Using HOBOware® Pro with 21 CFR Part 11 Systems

This document is intended to clarify how Onset Computer Corporation HOBOware Pro Software is compatible within an environment where 21 CFR Part 11 is being employed. This excludes the HOBOnode Manager portion of HOBOware, which is used with Onset's ZW product line.

Title 21 CFR Part 11 of the Code of Federal Regulations deals with the Food and Drug Administration (FDA) guidelines on electronic records and electronic signatures in the United States. Part 11, as it is commonly called, defines the criteria under which electronic records and electronic signatures are considered to be trustworthy, reliable and equivalent to paper records.

The following table shows how the 21 CFR Part 11 requirements can be addressed using HOBOware Pro (Version 2.3 or above) in conjunction with the customer's computer systems and the customer's internal procedures.

Regulation Reference	Onset Comments
Sec. 11.10 Controls for Closed Systems 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. Such procedures and controls shall include the following:	
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	NIST-traceable temperature accuracy certification available for loggers for an additional fee. Test files are included with HOBOware Pro that can be used to verify it is properly detecting files that have been altered.
(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.	Electronic records produced by HOBOware Pro can be viewed with HOBOware Pro or HOBOware Lite, and can be printed from either of these as well. Secure electronic copies of files can be made and shared by e-mail or other electronic transfer methods.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.	HOBOware Pro stores the electronic records in the location specified by the user. The customer systems must ensure that these files are backed up regularly, and that the data files are stored in a location where they can be readily available on request. The computer system must have sufficient redundancy to prevent loss of data for records retention period.
(d) Limiting system access to authorized individuals.	It is up to the customer to establish unique log-in names and passwords for users authorized to launch and offload secure data files. Both Windows and Mac OSX offer a mid-level security package by including robust user log- in systems which ensure that each user name is unique, and that only the authorized user can sign in with that user name.
(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.	In Secure Mode, HOBOware Pro stores digitally secured files that include the date, time and user name for the HOBO logger launch and logger readout. This audit trail information is a permanent part of the secure data file and cannot be deleted, any attempt to alter this information will be detected, and the data file will no longer be shown as secure.
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	No comment.
(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.	Log-in is handled by the Windows or Mac OS log-in system, and the security tools inherent to these should be utilized to ensure only the authorized users can log-in under their user names.

Regulation Reference	Onset Comments
Sec. 11.10 Controls for Closed Systems (continued)	
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Every HOBO data logger has a unique serial number that is stored with the secure data file that uniquely identifies that data file as coming from that logger.
(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.	User guides and on-line training are available to ensure the user has the information needed to operate the system.
(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 applicable.
(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 is under version control.	No comment.
Sec. 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.	In secure mode all files stored by HOBOware Pro include a digital signature that ensures the authenticity and integrity of the data.
Sec. 11.50 Signature Manifestations	
(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.	HOBOware does not provide electronic signatures. In Secure Mode, the files stored by HOBOware Pro include the name of the user and the date and time when the logger was launched and when the data file was read out.
(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).	Not applicable.

Regulation Reference	Onset Comments
Sec. 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.	Not applicable.
Electronic Signatures **Sec. 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.	HOBOware Pro stores a unique digital signature with each data file, along with the current user name. It is up to the customer to establish procedures that ensure that only the authorized user can login with their user name. Both Windows and Mac OSX offer a mid-level security package by including robust user log- in systems that ensure that each user name is unique, and that only the authorized user can sign in with that user name.
(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.	Not applicable.
(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.	Not applicable.
Sec. 11.200 Electronic Signature Components and Controls	
Electronic signatures that are not based upon biometrics shall: (1) Employ at least two distinct identification components such as an identification code and password.	The customer should set up their Windows or Mac OSX log-in systems to require that authorized users enter their unique user names and corresponding passwords before they run HOBOware Pro.
(2) Be used only by their genuine owners	Require user name and password. Per Microsoft medium security guidelines, passwords must be changed at least every 90 days per current customer guidelines.
(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.	No comment.

Regulation Reference	Onset Comments
Sec. 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. (b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging). (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. (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. (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.	The customer should set up their Windows or Mac OS log-in systems to meet the requirements in this section.