Red Nucleus

DirectusPRO CFR Part 11 White Paper

OVERVIEW

Life sciences companies must comply with general FDA regulations related to the qualification and validation of systems. Qualification is a process that is used to evaluate whether a system complies with regulations, specifications, or conditions imposed at the start of a development phase. Validation is a process of establishing evidence that provides a high degree of assurance that a system accomplishes its intended requirements. Generally, infrastructure must be qualified, while applications must be validated. This document focuses on validation specifically related to "21 CFR Part 11" (The term 21 CFR Part 11 refers to the Code of Federal Regulations [CFR]: Title 21 – Chapter 1, Food and Drug Administration Part 11 – Electronic Records; Electronic Signatures), as opposed to the qualification and validation processes related to broader FDA regulations. 21 CFR Part 11 is part of the Code of Federal Regulations, which have been promulgated to enforce the law embodied in the Federal Food, Drug, and Cosmetic Act. Life sciences companies must comply with 21 CFR Part 11 if they want to take advantage of electronic records and "electronic signatures." The law applies to computer systems that are regulated by existing FDA regulations, also called predicate rules, as opposed to non-FDA-regulated business systems. The FDA also produces guidance documents to assist with interpretation and enforcement.

The 21 CFR Part 11 regulations created guidelines for the proper handling of FDA-regulated information that is stored electronically and the application of electronic signatures that are considered to be the legally binding equivalent to handwritten signatures on documents. Computer systems that maintain records electronically must ensure the integrity of the record and ensure that:

- the information gathered is accurate and complete
- there is accountability for actions that create, modify, or delete information
- a complete history of the record is available from point of inception
- electronic signatures on records cannot be repudiated.

Computer systems need to have adequate technical capabilities and features to permit organizations to meet the compliance requirements mandated by these regulations. Yet, the computer system used for any regulated business process is only one component of the regulated.

process. To determine that a process is compliant with the federal regulations, an organization must address not only the functions and features of the computer system used, but also how it is being deployed and configured, the intended use of the system, and the supporting processes and procedures for the application. **DirectusPRO has the native functions and features enabling the computer system owner to satisfy the compliance requirements of 21 CFR Part 11.**

COMPLYING WITH 21 CFR PART 11

Life sciences companies that have chosen to maintain records electronically must comply with 21 CFR Part 11 by ensuring that:

- the software products they use have been built / configured to function in a way that enables them to comply
- they develop and follow supporting SOPs that describe how to use and maintain the system in a way that enables them to comply.

21 CFR Part 11 regulations provide guidance for life sciences companies to meet the following goals:

- ensure the authenticity, integrity, and confidentiality of electronic records from the point of creation to the point of receipt by the FDA or point of lifecycle of retention of the record
- generate accurate and complete copies of records for the FDA to inspect and review
- ensure the security and easy retrieval of electronic records
- ensure that only authorized individuals can access, manipulate, and electronically sign records
- maintain a log of all changes made to electronic records throughout their lifecycle
- record and securely link electronic signatures to the electronic records to which they have been applied
- ensure that record processing steps are performed in the proper order
- ensure individuals who develop, maintain, or use the electronic record / electronic signing system are properly trained
- ensure individuals are accountable for actions initiated under their electronic signatures

- maintain control over system documentation
- establish and maintain controlled SOPs regarding all of the above and other requirements.

The regulations in 21 CFR Part 11 aim at reducing fraud while ensuring that electronic signatures and records are as reliable as their traditional paper counterparts.

§ 11.1 Scope.

(a) The regulations in this part 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 handwritten 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 mean 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 content of electronic records that are on the system.

(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication that is 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 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.

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:

Based on Section VI Definitions (§ 11.3) 41.-, the agency states that the most important factor in classifying a system as closed or open is whether the people responsible for the contents of the electronic records control access to the system containing those records. A system is closed if access is controlled by people responsible for the contents of the records. Because customers control the access rights to their DirectusPRO instance of the system and to their records, customers are well founded in concluding that the DirectusPRO system critical criterion and may be qualified as a closed system for purposes of this legislation.

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

In deploying DirectusPRO, DirectusPRO recommends that customers implement policies and procedures that include a periodic audit of the production system to ensure accuracy, reliability, and consistent intended performance in the installed active environment. Audit logs and history tracking provide for automatic data and username assignment to entries and edits in the history log, enabling tracking and accountability.

(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.

DirectusPRO provide extensive reporting capabilities, so reports can be generated to satisfy regulatory needs. Reports can be generated in both electronic and hard copy form, and once created, can be locked down to prevent manipulation of all data output. Data stored within the system can be exported in a variety of formats for the purposes of review, audit, and archive. Such formats include MS Word, pdf, XML and CSV.

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

All electronic records, as well as audit trail logs and any reason for change records, are maintained in the secure tenant isolated database of the DirectusPRO system. Access to the data is limited to specific individuals or groups. The modification and / or deletion of records is restricted, to ensure integrity throughout the record retention period; audit trail is also available for deletions. DirectusPRO does not contain an archiving mechanism. All records and associated audit trails are available for retrieval / data export until they are deleted from the DirectusPRO repository, and customers control deletion. DirectusPRO recommends that customers develop policies and procedures covering records retention (how long a record should be maintained) and disposition (what is done with the record at the end of its lifecycle). The policy should include specific rules for deleting, purging, or archiving records at the end of their lifecycle. DirectusPRO can assist in the development of these policies and procedures as well as in system configuration. DirectusPRO also has robust data backup and disaster recovery mechanisms in place.

(d) Limiting system access to authorized individuals.

All electronic records, as well as audit trail logs and any reason for change records, are maintained in the secure database of the DirectusPRO system. Record access is controlled by use of a unique sign-in (username) and password pair. Multiple levels of security and limitation of access to records and functionality are based on user roles, organization, and responsibilities. DirectusPRO recommends that customers implement policies and procedures to control the circumstances under which system access is granted as well as the user roles that define such access. DirectusPRO monitors and logs all access attempts, recording the username used, the date and time of the access attempt, and whether the attempt was successful or not.

(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 as long as it is required for the subject electronic records and shall be available for agency review and copying.

Time stamps are pulled from a common server. Each DirectusPRO data center has a network time protocol server that is synchronized to all production systems. Also, all electronic records contain information identifying the user who created or modified the record. When an electronic record is changed, the date, time, and action are recorded, along with both the previous and changed field values, which are recorded in fields flagged for audit history. All audit trail records are

maintained and can be archived for maintenance and stored for the required time periods. History tracking provides for automatic data and username assignment to entries and edits in the history log, enabling tracking and accountability. The system is also flexible in that customers can request to add their own custom data elements to the audit trail.

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

The DirectusPRO data collection and maintenance operations are managed through a well-defined sequence of steps (workflow) as defined by the system administrator. These workflow steps limit operators or users to specific functions and controlled entries or responses. DirectusPRO workflows can be used to ensure that the sequence of events prescribed in the customer's policies and procedures for a given process is strictly observed.

(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.

The DirectusPRO service maintains a list of users, roles, and access rights within its isolated tenant database. User authentication is provided by a unique sign-in and password maintained within the database (system configurable).

- All passwords are encrypted within the database.
- Password complexity requirements can be set by customers to inhibit the use of weak passwords.
- Password aging can be set to forces users to change passwords after a specified period of time.
- Password recycling configuration can be set to inhibit users from reusing a password for a specified period of time.
- Automatic account lockout can be set to guard against unauthorized use.
- Automatic sign-out after a specified idle period can be set to force additional sign in to continue system access.

(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.

DirectusPRO provides a variety of training and educational materials tailored to meet the requirements of the various categories of users who will utilize the system. Additionally, DirectusPRO works closely with clients to customize

training classes based on their specific needs. Conformance with this requirement is the responsibility of the customer.

(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.

DirectusPRO recommends that customers implement policies and procedures to cover the actions that administrators and end users must perform when using the DirectusPRO system. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management and audit trail configuration, archiving, and purging. For individual users, policies and procedures should be developed for actions such as data entry and data updates.

Conformance with this requirement is the responsibility of the customer.

(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.

DirectusPRO provides documentation for the software system in electronic form. This documentation should be included in part or in whole with the customer's own specific systems documentation. DirectusPRO recommends that customers develop policies and procedures covering the control of system operational documentation, system maintenance schedules and update activities.

§ 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.

All records within DirectusPRO are linked to the user who created or modified the record. Audit-trail / change-history records cannot be deleted or modified in any way from the DirectusPRO system. The user object cannot be disassociated from the original record or re-associated to another record.

Subpart C—Electronic Signatures

§ 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.

Each DirectusPRO user is identified by a unique identifier in the database that cannot be deleted or removed but whose further use can be disabled. These unique identifiers are linked, thereby identifying the user who created or modified a record. As a further security measure, new users are required to specify a unique password during their first use of DirectusPRO. This ensures that the users, and no one else (not even the administrator), know their password. DirectusPRO also recommends that customers implement policies and procedures to ensure that a given username is assigned to only one individual, that all individuals set their own password at the first login, and that all individuals agree not to divulge their password under any circumstances.

(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.

DirectusPRO recommends that the deploying organization implement policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval from their superiors. Conformance with this requirement is the responsibility of the customer.

---

§ 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.

A unique login name and password are required for gaining access to the DirectusPRO system. These two items uniquely identify a DirectusPRO user, and that person's name is subsequently associated with every record transaction performed by that user. The initial login to the system is considered the first signing.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components. Subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

DirectusPRO requires the entry of all signature components (username and password) at first sign-in. Where a signature action is required, re-entry of the User ID and Password signature components can be added, based on the application processes. An example might be to require the user to re-authenticate (e.g. enter User ID and Password as a signature execution action) before saving entered or reviewed data. Automatic sign-out requirements (forcing a subsequent sign-in) can be implemented, based on a predetermined time of inactivity or completion of a data entry operation. In this case, the subsequent sign-in counts as a new first signing.

---

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

Security measures built in to the DirectusPRO system help ensure that an electronic signature is used only by its actual owner. These measures include password aging, password recycling, idle account lockout, retry lockout, and password encryption. Training of users on the appropriate safeguards and use of passwords is fundamental to the integrity of their use. Non-sharing of electronic signatures via training and policies is the responsibility of the customer.

---

(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.

Only administrators with appropriate rights can invite and grant users access to the DirectusPRO system. The passwords must be created by their owners on first use, before they can receive access to DirectusPRO. All passwords are encrypted. Customers are responsible for training users on password security and enforcing that passwords cannot be shared.

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

DirectusPRO does not directly support biometric devices such as fingerprint recognition and retinal scanning.

---

§ 11.300 Controls for identification codes / passwords.

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.

DirectusPRO maintains a unique login-name / password combination associated with every user granted system access. These combinations uniquely identify every user logging into the systems, so no two users can be granted access to the system under the same login name and password. User IDs can never be reassigned to another person. All passwords within the DirectusPRO system are encrypted. Password length and complexity, such as the option to require both alphabetical and numeric characters, are system-configurable.

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

Password aging requires users to change their password after a specified period of time (system-configurable).

(c) Following loss management procedures to electronically de-authorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

Users may change their password anytime they believe that the integrity of the password has been violated. Administrators may revoke a user's access at any time or force the user to enter a new password at any time, when necessary to protect the integrity of the system. Customers should also have Standard Operating Procedures related to loss management procedures.

(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.

All records of system access are maintained in the login history list within the DirectusPRO database. This information includes the user to whom access is being granted (username), login time of access, source IP address of the computer where access occurred, the login type for which access is being granted, the success of the login attempt, the browser program used for access to the application and the computer platform used for access.

All records of access violation are maintained in the DirectusPRO database and may be displayed online. The system administrator also has access to audit reports that logs all records of access violation.

(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.

DirectusPRO periodically performs internal security assessments to perform an application vulnerability assessment after each major release. These assessments include tests on authentication infrastructure to ensure there are no vulnerabilities. Customers should also consider implementing best practices such as IP address restriction, etc.
