IKA

designed for scientists

Labworldsoft 6

/// FDA 21 CFR Part 11

www.ika.com/LWS6

IKA

designed for scientists

Sub Part B - Electronic Records

11.10 Controls for Closed Systems

Section	Requirement	Implementation in Labworldsoft
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	Labworldsoft 6 was designed as open system. It is possible to use Labworldsoft as closed system as well.
11.10a	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Based on the used purpose of Labworldsoft and the individual processes, customers are responsible for validating and following established company policies and procedures. IKA does not provide any documentation for software validation. Validate the computer system, following your organizations defined procedures for validation. **Responsibility of the user**
11.10b	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.	Records are saved as PDF/A (ISO 19005) and XLSX. It is possible to create accurate and complete copies of these electronic records in a human readable form for reviewing and printing.
11.10c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records are saved in a database on a server which is protected from access by users. The records are protected as well and cannot be manipulated. Data stored within computer systems should be protected throughout the full record retention period. During this period, electronic records should be able to be accessed or retrieved within a reasonable period of time. Organizations need to plan for such common contingencies as hard drive or server failure.

IKA

designed for scientists

Section	Requirement	Implementation in Labworldsoft
11.10d	Limiting system access to authorized individuals.	Only users with valid and individual login information (user name and password) have access to the system. The login will be blocked after a defined amount of unsuccessful login attempts. Only administrators can unblock the access again. Only Administrators can create, update or delete users. The password has to be changed after a defined amount of days.
11.10e	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.	All process relevant changes are documented with an audit trail. Those audit trails are user specific and accurate to the second of every process change. The audit trails are saved together with all relevant process data in an electronic and human readable form. System access is logged in an audit trail as well.
11.10f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Customers need to define standard operating procedures (SOP) that describe their processes. Processes are specified by user configurations. **Responsibility of the user**
11.10g	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.	Login to the system is only possible entering a valid user name and a matching password. The user is logged out automatically after a defined time, if the user is inactive, to prevent an unauthorized access while the running process is unaffected.
11.10h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Users see their own entered input values. The system does input checks where it is required. It is possible to use an additional confirmation of user inputs. Users have to confirm entered inputs. Errors like connection loss are logged.

IKA

designed for scientists

Section	Requirement	Implementation in Labworldsoft
11.10i	Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Persons who develop the electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks. The end users have to make sure that persons who work with the system have the needed education and training as well. **Responsibility of the user**
11.10j	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.	There should be policies defined by the company that clearly state that the electronic signing is the equivalent of a person's handwritten signature and that all responsibilities that apply to handwritten signatures also apply to electronic signatures. **Responsibility of the user**
11.10k	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.	The procedures and other documentation for system operation and maintenance must be controlled. An organization needs policies for creating compliant documentation and making changes to that documentation. All expired versions of SOPs or other compliant documentation should be retained for future regulatory review. All computer systems require a procedure describing the operation, maintenance, security, and administration for the system. **Responsibility of the user**

11.30 Controls for Open Systems

11.30	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.	Labworldsoft has to be used as closed system. The software provides options for mandatory login. Login has to be required for each user. Setting up Labworldsoft 6 as closed system is **the Responsibility of the user**

IKA

designed for scientists

11.50 Signature Manifestations

Section	Requirement	Implementation in Labworldsoft
11.50	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. (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).	All signed electronic records are linked with electronic signatures which contain the following information: › The name of the signer › The date and time when the signature was executed › The meaning (such as review, approval, responsibility, or authorship) associated with the signature › An optional comment entered by the user

11.70 Signature / Record / Linking

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.	The system does not use handwritten signatures. If electronic and handwritten signatures are used in parallel by the end users they have to makes sure that this requirement is fulfilled. **Responsibility of the user**

IKA

designed for scientists

Sub Part C - Electronic Signatures

11.100 General Requirements

Section	Requirement	Implementation in Labworldsoft
11.100a	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Each electronic signature is unique in the system. A signature is assigned to an individual person and cannot be used by other users (not even administrators).
11.100b	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.	The organization who uses the system has to verify the identity of each individual that uses electronic signatures. Responsibility of the user
11.100c	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 s	End users who are using a CFR 21 Part 11 related system, have to certify to the FDA that the electronic signatures in their system are intended to be the legally binding equivalent of traditional handwritten signatures. End users have to make sure that the requirements given by the FDA are fulfilled. **Responsibility of the user**

IKA

designed for scientists

11.200 Electronic Signature Components and Controls

Section	Requirement	Implementation in Labworldsoft
11.200a	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. (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.	The electronic signatures are not based on biometrics. This is why two distinct identification components (user name and password) are used to access the system functionalities. Users can change their own passwords. Passwords are saved encrypted and cannot be read by another person. The system makes sure that passwords have a minimum length and contain special characters to improve the security of user passwords. A user will be logged out after a defined period of inactivity. The number of unsuccessful login attempts is limited. The user account will be disabled after too many unsuccessful login attempts.
11.200b	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Electronic signatures of the system are not based on biometric. **Not relevant**

IKA

designed for scientists

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:

Section	Requirement	Implementation in Labworldsoft
11.300a	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Each user account is unique in the system and can only be used once. The user management does not allow to create a user with an already existing user name.
11.300b	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The password of a user has to be changed every 90 days. The latest password cannot be used again. In case users cannot remember their password, administrators can reset the password individually.
11.300c	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.	The system does not use authentication chips or cards. **Not relevant** Passwords can be reset by administrators if forgotten. The account holder should then immediately define a new password afterwards. Compromised accounts can be disabled.
11.300d	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.	A user account is automatically deactivated after 3 consecutive unsuccessful login attempts. After deactivation the user account can only be reactivated by an administrator. A user account can be manually deactivated and reactivated by an administrator as well. All successful and unsuccessful login attempts are automatically logged in the audit trail. An inactive user will be logged out after a configurable defined period.
11.300e	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.	The system does not use chips, cards or other hardware for user authentication. Not relevant