PcVueSolutions 21 CFR Part 11 EN

Compliance table

Last update :	October 2020
Revision :	1
Content :	Contains the 21CFR11's compliance with PcVue
Confidentiality :	Public

PcVue Solutions

Content

PcVue and the 21CFR11

1. Overview

21 CFR Part 11 is a reference document of the FDA (Food and Drug Administration in the United States) which defines the requirements to be met so that electronic records and signatures are considered as trustworthy as signed paper documents. manually.

PcVue integrates a certain number of functionalities responding to an interpretation of the requirements of the 21CFRpart11 regulation for the following sub-parts:

Subpart B - Electronic Recordings. Describes the controls for closed and open systems. The Supervisor is considered a closed system.

Subpart C - Electronic Signatures. Describes the implementation and use of electronic signatures. In the Supervisor, an electronic signature corresponds to a user account.

It is important to note that most of these features are natively integrated in PcVue available for free in all PcVue versions.

They are widely described in the PcVue online help.

The application developer should be aware that using these features does not guarantee compliance because software alone cannot provide compliance.
Most of the requirements are met by procedures, while compliance vis-à-vis others can be resolved by restricting access to the PC from a physical and electronic point of view.

It should also be taken into account that 21 CFR Part 11 is a document regarding electronic records and signatures - it is not specific to the use of PCs and applications such as SCADA.
Therefore, it is open to interpretation and its application must take into account the advisory documents that are regularly issued by the FDA.

This document describes the conformity between the 21CFR Part 11 “Electronic files and signatures” regulation and the PcVue software, developed by ARC Informatique. Responses to requests for the standard can be applications, or integrated from version 7.20 of the product.

2. PcVue compliance table

2.1 Subpart A - General Provisions

Section	Regulation	Conformance
11.1	Scope. Defines the scope of regulation.	ARC Informatique accepts the intentions of the regulations.
11.2	Implementation. Files can be stored in computer format and submitted to the FDA, provided that the rules of 21CFR are followed	This point of the rule applies to system users for an application. ARC Informatique does not submit documents directly to the FDA.
11.3	Definitions. Defines terms used in correspondence with the FDA. This is mainly a lexicon.	No comment.

2.2 Subpart B - Electronic records

Section	Regulation	Conformance
11.10	Controls for closed systems. A closed system is a system to which access is restricted to managers. The measures that must be taken, in order to prove control are:	PcVue can be configured as a proprietary system, in which case all functions of PcVue and the operating system are reserved for authorized users. All the information collected by PcVue is part of the project and can only be generated by PcVue except for explicit export.
	a. Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	PcVue uses a proprietary real-time variable database and historical binary, ASCII or SQL server database files PcVue stores, in the format chosen during configuration, changes in measurements, changes in bit status and alarms. In the case of a Project configured as a proprietary system, the data files can only be accessed from PcVue.

	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.	Recordings are kept in archive files and can be easily retrieved. PcVue offers the possibility of extracting, on a specific date, the number of records desired, either directly in the application or using a complementary data extraction tool.
	c. Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Files can be saved on the computer hard drive, in the project structure, on a network drive or in storage space (private cloud). The project can be configured to ensure access only to authorized persons. Files can be read-protected. Mechanisms allow the archiving of data automatically or manually on another medium by an authorized user. To activate this function, it is not necessary to go through the operating system. The customer user must apply the applicable terms and procedures to ensure the retention of data for the appropriate period.
	d. Limiting system access to authorized individuals.	The project can be configured so that only users corresponding to a configured profile can access it. A "Username" and "Password" are required to access the system.
	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	User actions, logging in, logging out, acknowledging alarms and changing setpoints, can all be recorded in log files. The event file is protected from intentional modifications. An additional mechanism allowing other user actions to be recorded (generate a report, open a mimic, etc.) can be implemented by application.

	that required for the subject electronic records and shall be available for agency review and copying.	It is possible to trace operator actions such as modification of a setpoint (old and new value). All system events can be saved to log files.
	f. Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	This comes under application development.
	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.	Any modification or access to the operating system is limited to the appropriate operators. A history of allocation and evolution of access rights must be created. It is also possible to rely on a Windows user directory (Active Directory) to control access to the monitoring application.
	h. Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	In order to validate the origin of the data input source, the designer of the system must take into account the producer / consumer architecture of PcVue in order to limit the storage of data to dedicated stations (archive server) so that the generation is unique.
	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.	ARC Informatique offers training relating to the configuration of PcVue. In principle, training on a specific project is carried out by the people in charge of the development of the project. Users of an application involved in a regulated system must have the necessary training and experience to perform their tasks.
	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.	The user customer is responsible for developing the terms and procedures for using an application in a regulated environment.

	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.	The user customer is responsible for developing the terms and procedures for using an application in a regulated environment.
	k Use of appropriate controls over systems documentation including: (2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	The list of the main modifications made to PcVue is recorded in a “readme.txt” document installed with the software release. Additions describing the implementation of the new features are provided in the electronic documentation. An exhaustive and detailed list of new features and corrections exists in an ARC Informatique document. For the traceability of application modifications, PcVue has a "Version management" function allowing to trace the changes made to the project and to restore the original version if necessary, and a file tracing the modifications made to the variables. .
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	PcVue can be configured as a proprietary system, in which case all functions of PcVue and the operating system are reserved for Authorized Users. All the information collected is part of the Project and can be generated only by PcVue except for explicit export.

	appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.	
11.50(a)	Signature manifestations. Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:	
11.50(a)(1)	The printed name of the signer	The user "Login" is currently traced during the connection or disconnection of this user.
11.50(a)(2)	The date and time when the signature was executed	Any connection or disconnection of a user is time-stamped in the PcVue events.
11.50(a)(3)	The meaning (such as review, approval, responsibility, or authorship) associated with the signature.	The user definition dialog box will eventually contain the Last Name, First Name and Quality fields.
11.50(b)	The items identified in paragraphs (a)(1), (a)(2), and (a)(3) 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 electronic display or printout).	
11.70	Signature/record 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.	The name of the operator (Login) appears in each record. It is very difficult, if not impossible, to transfer a signature from one recording to another in PcVue archives defined in binary format. The user.dat file can be encrypted using ARC Informatique encoding. The BINARY nature of the recording file prohibits any attempt at tampering.

2.3 Subpart C – Electronic Signatures

Section	Regulation	Conformance
11.100	General requirements. (a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	A unique "Username" and "Password" are issued to each user with a configured profile. The old "Password" are stored and cannot be reused, for the "Login" the modification is in progress.
	(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.	The customer using an application in an FDA-regulated environment must take responsibility for verifying the identity of individuals who may be using electronic signatures.
	(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.	The customer using an application in an FDA-regulated environment must be able to certify that the electronic signatures in their system are intended for use as the legal equivalent of traditional handwritten signatures.
11.200	Electronic signature components and controls. (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.	A username and a unique password are issued to each user with a configured profile. It is the user's responsibility to provide the best security in order to prevent fraudulent use of passwords.
	a.(1)(i))When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall	PcVue requires the user to re-enter their name and password when logging into the system. It is also possible to force the user to re-enter his password before any critical action.

	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.	
	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.	PcVue includes an "idle time" parameter for each user. The expiration of this period causes the automatic "Delog" and requires that each user accessing the system re-enter their name and password.
	a.(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.	To allow an unauthorized user to intervene occasionally on the application, it is possible to use the "Double Signature" option integrated in PcVue. This function requires the "Login" and "Password" of at least two separate users.
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:	
	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.	Any combination of "Login" and "password" is unique. It is not possible to define two users with the same "Login". a password cannot be reused multiple times.

	b. Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	The configuration of PcVue requires the user to change his password, every n days (not configurable from 1 day to 12 months).
	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.	This is an internal procedure at the customer's expense. After the first change of the password on the initiative of the user, the latter is the only one to have it.
	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.	An integrated solution generating, after 3 unsuccessful attempts, an alarm traced in the archives is offered in PcVue. It is possible to notify the system administrator by email or SMS of the attempted fraudulent access to the application.
	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.	It belongs to the reader system builder badges to guarantee the inviolability of its supply and to ensure its interfacing with the computer system.

ARC Informatique

Private limited company
capitalized
at 1 250 000 €
RCS Nanterre B 320 695 356
APE 5829C
SIREN 320 695 356
VAT N°FR 19320695356

PcVueSolutions 21 CFR Part 11 EN

ISO 9001 and ISO 14001 certified

ARC Informatique

Headquarters and Paris offices
2 avenue de la Cristallerie
92310 Sèvres - France
tel + 33 1 41 14 36 00
fax + 33 1 46 23 86 02
hotline +33 1 41 14 36 25
arcnews@arcinfo.com
www.pcvuesolutions.com

GERMANY - Munich
PcVue GmbH
Bernsteinstrasse 19B
D-84032 Altdorf
Tel: +49 871 976 936 0
Fax: +49 871 976 936 29

SWITZERLAND - Beringen
Schleitheimerstrasse 42a
CH-8222 Beringen
Switzerland
Tel + 41 52 682 19 38
Fax + 41 52 682 19 58

UK – London control
PcVue Solutions Ltd
Regal Chambers
49/51 Bancroft, Hitchin
Hertfordshire, SG5 1LL
England
Tel + 44 1 462 45 77 00

Italy - Milan
PcVue Srl
Piazza IV Novembre, 4
20124 Milan
Tel +39 02 9267248
Fax +39 02 92165771

SPAIN - Irun
PcVue Solutions S.L Spain
Calle Santiago,7
20304 Irun Spain
Tel +34 678 360 822
pcvuesl@pcvuesolutions.com

UAE - Dubaï
PcVue DMCC
Office Tower 1708
GoldCrest Executive Tower
Jumeirah Lake Towers
Cluster C Dubai, UAE
Tel +971 (0) 48 747 980
pcvue-uae@arcinfo.com

RUSSIA – Saint Petersburg
PcVue Russia and CIS
197198 Russia, Saint Petersburg,
Malyy pr. P.S., 5
Tel: + 7 812 648 67 60
support_ru@pcvuesolutions.com
order_ru@pcvuesolutions.com

BRAZIL - São Paulo
PcVue Brazil
São Paulo - Brazil
Adriano Pedroso Puda
Business Developer
Mobile: +55 (11) 9 9123-5178
Email: a.pedroso@arcinfo.com

USA - Boston
PcVue Inc.
10 Tower Office Park,
Suite # 204
Woburn, MA 01801 - USA
Tel: +1 781 460 3272
Fax: +1 781 459 0252
sales@pcvueinc.com

Chile - Santiago
PcVue Lat
Eliodoro Yañez 2876
office N°302 Providencia
Santiago - Chile
Tel: +56 2 2298 6562
c.bastidas@arcinfo.com

JAPAN - Nagoya
PcVue Japan
4F Famous-Marunouchi Bldg 3-18-22
Marunouchi Naka-ku, Nagoya City
460-0002 Aichi
Japan
Tel + 81 90 2349 7701

SINGAPORE - Singapore
PcVue Sea
Blk 808 French Road
#05-165 Kitchener Complex
Singapore 200808
Tel + 65 6396 9186

CHINA- Shangai
PcVue China
228, MeiYuan Road,
2119-2120# Enterprise Square,
Jing'An District,
200070 Shanghai
Tel + 86 21 52400 496
Fax + 86 21 52400 456

MALAYSIA- Kuala Lumpur
PcVue Sdn Bhd
Unit 801, Block A, Phileo Damansara 1
No.9, Jalan 16/11
46350 Petaling Jaya Selangor Darul Ehsan
Malaysia
Tel + 60 3 7957 5187
Fax + 60 3 7958 8760