Support for 21 CFR Part 11 Compliance

Product: BWID® Software for B&W Tek portable Raman Systems

21 CFR Part 11 titled "Electronic Records and Electronic Signatures" March 20, 1997
"Guidance for Industry Part 11 Electronic Records and Electronic Signatures – Scope and Application" August 2003

In March of 1997, the US FDA issued 21 CFR Part 11 regulations that provide criteria for acceptance by FDA, under certain circumstances, of electronic records, electronic signatures, and handwritten signatures executed to electronic records as equivalent to paper records and handwritten signatures executed on paper. These regulations apply to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in FDA regulations. The regulation is meant to prevent abuse, falsification, or inadvertent corruption of electronic data. Guidance on Electronic Records and Electronic Signatures published by the FDA in August 2003 clarify the scope and application of 21 CFR Part 11 with a narrower interpretation than adopted in 1997. 21 CFR Part 11 sets forth guidelines that relate to records that are required to be maintained under predicate rule requirements and that are maintained in electronic format

- in place of paper format
- in addition to paper format, and that are relied on to perform regulated activities.

21 CFR Part 11 is also applicable to electronic signatures that are intended to be the equivalent of handwritten signatures, initials, and other general signings required by predicate rules.

B&W Tek's implementation of procedures complying with these requirements include the appropriate administrative controls to ensure that persons who develop, maintain, or use electronic records and signature systems have the education, training, and experience to perform their assigned tasks. In addition, compliance with 21 CFR Part 11 requires designing and embedding appropriate technical controls in the instrumentation to ensure the integrity of system operations and information stored in the system as well as maintaining appropriate audit trails and producing copies of records held in common portable formats.

In summary 21 CFR Part 11 applies to:

- Validation of computerized systems
- Content integrity
- Use of electronic signatures for authentication of electronic documents
- Audit trails for all records/signatures
- Copies of records
- Record retention

19 Shea Way, Newark, DE 19713, USA
Tel: +1 (302) 368-7824 Fax: +1 (302) 368-7830
Web: http://www.bwtek.com

The US FDA will enforce the following provisions within the scope of 21 CFR Part 11

- limiting system access to authorized individuals
- use of operational system checks
- use of authority checks
- use of device checks
- determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks
- establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures
- appropriate controls over systems documentation
- controls for open systems corresponding to controls for closed systems bulleted above (§11.30)
- requirements related to electronic signatures (e.g., §§ 11.50, 11.70, 11.100, 11.200, and 11.300)

The sections that follow provide a concise summary of relevant sections of 21 CFR Part 11, and the company's interpretation and solutions addressing these core requirements as applicable to B&W Tek **BWID® Software for B&W Tek Instrumentation and Systems**. In the following requirements assessment, applicable 21 CFR Part 11 sections are indicated in italics and the corresponding solutions follow. This summary is for information purposes only, and is by no means comprehensive.

Please contact a B&W Tek representative if further detail is required.

Requirements Assessment:

Note: B&W Tek will keep this documentation up-to-date, and control its distribution over the different software/hardware releases.

Definition: § 11.3 (4) *Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*
BWID Compliance: In order to use the software users must first be granted a user profile with appropriate level of access as determined by the system administrator. It is our interpretation that the spectrometer is a closed system under this definition.

Requirement: § 11.10 (a) *Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.*
BWID Compliance:
It is the customer's responsibility to develop appropriate validation protocols for the system. However, B&W Tek offers services including documentation to support and assist with installation and operational qualification, performance qualification and method validation.

Within BWID, functionalities are provided that automatically verify the instrument performance. Reference materials are available from B&W Tek.

Requirement: § 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.*
BWID Compliance: BWID provides complete functionality for locating and viewing the electronic records on the system, and for generating complete, accurate paper and electronic copies for agency submissions. BWID uses database files to store its records, and the database files are encrypted to prevent unauthorized access. The electronic format of records can be read in BWID and can be exported as pdf files and/or printed. Printed copies include time/date stamps to facilitate traceability of paper documents. It is the customer's responsibility to assure that exported and printed records are accessed, approved and controlled as appropriate to their internal SOP for Records Control and Retention.

Requirement: § 11.10 (c) *Protection of records to enable their accurate and ready retrieval throughout the records retention period.*
BWID Compliance: BWID provides several layers of protection to ensure that accurate records can be readily retrieved. The foundation for record protection is a secure operating system that provides positive user tracking and prevents unauthorized access to computers and files. B&W Tek recommends the use of Microsoft Windows 7, and higher versions of operating system.

The next level of protection is provided by a secure relational database system. All records stored in the BWID database can only be accessed via the BWID software, therefore are protected from unauthorized access.

The third level of protection is afforded by the security features built in BWID itself. These include controlled access to BWID by means of user names and passwords; controlled access to various functionalities according to different levels of user privileges; retention of raw measurement data and parameters with all measurement records; protection of records from alteration or deletion; and software generated audit trails to record all actions affecting the electronic records.

The software will record each spectrum together with all acquisition parameters and audit trails in the encrypted database. Through data encryption, B&W Tek guarantees the security of the data.

No data manipulation is possible within BWID software.

Requirement: § 11.10 (d) *Limiting system access to authorized individuals.*
BWID Compliance: User profiles must be granted by the system administrator before a user has access to the software. User access to all functions is restricted by user names and passwords. The customer should assure that pertinent administrative/procedural controls are in place to restrict physical access to the system when not in use. Administrators can manage User's profiles, create new profiles, reset

passwords and change access level using the BWID Software. In the software Administrators can add Administrators, Developers or Operators/Users.

Requirement: § 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 is required for the subject electronic records and shall be available for agency review and copying.*
BWID Compliance: The software automatically generates audit trails containing all relevant information. Audit trails for measurement records are treated as part of the record themselves, and are synchronized, archived/restored, and retrieved along with the records.
Electronic records and their audit trails cannot be changed once created.

Requirement: § 11.10 (f) *Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.*
BWID Compliance: The software has a strictly enforced workflow and will not allow operation outside of the permitted sequencing of steps. For a detailed description of the permitted workflow, please see the appropriate system user manual.

Requirement: § 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.*
BWID Compliance: The software has three authority levels: operator, developer, and administrator. The user level for each user is set by the system administrator during creation of the corresponding user profile in the system software.

Requirement: § 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.*
BWID Compliance: The software records data input in the electronic record; the validity of that input should be assured by procedures and external measures.

Requirement: § 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.*
BWID Compliance: Enforcement of this requirement should be assured through appropriate administrative control of user system access; however, we offer documented training for all user levels including system administrators, developers, and operators. Additionally, B&W Tek provides complete system documentation, help files and user/administrator guides.

Requirement: § 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.*
BWID Compliance: The establishment and adherence to such policies should be assured by external measures.

Requirement: § 11.10 (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.*
BWID Compliance: The establishment and adherence to such controls should be assured by external measures. The BWID software maintains a system configuration audit trail that documents changes made to the system configuration by developers and administrators. B&W Tek will keep track of the documentation for the different versions and releases of hardware and software and provide release notes detailing changes.

Requirement: § 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.*
BWID Compliance: The electronic signature generated by the software contains information pertinent to when and how the data was collected and by whom. To ensure the identity of the signer, the same password used for login must be entered at time of signing.

Requirement: § 11.50 (b) *The items identified in § 11.50 (a) 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).*
BWID Compliance: The software maintains signature manifestations as described in § 11.50 (a) in the same fashion as for electronic records. .

Requirement: § 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.*
BWID Compliance: The software's electronic signatures or user identification are embedded in the electronic record and cannot be excised or copied.

Requirement: § 11.100 (a) *Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to anyone else.*
BWID Compliance: The software does not allow for duplicate user names to be in use in the same BWID database. User accounts can be disabled from the system (an action which is audited in the system logs), and external documentation and policies should be used to ensure that the same user name is not later assigned to a different individual. Users will have unique user names and passwords.

Requirement: § 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.*
BWID Compliance: The establishment and adherence to such controls should be assured by external measures.

Requirement: § 11.100 (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 legally binding equivalent of traditional handwritten signatures.*
BWID Compliance: The establishment and adherence to such controls should be assured by external measures.

Requirement: § 11.200 (a)(1) *Electronic signatures that are not based upon biometrics shall (1) employ at least two distinct ID components, such as identification code and password.*
BWID Compliance: The software employs a user name and password as identification components.

Requirement: § 11.200 (a)(1)(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.*
BWID Compliance: To electronically sign a record, BWID requires a user name and password for the initial system login, and the user must re-enter the same password at every subsequent signing. The software does not allow another user to sign a record until the current user is logged out and the other user is logged in.

Requirement: § 11.200 (a)(1)(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.*
BWID Compliance: The software requires both a user name and a password for the initial system login to start a continuous period of controlled system access to execute signing.

Requirement: § 11.200 (a)(2) *Electronic signatures that are not based upon biometrics shall be used only by their genuine owners.*
BWID Compliance: The establishment and adherence to such controls should be assured through external measures and controls by the customer.

Requirement: § 11.200 (a)(3) *Electronic signatures that are not based upon biometrics shall be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than it's genuine owner requires collaboration of two or more individuals.*
BWID Compliance: The software supports electronic signatures for a user that are a single user name and password combination. System access is restricted unless an appropriate user name/password

combination is selected. Should a user forget their password, the system administrator can reset the password.

Requirement: § 11.300 *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.
b) Ensuring that identification and password issuances are periodically checked, recalled, or revised.
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.
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.
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.

BWID Compliance:

a) The software does not allow duplicate user names (identification code) for different individuals on the same unit.
b) The software allows for passwords to be periodically recalled or revised by a password aging feature.
c) The system administrator has the ability to deactivate user accounts as necessary.
d) The software records all login attempts in audit logs for administrator audit.
e) The software has no reliance on tokens or cards.

Approval History

Version A:	**CO Number: 650004303**
	CO Initiator: Thomas Zawislak
	Description of Change: Initial release January 13, 2020
Version B:	
Version C:	

Department Manager: Philip Zhou	**Title:** Software Product Manager	**Signature:**	**Date:** 01/13/2020
QA: Thomas Zawislak	**Title:** General Manager	**Signature:**	**Date:** 01/13/2020