AuditSafe Regulatory Compliance Guide

version 1.0

This document presents the regulations relating to electronic records and signatures, namely:

- US: 21 CFR Part 11, subparts B and C
- EU: Annex 11

and how the technical features of the *AuditSafe* product meet these requiremments.

Each regulation is listed below, with an accompanying explanation of how the *AuditSafe* software meets the regulation, along with information relating to your organisation's responsibilities.

Before reading this document, please note that the explanations we provide represent our interpretation of 21 CFR Part 11 and Annex 11. We do not represent any government organisation, nor are we a legal practitioner. Therefore, information given below should be used in conjunction with local legal advice. The text of each regulation is current as of December 2023.

AuditSafe software is intended to address GLP/GMP requirements. It is the user's responsibility to ensure that the software is appropriately validated within their quality management system or equivalent operating environment. For organisations developing medical devices, refer to ISO 13485:2016 Clause 4.1.6, ISO TR 80002-2, and General Principles of Software Validation (FDA, 2002).

US: 21 CFR Part 11

Subpart B - Electronic Records

Section 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:

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

Interpretation: How an organisation validates that the data produced from the system can be trusted.
How *AuditSafe* complies: All TotalLab software is tested and follows a documented life-cycle process.
Customer responsibility: The customer organisation is responsible for validating the software for its intended purpose and ensuring that it meets expected performance requirements within the organisation's operational environment.

(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.

Interpretation: How an organisation ensures that all electronic records can be provided in human readable form.
How *AuditSafe* complies: *AuditSafe* retains historical copies of projects as they are modified, allowing read-only access to previous revisions. It also generates date- and time-stamped audit trails of changes to projects. Audit trails are made available in PDF format for read-only inspection.
Customer responsibility: The customer organisation is responsible for restricting access to the *AuditSafe* system.

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

Interpretation: How an organisation protects documentation and keeps it readily available for the required retention period.
How *AuditSafe* complies: Records are stored securely within the *AuditSafe* server, a new revision being created when updates are commited to the system. *AuditSafe* users may access read-only copies of project revisions through the *AuditSafe* client software.
Customer responsibility: The customer organisation is

responsible for ensuring restricted access to the *AuditSafe* server and secure folder, for verifying retention periods relevant to their domain and for backups of the project data.

(d) Limiting system access to authorized individuals.

Interpretation: How an organisation ensures that only authorised users have access to the system.
How *AuditSafe* complies: Access to the *AuditSafe* software is controlled by username / password credentials assigned to individuals.
Customer responsibility: The customer organisation is responsible for designating which users have access to the *AuditSafe* system and with which permissions.

(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.

Interpretation: How an organisation ensures that the complete audit trail of a project is captured by the system, retained and accessible by authorised users.
How *AuditSafe* complies: The *AuditSafe* system automatically generates time-stamped records showing user actions and maintaining the project-related data at each timestamp. The user who took the action is also recorded. Data is never deleted.
Customer responsibility: The customer organisation is responsible for maintaining the records for the defined retention period. This will need to take into consideration the likes of hardware and software updates (including operating system updates), etc.

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

Interpretation: How an organisation ensures that electronic workflows within the software operate correctly.
How *AuditSafe* complies: Workflows are defined within the software and users are not able to take actions that are outside of these workflows. Actions are visible in the audit trail.
Customer responsibility: The customer organisation is responsible for validating the software for its intended purpose and

ensuring that it meets expected performance requirements within the organisation's operational environment.

(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.

Interpretation: How an organisation restricts user access (system and record level) and verifies that the users performing functions within the system are authorised to do so.
How *AuditSafe* complies: Access to the system, and therefore the records stored within, is limited to authorised users by username and password credentials. In addition, users must be granted additional privileges to perform certain actions, such as sign-off. Certain actions (e.g. sign-off) require password re-entry. User sessions timeout after a duration specified in the server, requiring re-entry of credentials.
Customer responsibility: The customer organisation is responsible for granting access and privileges to individual users.

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Interpretation: How an organisation verifies that equipment being used for regulated purposes is functioning properly.
How *AuditSafe* complies: Users are able to visually check the text / files they are adding to the *AuditSafe* system.
Customer responsibility: The customer organisation is responsible for hardware qualification.

(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.

Interpretation: How an organisation ensures that only trained and qualified personnel perform functions on or within the system.
How *AuditSafe* complies: TotalLab only employs staff with extensive, relevant experience in the area for which they have responsibility, be that software development, software testing, or other business functions.
Customer responsibility: The customer organisation is responsible for ensuring that users of their systems, including the *AuditSafe* software, are suitably trained and qualified.

(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.

Interpretation: How an organisation holds individuals accountable for the integrity of their actions relating to electronic records and signatures.
How *AuditSafe* complies: This is not directly applicable as it involves controls that must be implemented by the customer organisation. However, the *AuditSafe* software can help organisations to meet this requirement by limiting access to records and recording the actions of individuals.
Customer responsibility: The customer organisation is responsible for implementing policies that meet this requirement.

(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.

Interpretation: How an organisation controls documents related to system operation and maintenance and preserves the complete history of changes made to these documents.
How *AuditSafe* complies: User documentation is supplied as part of the installation package. Newer versions are supplied when the software is updated.
Customer responsibility: The customer organisation is responsible for the internal document controls, including supplied manuals and operation and maintenance procedures.

Section 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.

Interpretation: For organisations using open systems, everything for closed systems (Section 11.10) still applies. In addition, it must implement further measures to ensure the authenticity and integrity of records.
How *AuditSafe* complies: Not applicable as *AuditSafe* software is a closed system under definition (b)(4) of 21 CFR Part 11 §11.3.
Customer responsibility: Not applicable.

Section 11.50 Signature manifestations

(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.

Interpretation: Any time that an electronic record is signed, the following information must be visible alongside the signature: The name of the signer; Date and time of the signature; The meaning associated with the signature (e.g. update to records, sign-off by reviewer, etc.)
How *AuditSafe* complies: Audit reports show all three data points, clearly associated with each signature.
Customer responsibility: The customer organisation is responsible for correctly configuring user names and the correct privileges for each user.

(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).

Interpretation: That the requirements set out in 11.50(a) are subject to the same controls as records and must be human readable.
How *AuditSafe* complies: Signatures are associated with the related records internally within the software. Once applied, these signatures may not be edited, deleted or re-assigned. These signatures are available in a human-readable form through the

generation of PDF audit reports.
Customer responsibility: The customer organisation is responsible for correctly configuring user names and the correct privileges for each user.

Section 11.70 Signature / record linking

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.

Interpretation: Signatures must remain connected to the related record. Such signatures cannot be removed or altered once applied to a record, nor can they be applied falsely to another record.
How *AuditSafe* complies: *AuditSafe* restricts access to records through the use of username / password credentials and only certain users have the privileges required to sign-off / approve work. Signatures affixed to records within the *AuditSafe* system are permanently attached within the system and are not accessible by any user for the purposes of deletion, alteration or transfer.
Customer responsibility: The customer organisation is responsible for assigning the correct privileges to users. However, the organisation is not able to manipulate the affixation of signatures to records under the control of the *AuditSafe* system.

Subpart C - Electronic Signatures

Section 11.100 General requirements

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

Interpretation: Each user must have a unique electronic signature which must not be shared with other users.
How *AuditSafe* complies: *AuditSafe* allows organisations to create multiple electronic signatures in the form of username / password pairs that can be assigned to individuals.
Customer responsibility: The customer organisation must have procedures in place to ensure uniqueness of user credentials.

(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.

Interpretation: A user's identity must be verified before an electronic signature is created and assigned to that user.
How *AuditSafe* complies: This is not applicable to the *AuditSafe* software as it relies on the organisation's internal procedures.
Customer responsibility: The customer organisation must have procedures in place to verify the identity of individuals.

(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.

(1) The certification shall be signed with a traditional handwritten signature and submitted in electronic or paper form. Information on where to submit the certification can be found on FDA's web page on Letters of Non-Repudiation Agreement.

(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.

Interpretation: Before an organisation implements electronic signatures, it must notify the FDA of its intention to do so, and state that it intends to treat electronic signatures as legally binding.
How *AuditSafe* complies: This is not applicable to the *AuditSafe* software as it relies on the organisation's internal procedures.
Customer responsibility: If the customer organisation is using the *AuditSafe* software to comply with US medical device regulations, it must make the appropriate notification to the FDA.

Section 11.200 Electronic signature components and controls

(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.

Interpretation: Electronic signatures that are not biometric in nature, must be made up of two distinct parts, e.g. a user name and a password.
How *AuditSafe* complies: *AuditSafe* user credentials consist of

both a unique user identifier and a secret password.
Customer responsibility: The customer organisation is responsible for creating user credentials.

(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.

Interpretation: The first time a user signs a record, the system must require them to enter all parts of their electronic signature. Subsequent signings during the same session require only a single part of the signature, e.g. a password.
How *AuditSafe* complies: A user is required to enter both parts of their electronic signature when first accessing the *AuditSafe* system. Subsequent signatures require entry of their password.
Customer responsibility: The customer organisation is responsible for configuring electronic signatures for users.

(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.

Interpretation: When a user logs out of a system (by choice or by timeout) and logs back in, the user is required to enter all parts of their electronic signature.
How *AuditSafe* complies: Once logged out of the *AuditSafe* software, a user is required to enter both username and password to regain access. Subsequent signatures also require entry of their password.
Customer responsibility: The customer organisation is responsible for configuring electronic signatures for users.

(2) Be used only by their genuine owners; and

Interpretation: Electronic signatures must only be used by the individuals to whom they are assigned.
How *AuditSafe* complies: The *AuditSafe* software gives administrators the ability to configure user access and ensure duplicate user IDs are not allowed.
Customer responsibility: The customer organisation is responsible for configuring user accounts correctly (e.g. Windows and *AuditSafe* accounts).

(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.

Interpretation: In circumstances where an individual's electronic signature must be used by someone to whom it has not been assigned, the system must require two users to operate together.
How *AuditSafe* complies: The *AuditSafe* system allows for emergency login (in the event that a user has left the organisation, is on leave, etc.). Two users with the required privileges are needed to gain access to the user's account. Such access is recorded in the system audit trail and each action undertaken during such a login session is tagged with the two users.
Customer responsibility: The customer organisation is responsible for configuring user accounts correctly and ensuring that the necessary privileges are assigned to suitable users (e.g. supervisor, managers), according to internal policies.

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Interpretation: Where an electronic signature is of the biometric type, this may only be used by the individual to whom it has been assigned.
How *AuditSafe* complies: Not applicable as *AuditSafe* does not support biometric signatures.
Customer responsibility: Not applicable for *AuditSafe*.

Section 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:

(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.

Interpretation: No two users can have the same combination of user ID and password and each user ID can never be assigned to more than one individual.
How *AuditSafe* complies: The *AuditSafe* software prevents the creation of duplicate usernames.

Customer responsibility: The customer organisation is responsible for ensuring that user IDs are only ever assigned to one user.

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Interpretation: Passwords must be checked, recalled, or changed from time to time.
How *AuditSafe* complies: The *AuditSafe* software allows for timed password expiry, forced password expiry and deactivation of user accounts.
Customer responsibility: The customer organisation is responsible for configuring user accounts correctly.

(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.

Interpretation: If the credentials relating to an electronic signature are lost or stolen, it must be deauthorised and a secure replacement issued.
How *AuditSafe* complies: While *AuditSafe* supports the deauthorisation (deactivation) and creation of new accounts, the responsibility for implementation lies with the customer organisation.
Customer responsibility: The customer organisation is responsible for configuring user accounts correctly and for implementing internal policies and procedures to manage account creation and deletion.

(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.

Interpretation: Unauthorised attempts to access user accounts must be detected and reported.
How *AuditSafe* complies: *AuditSafe* records all failed login attempts in the system audit trail to allow for further investigation. A warning count is also displayed on the *Users* tab of the *AuditSafe* server webpage.

Customer responsibility: The customer organisation is responsible for configuring user accounts correctly.

(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.

Interpretation: Passcode tokens must be tested before they are issued for use and periodically while in use to ensure they are functioning correctly.
How *AuditSafe* complies: This is not applicable as the customer organisation is responsible for generating identification codes.
Customer responsibility: The customer organisation is responsible for the generation of identification codes or passwords following their internal procedures using whichever method is generally employed.

EU: Annex 11

While this document is primarily focussed on US FDA regulations (21 CFR Part 11), it should be noted that the *AuditSafe* software may also assist in meeting the recommendations listed in EU Annex 11 to the good manufacturing practice requirements set out in Directive 2002/94/EC and Directive 91/412/EEC.

While Annex 11 is not a legal requirement, it is a strongly recommended guideline and covers similar ground to 21 CFR Part 11. The following clauses are particularly relevant:

9. Audit Trails: Consideration should be given, based on a risk assessment, to building into the system the creation of a record of all GMP-relevant changes and deletions (a system generated "audit trail"). For change or deletion of GMP-relevant data the reason should be documented. Audit trails need to be available and convertible to a generally intelligible form and regularly reviewed.

AuditSafe generates a date- and time-stamped audit trail of changes to projects. Audit trails are made available in PDF format for read-only inspection.

12. Security:

12.1: Physical and/or logical controls should be in place to restrict access to computerised system to authorised persons. Suitable methods of preventing unauthorised entry to the system may include the use of keys, pass cards, personal codes with passwords, biometrics, restricted access to computer equipment and data storage areas.

Access to the system, and therefore the records stored within, is limited to authorised users by username and password credentials. In addition, users must be granted authority to perform certain actions, such as sign-off.

12.4: Management systems for data and for documents should be designed to record the identity of operators entering, changing, confirming or deleting data including date and time.

AuditSafe automatically generates time-stamped records showing user actions and maintaining the project-related data at each timestamp. The user who took the action is also recorded.

14. Electronic Signature: Electronic records may be signed electronically. Electronic signatures are expected to:
a. have the same impact as hand-written signatures within the boundaries of the company,
b. be permanently linked to their respective record,
c. include the time and date that they were applied.

AuditSafe restricts access to records through the use of username / password credentials and only certain users have the privileges required to sign-off / approve work. Signatures affixed to records within the *AuditSafe* system are permanently attached within the system and are not accessible by any user for the purposes of deletion, alteration or transfer.

17. Archiving: Data may be archived. This data should be checked for accessibility, readability and integrity. If relevant changes are to be made to the system (e.g. computer equipment or programs), then the ability to retrieve the data should be ensured and tested.

AuditSafe maintains revisions of projects on the server. These revisions are accessible by server administrators for backup to another storage system, if required.

21 CFR Part 11 Compliance matrix

SECTION	*AUDITSAFE* COMPLIANCE
Subpart B	
11.10 (a)	Compliant
11.10 (b)	Compliant
11.10 (c)	Compliant
11.10 (d)	Compliant

SECTION	*AUDITSAFE* COMPLIANCE
11.10 (e)	Compliant
11.10 (f)	Compliant
11.10 (g)	Compliant
11.10 (h)	Not Applicable
11.10 (i)	Not Applicable
11.10 (j)	Not Directly Applicable
11.10 (k)	Compliant
11.30	Not Applicable
11.50 (a)	Compliant
11.50 (b)	Compliant
11.70	Compliant
Subpart C	
11.100 (a)	Compliant
11.100 (b)	Not Applicable
11.100 (c)	Not Applicable
11.200 (a)(1)	Compliant
11.200 (a)(1)(i)	Compliant
11.200 (a)(1)(ii)	Compliant
11.200 (a)(2)	Compliant
11.200 (a)(3)	Compliant
11.200 (b)	Compliant
11.300 (a)	Compliant
11.300 (b)	Not Applicable
11.300 (c)	Partially Compliant
11.300 (d)	Compliant
11.300 (e)	Not Applicable

References

- **21 CFR Part 11. US Government** (accessed 5 December 2023)
- **Annex 11. European Commission** (accessed 5 December 2023)

- ISO 13485:2016 Medical devices - Quality management systems - Requirements for regulatory purposes
- ISO/TR 80002-2:2017 Medical device software - Part 2: Validation of software for medical device quality systems