order to execute a dynamic element.

Customers must have procedures in place to define who is authorized to access the system and at which access level. Moreover, the customer's procedures should be in place at the operating system level to restrict user access across the PC operating system.

zenon Report Engine
Access to zenon Report Engine is limited to authorized users, i.e. users who have been enabled by the Administrator to access the Report Launcher.
Users/User groups can be given access rights to one or more folders that contain report(s). In addition, different user roles with different privileges can be configured, e.g. administrators can delete/rename report templates while standard users can only run reports.
zenon Report Engine can use both Windows local accounts and Active Directory accounts.

Only administrators can access the SQL database using the standard login functionality of the database itself.

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.

zenon Service Engine
Data input can be restricted to defined stations, limiting actions to specific locations.
For each acquired value, proper labels must be defined at an HMI level in order to identify the source of the data for both real-time acquisition and for historical trends.

zenon Report Engine
Checks on the validity of the data sources used by the report are carried out by zenon Service Engine since it interfaces with those source fields.
However, it is necessary to correctly configure reports in order to report the correct tag or ID for each plotted variable. This is the responsibility of the user who designs the reports.

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.

zenon Service Engine, zenon Report Engine
It is the customer's responsibility to ensure that all the individuals who develop, maintain, or use the system are properly trained to perform their tasks, according to the customer's SOPs. COPA-DATA personnel involved in product development have appropriate education, training, and experience to perform their assigned tasks and in the regulations governing the pharmaceutical and healthcare industries.

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.

zenon Service Engine
It is the customer's responsibility to satisfy this requirement, according to its SOPs.

zenon Report Engine
Not applicable, since zenon Report Engine does not implement electronic signatures.

11.10 (k) Use of appropriate controls over systems documentation including:

11.10 (k-1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

11.10 (k-2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

It is the customer's responsibility to satisfy this requirement, according to its SOPs.
Technical and quality documentation is managed by COPA-DATA using the Microsoft Azure DevOps platform, according to COPA-DATA internal SOPs. In the DevOps platform, COPA-DATA handles product requests, product malfunctions product documentation, software changes and extensions.

zenon has several measures in place to support the accurate control, documentation, and backup of project evolution and modification.

zenon Service Engine

Version control can be implemented in the zenon Engineering Studio. By utilizing major and minor project revision numbers, strict control of the project evolution can be enforced. The major revision number is user-defined, the minor revision number is incremented automatically after each project backup.

Using the XML backup option, external systems can be used to provide versioning and change control, with full backup capabilities in zenon.

With the project backup mechanism, previous projects can be restored, giving protection from the associated risk of modification.

The zenon Engineering Studio has a "History of Changes" mechanism, where any changes to a project are recorded in detail. All changes and modifications can be easily identified.

zenon also has a project comparison tool which provides a detailed account of the differences between two projects, displaying modified, additional, and deleted project elements. When used in combination with the project versioning, clear documentary evidence is provided of the evolution a project has undergone. This serves to highlight any risks and validation testing that must be performed.

zenon Report Engine

In order to support the configuration management process, it is recommended users manage report template versioning manually; adding a version number and an explanatory comment (e.g. in the Report Launcher comments and in the Reporting Studio comment fields) following changes to the report template.

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.

zenon Service Engine, zenon Report Engine

If the system architecture is distributed on different company sites, each system module installed on a site communicates with the other sites by means of the zenon IIoT Services,.

Data exchange between modules is TLS-secured and certificate-based.

11.50 Signature manifestations

11.50 (a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

11.50 (a-1) The printed name of the signer;
11.50 (a-2) The date and time when the signature was executed;
11.50 (a-3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

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).

zenon Service Engine
Electronic signatures can be enabled for each project field and button; for example, for modifying a GxP critical recipe parameter, for the steps of a recipe approval workflow, or for executing a lot.
The electronic signature can be defined at a central level e.g. at tag level for a CPP and is automatically applied whenever this tag is modified.
Each signature record consists of the full name of the user, the date and time of the signature, comment and the meaning of the signature (e.g. value change, verification of value change, recipe approval, etc.).
In zenon Engineering Studio, it is possible to configure signature workflows requiring 1, 2 or 3 different users. (i.e. User1 performs the change, User2 verifies the change, User3 approves the change). These Users must not be within the same user group.
Each user can add an individual comment to his signature manifestation.
All this information can be visualized when the signed record is visualized on the HMI and/or on the generated paper or .PDF report.

zenon Report Engine
zenon Report Engine does not have electronic signature functionality.
If it is necessary to satisfy the signature manifestation requirements for a record signed in zenon Service Engine or in any other interfaced system, it is the responsibility of the report designer to properly configure the report in order to include all the required signature information (i.e. the printed name of the signer; the date and time when the signature was executed; the meaning associated with the signature).

11.70 Signature/record linking

Electronic signatures and hand-written 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

zenon Service Engine
Electronic signatures are linked to the signed records and it is not possible to alter or falsify an executed signature.

Electronic signatures are stored in the same binary database as the audit-trail records, hence they are subject to the same controls described above, i.e. they are in proprietary binary format and, therefore, individual modifications are not possible external to zenon.

Customers should also establish policies and procedures to prevent unauthorized access to signature records (AML, CEL), which can be achieved using the security system of the Windows file system. Customers are also responsible for ensuring the appropriate backup systems are in place.

When Audit Trail (CEL) is stored in an SQL database or in zenon Data Storage based on MongoDB technology, customers should establish policies and procedures to prevent unauthorized access.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

5.2. Subpart C – Electronic Signatures

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.

zenon Service Engine
The user is required to enter an ID and a password to sign a record, ensuring that the electronic record is clearly attributable to the individual user.
Customers using zenon applications in FDA-regulated environments are responsible for ensuring that electronic signatures are attributable to one individual only and cannot be reused by or reassigned to any other individual.

zenon local user administration and Windows Active Directory do not permit the creation of duplicate login or user ID, provided that user accounts are disabled and not deleted.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine, zenon Report Engine
Customers using zenon applications in FDA-regulated environments are responsible for verifying the identities of individuals using electronic signatures.

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.

11.100 (c-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.

11.100 (c-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.

zenon Service Engine, zenon Report Engine
It is the customer's responsibility to satisfy this requirement, according to its SOPs.

11.200 Electronic signature components and controls

11.200 (a) Electronic signatures that are not based upon biometrics shall:

11.200 (a-1) Employ at least two distinct identification components such as an identification code and password.

zenon Service Engine
The zenon user administration and Windows Active Directory user administration require the input of a "User-ID" and a "Password" to sign a record.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

11.200 (a-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.

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.

zenon Service Engine
To indicate the start of a continuous period of controlled system access, the user must use their user ID and password to log into zenon.
zenon security requires the user to enter all signature components for each signing.

The zenon "User Login Timeout" period should be configured to limit the extent of a continuous period of controlled system access. Customers should also implement policies and procedures that require users to log out of the application during periods of non-use.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

11.200 (a-2) Be used only by their genuine owners.

zenon Service Engine
Customers using zenon applications in FDA-regulated environments are responsible for ensuring that non-biometric electronic signatures are nominal and used only by their genuine owners by means of appropriate training in this matter.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

11.200 (a-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.

zenon Service Engine
Within the local zenon user administration, when the administrator resets the password, zenon security automatically requires a new password entry the next time the user logs in.
When using Windows Active Directory, the customer's system administrators must enable the Windows security function "User Must Change Password at Next Logon" in order to prevent the system administrators from knowing both the user's user ID and password.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine
Biometric security identification systems are accommodated in zenon via an external security system. The responsibility for electronic signatures based upon biometrics that are designed to ensure that they cannot be used by anyone other than their genuine owner falls to this external biometric security identification system.

zenon Report Engine:
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine
The user is required to enter an ID and a password to sign records. Since the password is personal, control is carried out on the user ID. zenon local user administration and Windows Active Directory do not permit the creation of duplicate logins or user IDs, provided that user IDs are disabled and not deleted.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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).

zenon Service Engine
Both zenon local user administration and Windows Active Directory security should be configured to use the functionality for password aging.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine
When using such external security systems to provide login and signature credentials to the zenon system, this responsibility falls to the customer.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine
The system detects password and ID errors and it locks out the user after a certain (configurable) number of failed login attempts. Only an Administrator user can re-enable a locked user account.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

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.

zenon Service Engine
When using such external security systems to provide login and signature credentials to the zenon system, this responsibility falls to the customer.

zenon Report Engine
Not applicable, since zenon Report Engine does not offer electronic signature functionality.

© 2023 Ing. Punzenberger COPA-DATA GmbH.

All rights reserved. This document may not be reproduced or photocopied in any form (electronically or mechanically) without a prior permission in writing from Ing. Punzenberger COPA-DATA GmbH. The technical data contained herein have been provided solely for informational purposes and are not legally binding. Subject to change, technical or otherwise. Registered trademarks **zenon®** and **zenon Report Engine®** are both trademarks registered by Ing. Punzenberger COPA-DATA GmbH. All other brands or product names are trademarks or registered trademarks of the respective owner and have not been specifically earmarked. We thank our partners for their friendly support and the pictures they provided.