21CFR PART11

INTERPRETATION AND IMPLEMENTATION

IN

BL STUDIO (VERSION 1.04.02)

Revision History

Date	Version	Description	Author
30.04.2013	1.00	Created	Peter Senne
03.05.2013	1.01	Added BL Studio Version	Peter Senne
01.04.2015	1.02	Updated for BLStudion 1.04.02	Peter Senne
25.06.2015	1.03	Modified 11.10(g)	Peter Senne

1. Contents

2. Introduction

Achieving compliance with the CFR is best accomplished by a partnership between the user and the vendor. The user knows how they want the system to fit into their Quality Management System (QMS) and operate on a day-to-day basis in their organization. The vendor knows how the system supports compliance within its functionality. The partnership usually consists of the vendor supplying the technical means of becoming compliant and the user adding the procedural means to compliance via working practices, standard operating procedures and fit to their QMS.

The basic version of BL Studio is intended to be used in a research environment, where full and flexible access to all methods and data is important. Nevertheless, BL Studio offers a basic set of functionality to support 21CFR Part 11. The purpose of this document is to allow users of BL Studio to determine how functionality within the software supports the technical requirements for 21CFR Part 11. Still, there are several areas where standard operating procedures are needed to achieve compliance. The document is divided into three sections;

· Subpart A, General provisions
· Subpart B, Electronic Records (11.10, 11.30, 11.50 and 11.70)
· Subpart C, Electronic Signatures (11.100, 11.200 and 11.300)

Subpart A is included for background information only and shows the text as detailed in the 21CFR part 11 document. Subpart A contains the definitions used in the act.
Subparts B and C contain two columns. The column headed ‘21CFR Part 11’ including the text taken directly from the 21CFR Part 11 document for that section. The column titled ‘BLStudio’ details if and how the software or the customer meets the CFR technical requirements.

3. System Security

BL Studio functions on Microsoft Windows XP, Windows Vista and Windows 7. Operating under Windows allows the system to use the operating system to increase electronic record security by using the file security facilities within Windows. In addition to the file security, it is recommended that the Windows Administrator secure the appropriate folders using Windows permissions to prevent overwriting and accidental deletion of data. We also recommend that each user is set-up to use the password protected screen saver utility within Windows, with an appropriate time-delay set, to protect the system from unauthorized use during a period of inactivity.

4. BL Studio (Basic Version) vs. 21 CFR Part 11

4.1. 21 CFR Part 11 SUBPART A – GENERAL PROVISIONS

11.1 **Scope**	
11.1 (a)	The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.
11.1 (b)	This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.
11.1 (c)	Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically expected by regulation(s) effective on or after August 20, 1997.
11.1 (d)	Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.
11.1 (e)	Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.
11.2 **Implementation**	
11.2 (a)	For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.
11.2 (b)	For records submitted to the agency, persons may use electronic records in lieu of traditional signatures, in whole or in part, provide that: 1) The requirements of this part are met; and. 2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must any accompany electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with electronic submission.

11.3 **Definitions**	
11.3 (a)	The definitions and interpretations of terms contained in section 201 of the act apply directly to those terms when used in this part.
11.3 (b)	The following definitions of terms also apply to this part: 1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)). 2) *Agency* means the Food and Drug Administration. 3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable. 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. 5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified. 6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system. 7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature. 8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark. 9) *Open system* means an environment in which system access is not controlled by persons which are responsible for the content of electronic records that are on the system.

4.2. 21 CFR Part 11 SUBPART B – ELECTRONIC RECORDS

	21 CFR Part 11	BL Studio (Basic Version)
11.10 **Controls for closed systems**		
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	All data stored within BL Studio is protected by a checksum function. Only data with a valid checksum is readable by BL Studio. Exported data is NOT checksum protected. As soon as data is exported or printed the customer is responsible for its validity. Access to this data is controlled by user name and secret password.
11.10 (b)	The ability to generate accurate and complete copies of records in both human readable and electronic for 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 a review and copying of the electronic records.	All records are stored All records can be copied On-screen viewing of methods, curves, results and the audit trail are possible.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Data is automatically stored to a file on completion of data collection, when the user stops the measurement or in the event of an error. It is the customer's responsibility to introduce a suitable backup and archiving procedure to protect the data in the event of a total or partial loss due to a catastrophic failure, for example fire.
11.10 (d)	Limiting system access to authorized individuals.	BL Studio offers two login-systems: Secure login via operating system: The customer is responsible to set up an account for each user within the operating system. BL Studio acquires the identity of the current user from the operating system and maps it to a user defined within BL Studio. Login, password storage and encryption, password expiration etc. are handled by the operation system. Convenient login via BL Studio: The identities, names and passwords are defined within BL Studio. The user login is handled by BL Studio. Passwords are encrypted and

		can not be viewed within BL Studio. Passwords do not expire. There is no means to force passwords to have a certain format or length. In both cases every BL Studio user is assigned a unique GUID, which is stored in all electronic signatures. All user information is stored in a binary, checksum protected file: ../System/User/UserInfo.cfg. The customer is responsible to protect this file against deletion
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.	Each entry in the audit trail contains the user Name, a unique user id and a date/time stamp. Whenever a method or result is created or modified through BL Studio a new entry is added to the audit trail, containing the name and an unique id of the method/result. BL Studio does not track changes within records. To ensure record changes are not obscured, records must not be overwritten. It is the customer's responsibility to protect records against deletion on the operating system level. This is the only way to ensure they can not be deleted with other programs (e.g. the file explorer, or the standard file selection dialogue used in BL Studio). The audit trail is stored to checksum protected files on a daily base. The customer is responsible to archive these files.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Responsibility of customer.
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.	On the application level BLStudio performs authority checks, based on user rights.
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.	The serial number of the instrument and the last validation date is stored in all data collected.
11.10 (i)	Determination that persons who develop, maintain, or use electronic record/electronic signature systems	Responsibility of customer

	have the education, training, and experience to perform their assigned tasks.	
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.	Responsibility of customer
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 modifications of systems documentation.	Responsibility of customer Responsibility of customer
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 - Closed system only

11.50 **Signature Manifestations**		
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.	1) The printed name, is the full name of the user i.e. First Name, Middle Initial, Last Name and the User Name. 2) The date and time are included. 3) The current version only supports signatures for the creation of records.
11.50 (b)	The items identified in paragraphs (a) (1), (a) (2) and (a) (3) of this section shall be subjected 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).	Signatures of methods and results can be displayed on reports.
11.70 **Signature/ recording 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.	Signatures are embedded into records and part of the checksum protection.

4.3. 21 CFR Part 11 SUBPART C – ELECTRONIC SIGNATURES

	21 CFR Part 11	BL Studio
11.100 **General Requirements**		
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Customer responsibility (On creation each user is assigned a unique GUID by BL Studio, but this ID is not human readable in the current version)
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.	Responsibility of customer
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 the legally binding equivalent of traditional handwritten signatures. 1) The certification shall be submitted in paper form and signed with a traditional signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857. 2) Persons using electronic signature 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.	Responsibility of customer
11.200 (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. 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	1) BLStudio signatures contain an identification code and a password In the current version creation signatures are supported only. Based on the program login they are added automatically and do not require an additional identification.

	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 collaborations of two or more individuals.	A signature can only be used by its genuine user. The password is not visible to anybody including administrators. It is possible to delete and re-create a user to set a new password. However, during this procedure the unique user GUID is altered.
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.	Electronic signatures based upon biometrics are not supported.
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:	
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.	Responsibility of customer
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).	Supported by the Windows login system, not supported by BL Studio login system.
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.	Devices such as tokens or cards are not supported by BL Studio.
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.	Operating system login: All logins are reported to a login audit log, accessible by Administrator. This report is viewable and printable for inspection purposes. BL Studio login: All logins are recorded in the audit trail.

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.	Devices such as tokens or cards are not supported by BL Studio.

5. REFERENCES

i) Title 21 of the Code of Federal Regulations, Part 11 - "Electronic Records; Electronic Signatures." Released on 20th March 1997 and became effective on 20th August 1997. Reviewed April 1st. 2009