CFR21 Software Statement

NPOS Version 4.0

Paragraph	Summary	Features
11.10 Controls for closed systems		
11.10 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	Controls for closed systems	The NanoPhotometer® Software NPOS 4.0 contains the optional CFR21 feature. Once this CFR21 feature is activated all these requirements are fulfilled.
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	System validation	The complete NanoPhotometer® Software NPOS 4.0 is validated by Implen to ensure accurate, reliable and intended performance of all the components of the NanoPhotometer® system. IQ/OQ procedures for proper function of the NanoPhotometer® instrument can be put in place. The proprietary file format IDS is protected by hash codes and encryption to allow identification of altered files.
(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.	Record generation and copying	In addition to the protected IDS files, all relevant measurement parameters and results can be exported to PDF using the PDF/A standard as well as Excel file format.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Record protection	Every export is accompanied with an IDS file, which is protected by hash codes and encryption to allow detection of tampering. At any time, PDF and Excel reports can be regenerated from these IDS files. Security measures for storage of these reports lie within the responsibility of the operating company.
(d) Limiting system access to authorized individuals.	Access limitation	Before any use of the system, every user is required to login for system access. Each user has a defined role, including access privileges.
(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.	Audit trails	Time-stamped audit trails are recorded for actions performed on the instrument by the user such as file storage, transfer activities and preference changes. The audit trails can be exported in PDF format. The creation and signature of the report files also creates an audit trail report entry. Reports cannot be overwritten.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Operational system checks	Not applicable.
(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.	Authority checks	It is ensured that users have the proper authority to carry out particular functions based on their roles and access privileges. It is the responsibility of the operating company to ensure that each user name can be traced to a real individual and to ensure correct assignment of roles.

Paragraph	Summary	Features
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Device/ terminal checks	Checks are applied to allow only valid information input in respective files. All CSV and JSON input files are checked to ensure valid content.
(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.	Training and user accountability	Implen staff is fully and continuously trained. Implen provides NanoPhotometer® Software user trainings. The operating company is responsible for training on their SOPs in regard to electronic records and electronic signatures. Implen supports the installation of these SOPs in relation to NanoPhotometer® Software.
(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.	Policies	Responsibility of the operating company.
(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.	System Document Control	A release-specific software manual is distributed together with the NanoPhotometer® Software. NanoPhotometer® Software development is governed by a design and change control process that ensures the creation and tracking of relevant documents.
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.		Not applicable. The NanoPhotometer® operates as a closed system.
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.	Signature manifestations	The user management ensures that all user IDs are unique. (1) The system verifies the user credentials before creating any report (the user is required to re-enter his/her user ID and password). The protected IDS file as well as PDF and Excel files contain the user ID and the full name of the user. (2) The date & time when the signature was executed is associated with the signature. (3) The signature for creating the initial reports including the protected IDS file is indicated as "Author" as reason for signature. The signature for (re-)creating reports in PDF and Excel format are indicated as "Read/Save/Print" as reason for signature.

Paragraph	Summary	Features
(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).	Signature in electronic records and in human readable form	User's full name, date and time are included within the IDS file, which is protected by hash codes and encryption. When generating the human readable PDF and Excel files, the electronic signature is displayed with user ID, user's full name, date & time, and reason.
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.	Signature/ record linking	The signature is integrated in the IDS file and can therefore not be excised, transferred or copied.
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.	Uniqueness of electronic signatures	The user management system ensures that all user IDs are unique. Therefore, all electronic signatures are unique.
(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.	Verification of identity	It is the responsibility of the operating company to ensure the identity of the individual at the time of creating the individual's user account.
(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 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. (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.	Certification	Responsibility of the operating company
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.	Controls for electronic signatures	Users are requested to enter user ID and password for every signature action. In order to have access to a signature action, the user must have a user ID in the user management system and must be logged in with user ID 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.		

Paragraph	Summary	Features
(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. (2) Be used only by their genuine owners; and (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.		
(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.		Not applicable
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.	Uniqueness of ID/ password	The user management system ensures unique user IDs.
(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	The user management system provides password expiration and account locking after several authentication failures. Criteria can be set individually by the operating company.
(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.	Lost ID/ password management	The user management system allows an administrator to assign a new temporary password in case of lost, stolen or missing passwords. Proper loss management procedures are the responsibility of the operating company.
(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.	Controls to prevent unauthorized credential use	NPOS with activated CFR21 feature will lock the screen after an inactive period of time to prevent unauthorized attempted use. Other transaction safeguards such as supervision of blocked accounts etc. lies within the responsibility of the operating company.
(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.	Periodic testing of ID/ password generation	Responsibility of the operating company.

Features and specifications are subject to change without notice.

Important Notice: In accordance with FDA regulation, a vendor cannot claim that its software products are certified 21 CFR Part 11 compliant. A vendor, instead, can provide all Technical Controls for 21 CFR Part 11 compliance built into their product. As such Implen does not, at any time, imply that the use of any Implen CFR21 product will automatically give the customer protection to and therefore compliance with 21 CFR Part 11. It is the responsibility of the user to implement the Procedural and Administrative Controls (both correctly and consistently) along with using products with the correct Technical Controls for overall Part 11 compliance. All CFR21 systems must therefore be independently audited.