Ensuring 21 CFR Part 11 Compliance with NIV-DAS

21 CFR Part 11 is a regulation issued by the U.S. Food and Drug Administration (FDA) that establishes the criteria under which electronic records and electronic signatures are considered trustworthy, reliable, and equivalent to paper records and handwritten signatures.

It applies to organizations in regulated industries, such as pharmaceuticals, biotechnology, and medical devices, that choose to use electronic systems to meet FDA record-keeping requirements. The regulation focuses on ensuring the integrity, authenticity, and security of electronic records while providing a framework for the use of electronic signatures.

Key components include audit trails, user access controls, and validation of electronic systems, all of which are essential for maintaining compliance and ensuring data reliability in FDA-regulated activities.

This white paper has been created to demonstrate how NIV-DAS software aligns with the requirements of 21 CFR Part 11. It provides a comprehensive, rule-by-rule analysis to showcase the software's compliance with the regulation's standards for electronic records and electronic signatures.

By detailing each relevant requirement alongside NIV-DAS's technical capabilities and features, this document aims to offer a clear understanding of how the software supports regulatory compliance in FDA-regulated environments.

Wherever "Nihaar" is referenced in this document, it will refer to Nihaar Equipment Private Limited.

Wherever "Customer" is referenced in this document, it will refer to Nihaar Equipment Private Limited's customer.

Wherever "NIV-DAS" is referenced in this document, it will refer to Nihaar Intelligent Virtual Data Acquisition System.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Yes	Both	NIV-DAS Software has been internally validated. Upon deployment in the customer's environment, it is the customer's responsibility to perform validation in accordance with GxP and Part 11 regulatory requirements.
21 CFR Part 11, 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.	Yes	Both	NIV-DAS Software offers the following report types: 1. Data Reports 2. Audit Trail Reports These reports are available in both human-readable and electronic formats. It is the customer's responsibility to ensure that the records generated comply with the necessary requirements based on their intended use.
21 CFR Part 11, 11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Yes	Both	NIV-DAS software retrieves data directly from the SQL database without any modifications. It is the customer's responsibility to ensure that access to these databases is restricted to authorized personnel. While NIV-DAS software includes backup and restore functionalities, the archiving of database files remains the customer's responsibility.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 11.10 (d)	Limiting system access to authorized individuals.	Yes	Both	NIV-DAS software ensures system security through user and group-based access controls. Access to the system is managed using unique usernames and passwords. It is the customer's responsibility to implement and maintain access controls. The customer's system administrator assigns accounts with unique login credentials, combining the user's identity and role to determine appropriate access and privileges within the system.
21 CFR Part 11, 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.	Yes	Both	NIV-DAS software maintains an audit trail for all relevant user actions that result in data changes, generating secure, immutable, and time-stamped records of events. The software does not permit the deletion of electronic records. Users can generate Audit Trail reports detailing user activity directly through the NIV-DAS software. However, the responsibility for exporting and archiving audit trail data lies with the customer. Additionally, customers should periodically verify the system's date and time settings during validation or qualification processes or as specified by a standard operating procedure (SOP).

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Yes	Both	NIV-DAS software enforces permitted sequences of steps and events associated with users, equipment, and the system to ensure compliance and operational integrity.
21 CFR Part 11, 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.	Yes	Both	NIV-DAS software offers technical capabilities for performing security checks; however, it is the customer's responsibility to establish procedures to enforce these measures. Additionally, the customer is responsible for defining the electronic signature associated with records based on their intended use and ensuring proper authorization.
21 CFR Part 11, 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.	Yes	Both	NIV-DAS is designed to access data from equipment via an internal network using a web browser. To use NIVDAS software, the user's laptop or desktop must be connected to the customer's intranet. It is the customer's responsibility to verify devices connected to their internal network as sources of data input. The accuracy and validity of this input should be ensured through established procedural controls or standard operating procedures (SOPs).

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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.	Yes	Customer	Nihaar ensures the qualification of its development and support personnel in accordance with its internal processes. The customer is responsible for ensuring that administrators and users are appropriately qualified as per their own qualification procedures.
21 CFR Part 11, 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.	Yes	Customer	The customer is responsible for implementation in accordance with their established procedural controls or standard operating procedures (SOPs).
21 CFR Part 11, 11.10 (k)(1)	Use of appropriate controls over systems documentation including: Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	Yes	Customer	Nihaar maintains the system-related development documentation in a document control system with required access control. The customer is responsible to maintain their validation and other operating documentation per their procedure.
21 CFR Part 11, 11.10 (k)(2)	Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	Yes	Customer	Nihaar maintains the system documentation through a change control process and version control. The customer is responsible for maintaining their operating documents and validation documents with an established change control process.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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.	No	N/A	Remark: Section 11.30 requirement for open systems does not apply to closed system such as NIV-DAS software.
21 CFR Part 11, 11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: (1) The printed name of the signer; (2) The date and time when the signature was executed; and (3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	Yes	Both	NIV-DAS software includes technical features to capture all relevant information associated with signed electronic records. The customer is responsible for defining the use of electronic signatures for these records based on their intended purpose. Additionally, the customer is responsible for verifying and validating these requirements to ensure compliance.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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).	Yes	Both	NIV-DAS software provides technical features to capture the required information. It is the customer's responsibility to define the use of electronic signatures for records based on their intended purpose. The customer is also responsible for verifying and validating these requirements to ensure compliance.
21 CFR Part 11, 11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Yes	Both	Each electronic signature applied to an event is unique, making it virtually impossible to remove, replicate, or transfer the signature using conventional methods. The customer is responsible for determining the applicability of this system for electronic signatures on records based on their intended use.
21 CFR Part 11, 11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Yes	Both	A unique username and password combination is required for electronic signatures. It is the responsibility of the customer to provide each individual user with a unique username to ensure that it is not reused by, or reassigned to, anyone else. The customer is responsible to determine the use of this system for electronic signature for record based on their intended use.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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.	Yes	Customer	Customer Responsibility
21 CFR Part 11, 11.100 (c) (1)	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. 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.	Yes	Customer	Customer Responsibility
21 CFR Part 11, 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.	Yes	Customer	Customer Responsibility

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 11.200 (a) (1)	Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password. (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.	Yes	Nihaar Equipment	NIV-DAS software has technical features for this. For all executions of electronic signatures, username is prepopulated for the logged in user and non-editable. The user need only re-enter the correct password each time whether it is the first execution of the e-signature or consequent executions in the same user session.
21 CFR Part 11, 11.200 (a) (2)	Be used only by their genuine owners; and	Yes	Customer	The customer is responsible to assign access to the correct users and control the user access implementation. The customer is responsible to determine the use of an electronic signature for the record based on their intended use. The customer is responsible to verify and validate these requirements.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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.	Yes	Customer	Remark: The customer is responsible to implement this control. The customer is responsible to determine the use of an electronic signature for the record based on their intended use. The customer is responsible to verify and validate those requirements.
21 CFR Part 11, 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.	No	N/A	Remark: Electronic signature based on biometrics is not provided by NIV-DAS software or Modbus.
21 CFR Part 11, 11.300 (a)	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: Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Yes	Both	The “identification codes” are usernames in NIV-DAS software and are unique to the logged in user. The customer to ensure that no two individuals are given the same combinations (username and password). The customer is responsible to determine the use of an electronic signature for the record based on their intended use.
21 CFR Part 11, 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).	Yes	Both	NIV-DAS software features built-in password expiry, requiring users to update passwords periodically. The customer is responsible for configuring the password change interval according to their security policies.

Source	Control	Applicable	Responsibility	Implementation
21 CFR Part 11, 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.	Yes	Customer	NIV-DAS software enables the customer to administrate their own users, this includes disabling users. No tokens, cards, or other devices are provided as part of the system. The customer is responsible to implement this requirement based on the intended use.
21 CFR Part 11, 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.	Yes	Both	NIV-DAS software automatically locks user accounts after three consecutive unsuccessful login attempts. The customer is responsible to implement the following: (this is not a complete list; the customer to identify any additional implementation to meet this requirement): • Password management • Prevention of unauthorized use of password.
21 CFR Part 11, 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.	No	Customer	The customer is responsible for validating end-user devices. User authentication in NIV-DAS software is managed through its internal user and group policy framework.

This white paper summarizes how NIV-DAS software supports customers in meeting the FDA's 21 CFR Part 11 regulatory requirements.

While the software simplifies compliance efforts, ultimate accountability lies with customers to validate their systems based on their intended use. Achieving full compliance with 21 CFR Part 11 depends on the customer's specific applications and responsibilities.

Additionally, customers are required to establish and implement documented operational processes in key areas such as data archiving, business continuity planning, and other relevant procedures to ensure comprehensive compliance.

Disclaimer:

We provide information and guidance to our customers on regulatory matters to the best of our knowledge and ability; however, this is offered without obligation or liability. Customers are solely responsible for observing all applicable laws and regulations. Our advice and information do not absolve customers of their responsibility to ensure compliance with relevant regulations and to verify the suitability of our products for their intended purposes.

We make no warranties, express or implied, including but not limited to implied warranties of merchantability or fitness for a particular purpose, regarding any technical assistance or information provided. Suggestions related to the use, selection, application, or suitability of our products should not be interpreted as an express or implied warranty unless expressly confirmed in writing by an authorized representative of our company.

We shall not be liable for any incidental, consequential, indirect, exemplary, or special damages arising from the use or failure of our products or services. The rights and obligations of the parties are governed by the applicable agreement in place between them or, in the absence of such an agreement, by our standard Terms and Conditions of Sale.