BLUEHILL'S TRACEABILITY MODULE

FDA 21 CFR Part 11 Implementation

INTRODUCTION

Achieving compliance with 21 CFR Part 11 is best accomplished through a partnership between the end user and the original equipment supplier. The end user knows how the laboratory equipment should fit into their Quality Management System and how the laboratory equipment will be used daily. The original equipment manufacturer provides the tools to integrate the equipment effectively and efficiently into the end user's quality management system. By working together, they can ensure that the end user's data meets the guidelines for integrity and traceability as outlined by the FDA.

The purpose of this document is to inform the end user how the Traceability Module within Bluehill Universal or Bluehill Central can help meet thetechnical requirements of FDA 21 CFR Part 11. This document outlines the three key areas in Bluehill (Security, Audit Trail, and Signatures) and provides a row-by-row interpretation of how Bluehill addresses each of the Part 11 items. Ultimately, each end user should perform their own assessment and create appropriate work instructions that cover the Instron system, Bluehill Universal, Bluehill Central, the Windows file systems, and the user's Quality Management system.

SECURITY

A key component of electronic records is the validation and verification of the user performing the operation. To accomplish this, different security types are offered per the table below.

Security types	Bluehill Universal	Bluehill Central
Bluehill	Security profiles, i.e. user accounts, are created and stored in Bluehill Universal on the local computer.	Security profiles, i.e. user accounts, are created in Bluehill Central and stored in the Bluehill Central database. All connected Bluehill Universal or Bluehill Central clients use the shared security configuration.
Windows® Active Directory	Security permissions are based on user groups created on a company's corporate network. Permissions are configured to network user groups from Bluehill Universal on the local computer. Users log in with domain credentials and user groups dictate permissions.	Security permissions are based on user groups created on a company's corporate network. Permissions are configured to network user groups from Bluehill Central, and all connected Bluehill Universal or Bluehill Central clients use the shared security configuration.
Windows®	Security permissions based on user groups configured on the local computer's Windows® operating system. Permissions are configured to local user groups from Bluehill Universal on the local computer. Users log in with windows credentials and the groups dictate permissions.	Not applicable.

Each security model provides similar functionality. First, they authenticate the user with two distinct identification components: a username and a password. Second, once a user is identified, the security model authorizes certain software operations based on the configured security policies. The choice of which security model best suits your organization greatly depends on your assessment of how to integrate Bluehill into your existing Quality Management system.

The following permissions are available within each security model:

Permission	Related Application	
	Bluehill Universal	Bluehill Central
Log in	✔	✔
Configure the system	✔	×
Configure the team	×	✔
Configure security	✔	×
Configure Traceability*	✔	✔
View audit trail*	✔	✔
Group A reviewer (e-signature)*	✔	✔
Group B reviewer (e-signature)*	✔	✔
Group C reviewer (e-signature)*	✔	✔
Manage files and folders*	×	✔
Remove files and folders*	×	✔
Perform a test	✔	×
Edit methods	✔	×
Edit values on tested specimens	✔	×
Delete a tested specimen	✔	×
Change a tested specimen	✔	×
Exclude a tested specimen	✔	×
Change workspace properties	✔	×
Override sample folder location	✔	×
Discard the sample	✔	×
Overwrite an existing sample via Save As	✔	×
Analyze samples*	✔	×

* Only *available if associated add-on is purchased*

In addition, the visibility of items available for data entry can be configured to the user in the test method. This provides an additional layer for security by tightly controlling the values that can be modified by the operator.

SECURITY - BLUEHILL FILES

Bluehill Universal stores information in file format on the local file system, a network drive, or – if purchased - the Bluehill Central database. While Bluehill Universal's security models restricts operations within the application, the application relies on the appropriate PC or network policies to ensure authorized users have the proper folder and file access. It is recommended that the Windows Administrator secure the appropriate folders using folder permissions to prevent malicious or accidental record edits or deletions. When using network locations and with Active Directory, it is recommended that the same user be logged into both the PC account and Bluehill, which will ensure that all file operations are verified against the proper permissions.

Files	Bluehill Files	Recommended security settings	User configurable
Templates	Methods and reports	Read only access for Bluehill users Read/Write for authorized users File deletion for authorized users Default location: C:\Users\Public\Documents\Instron\Bluehill Universal\Templates	Yes
Output files	Samples files, Reports, Export files	Read/Write for Bluehill users File deletion for authorized users Default location: C:\Users\Public\Documents\Instron\Bluehill Universal\Output	Yes
Configuration	Configuration settings	Read/Write for Bluehill users Deny folder read access for all users Deny file deletion for all users Location: C:\ProgramData\Instron\Bluehill Universal\Common Files	No
Audit trail (Locally-hosted Traceability module)	SQL database files	Read/Write for Bluehill users Deny folder read access for all users Deny file deletion for all users Location: C:\ProgramData\Instron\Bluehill Traceability	No

AUDIT TRAIL

Bluehill Universal's Audit Trail captures system events and operations of the following types:

- Login/Logout/Invalid credentials
- Reviews - *signatures*
- Modify
- Create
- File overwrites
- File recovery
- System errors
- Delete - *Bluehill Central only*

For each event, the audit trail captures the following information:

- The event – The operation that triggered an entry to be added to the Audit Trial.
- What – A description of the action being captured.
- Who - Username of who performed the action.
- When – Date and timestamp of the action - captured in UTC and displayed in local PC time zone
- Why – A reason for the action.

AUDIT TRAIL – CHANGE TRACKING

Bluehill Universal Report templates, Method files, and Sample files now capture changes performed by the logged in user. These changes are saved as revision entries both in the file and in the system Audit Trail. Each time the file is saved, the file revision number is incremented, and the list of changes are stored with that revision. Each entry captures the action, affected item, the new value, and the previous value. When possible, these entries capture the changes from the time the file was last saved to the point of save.

Bluehill Universal files contain many settings, some of which are purely cosmetic in nature. Below is a breakdown of which actions are tracked and which are not tracked:

Tracked

- Sample, Method, Report template value changes that affect how the test is run or reported
- Parameter attributes for the values that affect how the test is run or reported
- Adding or removing items in list
- Deleting or excluding a specimen
- Specimen retested
- Reasons for a test being stopped
- Sample created
- Sample recovered
- Security settings
- Traceability settings
- Transducer balance/calibrate

Not tracked

- Show/hide the navigation bar in a Method file
- Display format changes to Results table 1 & 2 and Raw Data viewer
- Graph Advanced tab changes
- Workspace layout changes
- Reordering selected list items
- User preferences
- Hardware configuration settings.

SIGNATURES

Signatures identify which user performed the operation, when, and for what reason. This information is captured electronically in the following file types and linked in the audit trail:

1) Report templates
2) Methods files
3) Sample files
4) PDF reports

Bluehill Universal can be configured for up to three signatures (Primary, Secondary, and Tertiary). The primary signature is the user who is saving the document. The secondary and tertiary signatures represent an acknowledgement of the changes. . The secondary and tertiary signatures are linked to one of three groups (Reviewer Group A, B or C). A document requiring a signature from a specific review group can be performed by any member of that group. Unless the reviewer already provided the primary signature. The number of signatures and associated reviewer groups are configurable to each file type in accordance with your operating procedures. If required, comments and signature order can be enforced.

SECTIONS FROM FDA 21 CFR PART 11

The below text has been taking from FDA 21 CFR Part 11, subparts A, B, and C. Please refer to the references cited on the last page of this document.

SUBPART A – GENERAL PROVISIONS:

	21 CFR Part 11
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 excepted 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.

	21 CFR Part 11
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 paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided 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 accompany any 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 the electronic submission.

	21 CFR Part 11
11.3 Definitions	
11.3 (a)	The definitions and interpretations of terms contained in section 201 of the act apply 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.

11.3 (b) *continued*	(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 who are responsible for the content of electronic records that are on the system.

SUBPART B – ELECTRONIC RECORDS:

11.10 Controls for closed systems		
	21 CFR Part 11	Instron's software application(s)
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	It is the customer's responsibility to develop appropriate validation protocols for the system, however, Instron provides tools and services to assist in the IQ/OQ of the system. Instron's Service group can provide verification of the system to ensure the raw data collected meets performance requirements. Bluehill Universal and Bluehill Central software should be configured using security to ensure that only trained users can access the system. With security, approved users can access the software and run the Instron system after entering their username and password. Bluehill's report template, method, and sample files are XML encrypted and digitally signed. This obscures the human readable content of the file and ensures the integrity of the information. If an unauthorized user opens and changes the contents, Bluehill will notify and prevent the file from being used. In conjunction with this protection, it is recommended to deny the unauthorized user appropriate file permissions to further prevent accidental or malicious changes to these files.
11.10 (b)	The ability to generate accurate and complete copies of records in both human and readable 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 a review and copying of the electronic records.	Bluehill Universal provides users with on screen viewing of results, reports, raw data, file revision history, and the audit trail of the local Instron system. Bluehill Universal also has printing and export utilities for paper or electronic records. Bluehill Central provides users with on screen viewing of file revision history, access to prior file revisions, and the audit trail of all connected Instron systems.
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Bluehill Universal stores template and results data in file format on the local or network Windows® file system. These files can be protected using external file backup programs. Bluehill Universal's locally hosted Traceability module stores audit trail data in a SQL Server Express database on the local computer and can be backed up or restored using built-in functions in Bluehill Universal. Automated backups are not support in Bluehill Universal.

11.10 (c) *continued*		If a Bluehill Universal client is connected to a Bluehill Central database, the template and results files are stored on either a SQL database or the local files system. The database can be backed up or restored using built-in functions. Local files or automated backups can be supported with external applications not provided with Bluehill Universal. Bluehill Central's Traceability module stores audit trail data from all connected Bluehill clients in a SQL Server (or SQL Server Express) database on a single computer. The database can be backed up or restored using built-in functions in the Bluehill Server Configurator. Automated backups are not support in Bluehill Central. In the event of a power failure, Bluehill Universal provides a backup function of the current test data to ensure all available data can be captured. Onrestart of the software, the operator will be prompted to recover the test data.
11.10 (d)	Limiting system access to authorized individuals.	See system security section on page 1. Once security is configured, a unique username and password is required for all authorized users. All access or attempted access to the system is logged in the audit trail. Instron highly recommends that more than one Administrator is created in the event the Administrator is absent or forgets his/her password. In addition, it is recommended to follow best practices for restricting Windows folder and file access to prevent unauthorized users from accessing software configuration files. See the Bluehill Files and Folders sections for more details.
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.	The audit trail in Bluehill Universal or Bluehill Central contains the following information: • The event – The operation that triggered an entry to be added to the Audit Trial. • What – A description of the action being captured. • Who - Username of who performed the action. • When – Date and timestamp of the action captured in UTC and displayed in local PC time zone • Why – A reason for the action.
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Bluehill software has several mechanisms to allow enforcement of sequencing: • Individual roles are enforced through the assigning of permissions when using one of Bluehill's security types. Permissions given to a user, or user group for Active Directory, define the areas of the software he or she has access to. • The prompted test workflow can be configured to guide the operator throughout the testing process, providing both text and graphical guidance and limiting data entry to the specimen under test. • Data entry can be configured to restrict or permit data entry at three different states: before a test, during a test, or after a test. • Security settings can override method configuration preventing any value changes to tested specimens. • Transducer system checks can be configured to prompt the operator to perform routine calibrationor balance operations to verify that the measurements are reading correctly.

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 records or perform the operation at hand.	At installation, security must be configuredto define user permissions. Using any of the supported security models, the system administrator can configure the system so that only authorized users will be allowed or denied certain permissions. Please refer to security permissions on page 2. Generally, users who are set to Administrators have access to maintain the system security and settings for electronic signatures. Changes to the security and traceability configurations are logged in the system audit trail and can only be performed by an authenticated user.
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.	Bluehill Universal allows all input values to be displayed on the screen either in text or graphical form. Data entry for numerical values are validated at entry to allow proper formatting as well as upper and lower entry bounds to reduce operator input error. Bluehill Universal also includes customizable choice inputs, allowing values to be set through a defined dropdown list, further reducing the input errors.
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.	Instron service engineers are trained and certified to install, service, and maintain Instron systems with Bluehill Universal and Bluehill Central, with exception to components managed from non-Instron supplied computers. The end user training is the responsibility of the client and should be part of the system's procedural compliance. Instron provides Bluehill Universal training classes onsiteand at Instron's corporate facility in Norwood, MA.
11.10 (j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for action initiated under their electronic signatures, in order to deter record and signature falsification.	It is the responsibility of the customer to establish and adhere to written policies holding individuals accountable and responsible for action initiated under their electronic signatures, and should be part of the system's procedural compliance.
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 ofsystems documentation.	It is the responsibility of the customer to maintain appropriate controls of the installed system. Instron follows a structured product development process and is required to maintain this process per Instron's ISO 9001 certification. Written procedures control the development, testing, and maintenance of Instron systemsand software.

11.30 Controls for open systems		
	21 CFR Part 11	Instron's software application(s)
	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 digital signature standards to ensure as necessary under circumstances, record authenticity, integrity and confidentiality.	Not applicable – Bluehill Universal is considered a closedsystem.

11.50 Signature Manifestations		
	21 CFR Part 11	Instron's software application(s)
11.50 (a)	Signed electronic records shall contain information associated with the signing that clearly indicates all the following: 1.) The printed name of the signer 2.) The date and time when the signature was executed; 3.) The meaning (such as review, approval, responsibility or authorship) associated with the signature	At a minimum, the audit log within Bluehill Universal and Bluehill Central displaysthe primary, secondary, and tertiary signature (if applicable) which include: • The user ID • The date and time of signature • The user's comment • The action of the signature, i.e. approve, reject
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)	The audit trail with electronic signatures is viewable on screen in Bluehill Universal and Bluehill Central and is printable.

11.70 Signature/ recording linking		
	21 CFR Part 11	Instron's software application(s)
	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.	Electronic signatures are configurable per Bluehill Universal file type to include method files, sample files, report templates, and PDF reports. Electronic signatures can be configurable for a primary, secondary, and tertiary sign-off. All signatures are linked to the respective electronic file and cannot be excised, copied, or otherwise transferred.

SUBPART C – ELECTRONIC SIGNATURES:

11.100 General requirements		
	21 CFR Part 11	Instron's software application(s)
11.100 (a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else	It is the responsibility of the customer to configure unique users.
11.100 (b)	Before an organization establishes, assigns, certifies or otherwise sanctions an individual's electronic signature, the organization shall verify the identity of the individual.	It is the responsibility of the customer to configure and assign users. Bluehill Universal and Bluehill Central will require the user to sign into the software and sign out after completing a task that requires asignature. Time-out intervals can be configured in Bluehill Universal and Bluehill Central, or Window®, forcing a user to re-enter their username and password if the system is left idle for a specified amount of time.
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.	It is up to the customer to certify that electronic signatures are the legally binding equivalent of handwritten signatures.

11.200 Electronic signature components and controls		
	21 CFR Part 11	Instron's software application(s)
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 signing 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 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 required collaboration of the two or more individuals.	Bluehill Universal does not support biometric signatures. 1.) Users electronically sign via Bluehill files using their unique username and password. This is the case for continuous and intermittent use of the system. 2.) It is the responsibility of the customer to ensure usernames and passwords are not shared and are unique to their genuine owners. 3.) It is the responsibility of the customer to ensure usernames and passwords are not shared and are unique to their genuine owners. For collaboration, Instron recommends configuring the system with secondary and/or tertiary electronic signatures so each unique user can electronically sign their work for approval or rejection.
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.	Bluehill Universal does not support biometric signatures.

11.300 Controls for identification codes/passwords		
	21 CFR Part 11	Instron's software application(s)
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.	It is the responsibility of the customer to configure and assign users. Instron recommends configuring security with Active Directory in order to control uniqueness of usernames and password length, character, and expiration criteria.
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled or revised (e.g. to cover such events such as password aging).	It is the responsibility of the customer to configure and assign users. Bluehill Universal's built-in security has a feature to allow passwords to expire. This must be configured by the system Administrator. Alternatively, users can be configured using Windows or Active Directory security. In either of these cases, password criteria including prevention of password aging is the responsibility of the customer's IT department.
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.	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.	It is the responsibility of the customer to configure and assign users. Both failed login attempts and successful logins are captured in the secure 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.	Not applicable.

REFERENCES:

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.1

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.2

https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfcfr/CFRSearch.cfm?CFRPart=11&showFR=1&subpartNode=21:1.0.1.1.8.3