Signatrol.com
Data Logging Solutions

Using TempIT in secure data applications

Introduction

In many applications, especially when data loggers are used for monitoring storage and transport conditions of drugs, pharmaceuticals and blood products, it is essential that the data is a true and faithful record of the actual conditions the sensitive items have been exposed to.

Signatrol offer TempIT-lite and TempIT-pro software which stores the data in secure form whereby the data are not alterable by commonly available tools.

This paper deals with customers who wish to use the TempIT –Lite and Pro versions within an FDA or other similar high security system.

To support the various facets of FDA 21 CFR part 11 it is essential to use the loggers within an overall operating procedure that is approved by FDA.

Summary of Features

TempIT Pro and TempIT Lite offer the following features to enable the logging system to be used within an overall FDA validatable system:

- Data are stored in secure form, not alterable by normal means
- Charts can be signed indicating the following:
  - The printed name of the signer;
  - The date and time when the signature was executed; and
  - The meaning (such as review, approval, responsibility, or authorship) associated with the signature.
- Access is controlled by a series of passwords
- Calibration intervals are monitored and flagged

Controlling Access

There are two means of controlling and limiting access, the Password and the Passcode.

Password

This security feature limits access to the TempIT configuration and issue screens to be restricted to those with a valid password. The default setting is off. The password is set during the installation of the software. The password can be changed using the "Change Password" button. The password is also required to unlock the SL7000 series input trim parameters and SL5x series calibration on the issue form.

Passcode

The Passcode is required by all loggers except the SL5x series. The code is a one-time programmable number which is loaded into the logger the first time the logger is issued with manifest data. The passcode's purpose is to stop unauthorised users from clearing important information from the logger. Once set, the TempIT application will automatically send the passcode to the logger when stopping and starting new logs. If the incorrect passcode is sent, the stop or start command will be ignored. Not knowing the passcode does not prevent any user from reading the log data..

Calibration Interval

The re-calibration interval is the period between logger calibrations. This can be set within the software as 3, 6, 12 Months or disabled. Recommended calibration interval is 12 months. If the period exceeds the set period a ‘Tag out of Calibration’ message is displayed. It is important that the calibration state of all loggers is monitored to ensure that readings are correct and valid.
A re-calibration service is offered by Signatrol.

Archiving Records

Archiving is an essential operation to ensure a record of files is maintained even in the event of a hard disk crash. A procedure should be established to periodically back up all the log files. It should be noted that, in the event of a hard disk crash, any data not backed up would be lost. Data contained in the logger will be preserved until the logger is next issued.

Validation

The FDA do not approve or endorse any products but they do validate the customers entire control and monitoring systems. As such there is no such thing as an FDA validated or approved logger, however, as the customer must have his system validated it is essential that the logger complies with the regulations in all respects for the application. As the customers system will be validated it is also important that the key elements of the secure software are easily verified. The following table highlights elements required for a validatable system and how the TempIT-Lite or TempIT-Pro software complies.

Clause No.	How Compliance Achieved	Validation Method
Clause 11.10		
(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Regular system calibration at specified intervals. System flags when calibration due	The data logger records calibration data and flags calibration due. Audit of customer procedures
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	Records viewed through software, stored in encrypted form.	Check that data are not alterable by commonly available tools.
(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period	Secure backup copies to me made on a regular basis	Not viewable/alterable by commonly available tools.
(d) Limiting system access to authorized individuals	Passwords and Passcode operation	Check use of passwords are tightly controlled by audit of customer procedures
(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.	Computer maintained reader log file shows who has read data.	Not viewable/alterable by commonly available tools
(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Customers Procedures	Audit of customer procedures
(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.	Controlled by software	Try to gain unauthorized access
(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.	Customers Procedures	Audit of customer procedures
(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.	Customers Procedures	Audit of customer procedures
(j) The establishment of, and adherence to, written policies that hold individuals	Customers Procedures	Audit of customer procedures

accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.		
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 documents	Customers Procedures Computer maintained log files in encrypted format.	Audit of customer procedures

Signing for the record

Signed printed records shall contain information associated with the signing that clearly indicates all of the following:

- The printed name of the signer;
- The date and time when the signature was executed; and
- The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Extracts from FDA 21 CFR part 11 Standard

FDA 21 CFR part 11 covers electronic records and electronic signatures and its scope is as follows

Scope

Regulations establish the criteria the FDA considers for electronic records and electronic signature to be trustworthy, reliable, and generally equivalent to paper.
Applies to all records in electronic form under any records requirement within any FDA regulation.
Electronic records are considered equivalent to full hand-written signatures, initials, and other general signings.
Electronic records may be used in accordance with Part 11 unless paper records are specifically required.
Computer system (hardware and software), controls, and relevant documentation must be available for review during FDA inspections.

Requirements for Closed Systems

The Company must develop procedures and controls to ensure authenticity, integrity and confidentiality, and that signer cannot repudiate the signed record.

The controls must:

- Be validated
- Maintain accurate and complete records
- Limit the system to authorized persons
- Protect records through retention period
- Contain audit trails that are secure, operator independent, computer-generated, time-stamped, cover the creation , modification and deletion of records and do not obscure previous information
- Allow for the performance of operational system checks, authority checks, and device checks to ensure system, record, and data integrity
- Ensure appropriate personnel qualifications
- Policies written and followed to hold personnel accountable for actions and to deter records falsification
- Control over system documentation including distribution, access, use, revision and change control