

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

The following document informs about the CFR 21 Part 11 compliance status of the PTZ 32 Software Package which is used to drive and control an automated Tablet Testing System Type WHT 3ME and a Multiple Batch Feeder Type WHT SM/SM1.

The Software has to be installed at a suitable PC System which runs under Windows™ XP (GB/US version). The PC has to have a RS232 Port to drive the WHT 3ME, Printer port and CD Drive to install the software. A suitable back-up system should be available to safeguard the data.

21 CFR 11 – Requirements	Result	Comment
<p>... Such procedures and controls shall include the following: Validation of system to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.</p> <p>Is the system validated?</p> <p>Is it possible to discern invalid or altered records?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	<p>Yes</p> <p>Software Version management Its impossible to modify, change or alter existing records</p>
<p><b>11.10(b)</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...</p> <p>Is the system capable of producing accurate and complete copies of electronic records on paper?</p> <p>Is the system capable of producing accurate and complete copies of records in electronic form for inspection, review and copying by the FDA?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	<p>Ok for Method, Product data, actual test results and reports</p> <ul style="list-style-type: none"> <li>- By printout</li> <li>- Data-export (Excel)</li> <li>- Data-export (text-file)</li> </ul>
<p><b>11.10(c)</b> Protection of records to enable their accurate and ready retrieval throughout the retention period. Are the records readily retrievable throughout their retention period?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	<ul style="list-style-type: none"> <li>- By Databank</li> <li>- Data-export (Excel)</li> <li>- Backup Databank</li> </ul>

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.10(d)</b> Limiting system access to authorized individuals Is system access limited to authorized individuals?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	Protected login: password and User administration with Access rights
<p><b>11.10(e)</b> Use of secure, computer generated, time-stamped audit trails in independently record the data and time of operator entries and actions that create, modify, or delete electronic records. Records changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period as least as long as that required for the subject electronic records and shall be available for agency review and copying.</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	Changes are identified. Original data can be processed. The original is always discarded in the databank.  Audit Trail is available.  Changes like create and delete data of methods, products, results are password protected.  Changes must be justified
<p><b>11.10(f)</b> Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate. If the sequence of system steps or events is important, is this enforced by the system (e.g., as would be case in a process control system)?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	Validation (calibration and adjustment) Only for qualified users (user administration)
<p><b>11.10(g)</b> Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer input or output device, alter a record, or perform the operation at hand. Does the system ensure that only authorized individuals can use the system; electronically sign records, access the operation, or computer system input or output device, alter a record, or perform other operations?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	- By user authorisation, password and rights - Result release by manual signing of all printed results reports Administrator authorisations

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.10(h)</b> Use of device (e.g., terminal) checks to determinate, as appropriate, the validity of the source of data input or operational instruction. If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g., terminal) does the system check the validity of the source of any data or instructions received? (Note: This applies where data or instructions can come from more than one device, and therefore the system must verify the integrity of its source, such as a network of weigh scales, or remote, radio controlled terminals)</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	Instrument serial number identification
<p><b>11.10(i)</b> Determination that persons who develop, maintain, or use electronic record/ electronic signature systems have the education, training, and experience to perform their assigned tasks. Is there documented training, including on the job training for system users, developers, IT support staff?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	User training is performed by qualified personnel on customers demand, a training certificate is supplied
<p><b>11.10(j)</b> The establishment of an adherence to written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to determine record and signature falsification. Is there a written policy that makes individuals fully accountable and responsible for actions initiated under their electronic signatures?</p>	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input checked="" type="checkbox"/> NR	User responsibility

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.10(k)</b> Use of appropriate controls over system documentation</p> <p>Is the distribution of , access to, and use of systems operation and maintenance documentation controlled?</p> <p>Is there a formal change control procedure for system documentation that maintains a time sequence audit trail for those changes made by the pharmaceutical organization?</p>	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input checked="" type="checkbox"/> NR	<p>Customer-Responsibility</p> <p>User manuals are delivered in German and English language. The documentation is available (On the delivered CD). Updates, product information and documentation are available on the homepage of Pharma Test and in the QC, IQ, OQ documentation</p>
<p><b>11.30</b> 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 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.</p> <p>Is data encrypted? Are digital signatures used?</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	<p>Databank Super Password</p> <p>Databank itself is password protected.</p> <p>Software access protected by password and access rights (User Administration)</p>

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.50</b>                      (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.                      (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 the electronic record (such as electronic display or printout).                      Do signed electronic records contain the following information?                      - The printed name of the signer                      - The date and time of signing                      - The meaning of the signing (such as approval, review, responsibility)</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	manual release of reports by signature Printout should be signed on each page. Printout includes the actual date and time
<p><b>11.70</b> 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.                      Are signatures linked to their respective electronic records to ensure that they cannot be cut, copied, or otherwise transferred by ordinary means for the purpose of falsification</p>	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input checked="" type="checkbox"/> NR	manual release of reports by signature
<p><b>11.100</b> (a) Each electronic signature shall be unique to the one individual and shall not be reused by, or reassigned to, anyone else                      (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. Are electronic signatures unique to an individual? Are electronic signatures ever reused by, or reassigned to anyone else? Is the identity of an individual verified before an electronic signature is allocated?</p>	<input type="checkbox"/> OK <input type="checkbox"/> NOK <input checked="" type="checkbox"/> NR	manual release of reports by signature

PHARMA TEST GmbH  
 Siemensstrasse 5  
 D-63512 Hainburg (GER)



+49 6182 9532-600  
 +49 6182 9532-650  
 email@pharma-test.de  
 www.pharma-test.com



## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.200(a)</b> Electronic signatures that are not based upon biometric shall:</p> <p>(1) Employ at least two distinct identification components such as an identification code and password.</p> <p>(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 at least one electronic signature component that is only executable by and designed to be used only by the individual.</p> <p>(1)(ii) When an individual executes one or more signings not performing during a single, continuous period of controlled system access, each sign shall be executed using all of the electronic signature components</p> <p>(2) Be used only by their genuine owners, and</p> <p>(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</p> <p>(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners</p> <p>During a continuous session, is the password executed at each signing? (Note: both components must be executed at the first signing of a session)</p> <p>If signings are not done in a continuous session, are both components of the electronic signature with each signing?</p> <p>Are non-biometric signatures only used by their genuine owners?</p> <p>Would an attempt to falsify an electronic signature require the collaboration of at least two individuals?</p> <p>Has it been shown that biometric electronic signatures can be used only by their genuine owner?</p>	<p><input type="checkbox"/> OK <input type="checkbox"/> NOK <input checked="" type="checkbox"/> NR</p>	<p>manual release of reports by signature</p>

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p><b>11.300</b> Controls for Identification Codes and Passwords shall include:</p> <p>(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</p> <p>(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging)</p> <p>(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised token, cards, and other devices that bear or generate identification, and to issue temporary or permanent replacements using suitable rigorous controls.</p> <p>(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 system security unit, and, as appropriate, to organizational management. Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear to generate identification code and password identification, and to issue temporary or permanent replacements using suitable rigorous controls.</p> <p>(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. Are controls in place to maintain the uniqueness of each combined identification code and password, such that no individual can have the same combination of identification code and password? Are procedures in place to ensure that the validity of identification codes is periodically checked? Do passwords periodically expire and need to be revised? Is there a procedure for recalling identification codes and passwords</p>	<input checked="" type="checkbox"/> OK <input type="checkbox"/> NOK <input type="checkbox"/> NR	<p>The combination of Username and Password are definite.</p> <p>The use of identical Usernames is prevented. The password must consist of at least 8 characters.</p> <p>Calibration period can be edited</p> <p>User administration, an expiry date of the password can be entered</p>

## Checklist / 21 CFR part 11 Compliance for WHT32-Software

21 CFR 11 – Requirements	Result	Comment
<p>Is there a procedure for electronically disabling an identification code or password if it is potentially compromised or lost?</p> <p>Is there a procedure for detecting attempts at authorized use and for informing security?</p> <p>Is there a procedure for detecting attempts at unauthorized use and for informing security?</p> <p>Is there a procedure for reporting repeated or serious attempts at unauthorized use to management?</p> <p>Is there a loss management procedure to be followed if a device is lost or stolen?</p> <p>Is there a procedure for electronically disabling a device if it is lost, stolen, or potentially compromised?</p> <p>Are there controls over the issuance of temporary and permanent replacements?</p> <p>Is there initial and periodic testing of tokens and cards?</p> <p>Does this testing check that there have been no unauthorized alterations?</p>	<input checked="" type="checkbox"/> <b>OK</b> <input type="checkbox"/> <b>NOK</b> <input type="checkbox"/> <b>NR</b>	<p>User-administration</p> <p>Audit trail</p> <p>Audit trail</p> <p>After the second false login the program is closed</p> <p>License with serial number</p> <p>Each WHT has a serial number</p>

**OK** = fulfils requirement

**NOK** = does not fulfil the requirement

**NR** = not relevant