

UbiBot[®] Software FDA 21 CFR Part 11 Compliance




This document explains how the following UbiBot[®] software can help you comply with the regulations in 21 CFR Part 11 for electronic records and electronic signatures.

Table One: UbiBot[®] software applications that offer 21 CFR Part 11 compliance

UbiBot [®] IoT Cloud Platform
UbiBot [®] Mobile App
UbiBot [®] PC Tools

Statement:

Above mentioned software/application were evaluated for conformance to functional and performance specifications. The test performed during the evaluation were made in conformance to the software validation test protocol documented in UbiBot[®] Quality Management System and demonstrated that the software conformed to all applicable performance and functional specifications.

	Name	Signature	Date
Tester	Tim Zad		01/12/2021
Reviewer	Jacky Shawn		05/12/2021
Approved	Leon Lee		12/12/2021

Overview

Title 21 of the Code of Federal Regulations, Part 11 ("[21 CFR Part 11](#)") defines legal criteria under which the Food and Drug Administration ("FDA") considers electronic records, electronic signatures, and handwritten signatures executed on electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

Part 11 requires subject organizations to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data.

Definitions

Understanding the following terms is essential for the successful implementation of the regulations in 21 CFR Part 11. These definitions taken directly from 21 CFR Part 11 will be the starting point for our discussion of UbiBot® software compliance with the regulation.

Closed system—An environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

Open system—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.

Digital signature (DS)—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.

Electronic record—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.

Electronic signature—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.

Software application template files—May include parameter files, quant methods and macros.

Check List:

This check list shows the approach adopted in UbiBot® to help the validation procedures of the computer systems in the process. The left side shows the requirements and the right side shows how these requirements can be achieved with UbiBot® software.

11.10 Controls for Closed Systems Requirement:

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.

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.10 (a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	All software and platforms are subject to a functional testing and validation protocol, consisting of automated and manual tests that must be passed before any software is released.	<input checked="" type="checkbox"/>
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.	UbiBot® hardware's recordings and historical data files are encrypted and unreadable. All data files are available to export in PDF, CSV, and HTML file formats.	<input checked="" type="checkbox"/>
11.10 (c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	All records are generated by and communicated to the server database from only authorized users whose credentials have been authenticated. These records are stored permanently offsite in a secure database hosted by a major cloud services provider, with full database redundancy as well as point-in-time backup restoration. The records may be accessed at any time by authorized users.	<input checked="" type="checkbox"/>
11.10 (d)	Limiting system access to authorized individuals.	Users must be authenticated by a unique	<input checked="" type="checkbox"/>

		username and password before they are able to access any software system features.	
11.10 (e)	Use of secure, computergenerated, 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 system automatically generates audit trails (including timestamp and username) of all user actions pertaining to records in permanent storage that cannot be altered, overwritten, or deleted. These logs of user activity consist of, but are not limited to: (a) Activating and deactivating monitoring devices (b) User logins and logouts (c) Synchronization of data from monitoring devices (d) Creation, editing, and deletion of user accounts and credentials In addition, for redundancy of security, permanent logs are stored in a separate storage location of all database activity, including data creation, editing, and deletion. All logs are permanent and retained indefinitely, unless otherwise requested by the end customer.	<input checked="" type="checkbox"/>
11.10 (f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	No user can create, delete, or modify records in a particular step in UbiBot software/platform that is out of order in the overall sequence.	<input checked="" type="checkbox"/>
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.	Users must be authenticated by a unique username and password before they are able to access any UbiBot software system features.	<input checked="" type="checkbox"/>
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 source of monitored data can only be a UbiBot sensor. The source of records can only be a terminal device that is executing UbiBot software and operated by a user that has provided	<input checked="" type="checkbox"/>

		authenticated credentials to an authorized user account. UbiBot's mobile app has log error detection, and the web back-end has tamper detection to prevent invalid data from being submitted.	
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.	Not applied to UbiBot. Process responsible staff should determine who the system users are.	N/A
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.	Not applied to UbiBot. Process responsible staff should determine who the system users are.	N/A
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.	Regarding UbiBot, the system has documentation explaining its features in every new version released. UbiBot records all systems documentation changes in a time-sequenced manner for proper audit trail recording.	<input checked="" type="checkbox"/>

11.30 Controls for Open Systems Requirement:

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.30	Controls for open systems	Not applicable. The UbiBot Software System is a closed system.	N/A

11.50 Signature manifestation

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.50	Signature manifestation	Not applicable for the software. The UbiBot Software System does not utilize signatures.	N/A

11.70 Signature/record linking

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.70	Signature/record linking	Not applicable for the software. The UbiBot Software System does not utilize electronic signatures.	N/A

11.100 General requirements – Electronic Signatures

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.100	General requirements – Electronic Signatures	Not applicable for the software. The UbiBot Software System does not utilize electronic signatures.	N/A

11.200 Electronic signature components and control

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
11.200	Electronic signature components and control	Not applicable for the software. The UbiBot Software System does not utilize electronic signatures.	N/A

11.300 Controls for identification codes/passwords

Ref No.	Part 11 Requirement	UbiBot® Implementation	Result
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 not possible to create two individuals with the same authentication in UbiBot System	<input checked="" type="checkbox"/>
11.300 (b)	Ensuring that identification code and password issuances are periodically checked, recalled, or	Application administrator can configure a password expiration date for each	<input checked="" type="checkbox"/>

	revised (e.g., to cover such events as password aging).	user, forcing users to define a new password.	
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 applied to UbiBot.	N/A
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.	Not applied to UbiBot.	N/A
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 applied to UbiBot.	N/A

Summary

This document was created based on our interpretation of the technical demands presented in FDA documents on 21 CFR Part 11. The development was done after consulting people with deep knowledge on the subject and participating in specialized events about computer systems validation. If needed, we can negotiate small adjustments in order to fully attend all your final system validation needs.

Disclaimer

We're pleased to provide information to help support our customers' compliance with FDA 21 CFR Part 11. However, the information above is not intended to be legal advice. We recommend you consult an attorney if you have any legal questions.