Bioreset® Plus 21 CFR

Managing data security in accordance with FDA 21 CFR Part 11 is no more a challenge. Bioreset Plus 21 CFR is equipped with the software designed to comply with the most stringent requirements to ensure traceability and integrity of archived data.

USER-FRIENDLY

Intuitive and easy to use: the operator can simply interact with the machine for set up and process.

HIGH-TECH DESIGN AND KNOW-HOW "MADE IN ITALY"

Our engineering team, based on field expertise and continuous R&D activity, designed it to meet customers' needs and with great attention to graphic layout.

AUTOMATIC PROCESS

Possibility to automatically configure and adjust the process thanks to the feedback of the integrated T/RH probe.

REPORT IN REAL TIME

Possibility to export reports in pdf format or print them on a network device to get immediate visibility of the processes outcome.

HIGHLIGTHS

- Protection of records to enable their accurate and retrieval readiness throughout the records retention period
- System access regulated by different authorization levels ensuring that only authorized individuals can operate in specific area
- Management of automatic log out, automatic lock out and password expiration date processes
- Use of secure, computer generated, time-stamped audit trails
- Management of electronic signature for the report.
- Possibility to generate protected back up on PC or remote server

amira Simply ahead.

COMPLIANCE MATRIX FOR 21 CFR PART 11

Electronic records			
Section Number	21 CFR part 11 Requirement	Compliant	Comments
11.10	Persons who employ closed systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity . . . of electronic records.	☑	Bioreset software is a closed system. All data records are protected and unmodifiable.
11.10 (a)	Validation of systems to ensure accuracy, reliability consistent intended performance and the ability to discern invalid or altered records.	☑	IQ/OQ/PQ are avaiable for every Bioreset instrument. All records are stored in a secure database inside instrument memory.
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 FDA.	☑	Reports can be printed directly when Bioreset is connected to a printer or exported as PDF file to be copied and reviewed.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	☑	Data records are saved to an encrypted and password protected database. The database can be downloaded to ensure a safe backup on any computer. Any report of the database can always be converted in PDF through proprietary Bioreset software.
11.10 (d)	Limiting access to authorized individuals.	☑	The access to Bioreset software requires unique username and password. Accounts privileges are settable so that each user only has access to part of the software according with client organization chart.
11.10 (e)	Use secure computer-generated, time-stamped audit trails to independently record the date and time of operator entries and action that create, modify or delete electronics 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.	☑	It is impossible to modify or delete any report. All reports will always be in the original form. Any action is registered and traced into an audit trail file stored into the unit. This document is saved in an encrypted and password protected database. The database can be downloaded to ensure a safe backup on any computer.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	☑	Once SOP is created on the instrument, the operator shall only select it and start the cycle.
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 records or perform the operation at hand.	☑	Complexity criteria for password can be set by administrator. Automatic lock-out from software occurs after an administrator-defined non-use period. Access is controlled by user authentication (User Id and Password). Unique combinations of user id and passwords are enforced by the Bioreset security system. Passwords can be set to expire after a period of time by an administrator. All input devices such as probes have a proprietary connections that assure only Bioreset devices can be connected.
11.10 (h)	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of data input or operational instruction.	☑	Every device can be yearly calibrated to assure the correct performance of the overall equipment.
11.10 (i)	Determination that persons who develop, maintain, use electronic record/electronic signature systems have education, training and experience to perform their assigned tasks.	**NOT APPLICABLE!**	Not applicable! Client is responsible for this part; Amira provides courses for instrument operational training.

Section Number	21 CFR part 11 Requirement	Compliant	Comments
11.10 (j)	The establishment of and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronics signatures, in order to deter record and signature falsification.	NOT APPLICABLE!	Not applicable! Client must establish SOPs and other written policies to deter falsification or fraudulent uses.
11.10 (k1)	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.	☑	Every Bioreset comes with electronic and printed manual describing all functions of the instrument.
11.10 (k2)	Use of appropriate controls over systems documentation including: Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	☑	Software contains version information that can be incorporated into client's documentation.
11.30	Persons who employ open systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure authenticity, integrity . . . of electronic records from the point of their control to the point of their receipt. Such procedures and controls shall include those identified in 11.10 . . . and use appropriate digital signature standards to ensure . . . record authenticity, integrity and confidentiality.	NOT APPLICABLE!	Not applicable! Bioreset software is a closed software. Records can only be opened or generated through Bioreset software.

Electronic signature

Section Number	21 CFR part 11 Requirement	Compliant	Comments
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all of the following: Printed name of signer; Date and time when signature was executed; and the meaning (such as review, approval, responsibility or authorship) associated with the signature.	☑	Bioreset software security system provides all relevant informations regarding the electronic signature, registered on the report and in the audit trail.
11.50 (b)	The items identified in 11.50 (a) 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 display or printout).	☑	Digital signatures are embedded within the electronic record and are included as part of the human-readable, on-screen and printed forms of the electronic record.
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 be transferred to falsify an electronic record by ordinary means.	☑	Digital signature is stored with each data record signed. Bioreset data records that are stored cannot be altered.
11100	(a) Each electronic signature shall be unique to one individual and shall not be reused, or reassigned to anyone else. (b) Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, or any element of such signature the organization shall verify the identity of the individual. (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.	☑	It is required by client to establish a unique user name and password and privileges in Bioreset software. The Bioreset security system setup procedure enforces unique user id and password combinations. Log-in failures include lock-out of user accounts. Only designated administrators can unlock the user. Reasons for a lockout are provided by the security system to the administrator. Client is responsible to comply with Parts (b) and (c).

Section Number	21 CFR part 11 Requirement	Compliant	Comments
11.200 (a1)	Electronic signatures 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.	☑	The Bioreset security system setup procedure enforces unique user ID, password and user PID (personal ID code) combinations for each user account. Every electronic signature requires user ID, PID and Password when signing.
11.200 (a2)	2. Be used only by their genuine owner.	**NOT APPLICABLE!**	Not applicable! Client is responsible for his employees.
11.200 (a3)	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.	**NOT APPLICABLE!**	Not applicable! Client is responsible for his employees.
11.200 (b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used anyone other than their genuine owners.	**NOT APPLICABLE!**	Not applicable!
11.300 (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.	☑	Every electronic signature requires user ID, PID and Password when signing. Unique combinations of user id and passwords are enforced by the Bioreset security system.
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g., to cover events as password aging).	☑	Passwords can be set to expire after a period of time by an administrator.
11.300 (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.	**NOT APPLICABLE!**	Not applicable!
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.	☑	Log-in failures and electronic signature failures include lock-out of user accounts. Only designated administrators can unlock the user. Reasons for a lockout are provided by the security system to the administrator.
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.	**NOT APPLICABLE!**	Not applicable!