FREQUENTLY ASKED QUESTIONS

Syngistix for ICP-MS Enhanced Security Software for Laboratories Subject to 21 CFR Part 11 Regulations

The regulations of 21 CFR Part 11 (Title 21 – Food and Drugs of the Code of Federal Regulations) cover overall system compliance and include administrative, procedural and technical elements. Software alone cannot be compliant without the development and implementation of the other elements. Syngistix™ for ICP-MS Enhanced Security™ software for PerkinElmer NexION® ICP-MS systems provides features that, when coupled with appropriate policies and procedure, fulfill the requirements for closed-system electronic records in 21 CFR Part 11. Syngistix Enhanced Security software also fulfills the elements relating to electronic signatures.

21 CFR Part 11 Subpart B – Electronic Records

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:

11.10 a Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Q **Is it possible to see on the system whether or not records have been altered?**

A Where changes are allowed, Audit Trails and a File History database record changes to records. The Audit Trails and File History database may be used to view or retrieve information on records that have been altered.

The software does not provide a means to modify the raw data once collected into a data file.

To prevent unauthorized changes, Syngistix Enhanced Security software appends a checksum value to all files.

Attempting to open a file that has been altered outside the system will generate an error message and the Syngistix software will not allow the file to be opened.

All files are checked before they are opened. Dataset files are checked when the dataset is opened and whenever data reprocessing is performed.

Q **Can the system identify invalid records?**

A Syngistix Enhanced Security software appends a checksum to all files.

Attempting to open a file that has been altered outside the system will generate an error message and the Syngistix software will not allow the file to be opened. All files are checked before they are opened. Dataset files are checked when the dataset is opened and whenever data reprocessing is performed.

PerkinElmer®
For the Better

Q **Who is responsible for validation of the system?**

A The customer is responsible for validation of the "system" (includes policies, procedures, hardware, software and people).

For initial selection and validation, the customer should conduct some form of vendor assessment to determine how the system software was developed and the level of testing. Based on a risk assessment, the customer can determine the nature and level of their validation effort.

Q **What is the vendor's role for validation?**

A To support the customer's validation effort, PerkinElmer allows customer audits and provides development information through this process.

Comprehensive documentation detailing the use and operation of the system is provided with every ICP-MS system. Known problems that could affect software operation are detailed in the Syngistix Enhanced Security software release notes. ICP-MS customer training courses that provide in-depth instruction on use and operation of the NexION system are also available.

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.

Q **Is the system capable of producing accurate and complete copies of records in electronic form suitable for inspection, review, and copying by the U.S. FDA?**

A All files and data objects can be read using the Syngistix application and inspected using the included tools. In addition, most data objects can be exported as Text which can be viewed using a Text editor in addition to being printed to a hardcopy or PDF.

Data files and Audit Trail can be read with the Syngistix Enhanced Security software and inspected using the ES Tools included.

With the Syngistix Enhanced Security software reporting tool, information from the following files can be exported to text files:

- Method
- Sample batch
- Optimization
- Tuning
- Calibration
- Dataset files

The Security Audit Trail can be exported to a text file.

Q **Is the system capable of producing accurate and complete copies of records in paper form for inspection, review, and copying by the U.S. FDA?**

A Files can be reported in paper form using the Reporter feature (includes Method, Sample Batch, Optimization, Tuning, Report Template, Calibration, and Dataset Files).

The Security Audit Trail, Audit Trail, and File History can be printed using the tools provided by using Syngistix Enhanced Security Tools utility (ES Tools).

11.10 c Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Q **Are the records readily retrievable throughout their retention period?**

A Records are always retrievable using the version of Syngistix Enhanced Security software used to create them. Wherever practical, the system is designed to make possible the retrieval of older records in newer versions of Syngistix Enhanced Security software.

ES Tools Archive and Restore utilities facilitate convenient data archival and retrieval.

The customer will need to document and implement suitable backup and restoration policies and procedures for the applicable data.

11.10 d Limiting system access to authorized individuals.

Q **Is system access limited to authorized individuals?**

A Syngistix Enhanced Security software and the recommended computer/operating system it runs on meets the electronic record requirements of a closed system for 21 CFR Part 11 compliance.

Access to the software is password-protected using a proprietary security module or integration with the company's Microsoft® Windows® Active Directory. If not using the Windows® login option, Syngistix Enhanced Security software can be used to force periodic password changes and render ID/password combinations inactive. If a user is deactivated, records of their activities are not removed and continue to be available for review.

User groups can be created and assigned different privileges consistent with their training. Electronic signatures and read-only access is used to enforce permissions.

Projects or studies may be organized by creating specific directory locations. Groups of users can then be assigned default access to different folders.

The customer will also need to properly configure the local Windows® security on the computer. This includes, but is not limited to, the following:

- Securing setup of the local administrator account
- Disabling guest accounts
- Restricting access to operating system files and controls such as the system clock
- Removing delete ability of the security group to software directories
- Adding/configuring Windows® groups and assigning users to those groups.

11.10 e Use of secure, computer-generated, timestamped 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.

Q Is there a secure, computer-generated, time-stamped Audit Trail that records the date and time of operator entries and actions that create, modify, or delete electronic records?

A The Audit Trail that is created by the system records every significant action performed by the operator that may affect the analytical results or electronic records written to a file or database. A File History database records file names and versions. Any difference between versions can be viewed in ES Tools, complete with timestamp and electronic signatures.

Each Audit Trail entry includes date, time, user ID, username, action performed, action details, electronic signature information, and reasons for the actions where appropriate. A default list of reasons can be customized by the Syngistix Enhanced Security administrator. Where a reason for an operation is required, users can select from the default list, select from the default list and annotate, or provide a different reason.

The Audit Trail records are saved in a password-protected database.

Q Upon making a change to an electronic record, is previously recorded information still available (i.e. not obscured by the change)?

A The old version of each file is copied to a File History database, a password-protected database, before the new version is saved. The version number of the file is incremented to indicate that a changed version was created. Any difference between versions can be viewed in ES Tools, complete with timestamp and electronic signatures.

Once analytical data have been acquired, no changes can be made to the original data. Reprocessing data creates a replicate copy of the data, and all reprocessed data is marked as such.

Q Is an electronic record's Audit Trail retrievable throughout the record's retention period?

A The Audit Trail and File History records can be retrieved at any time using the version of the Syngistix Enhanced Security software used to create the record.

Audit Trail and File History records associated with the data within each Project Folder are automatically archived when those dataset files are archived. Once restored, the Audit Trail and File History records can be retrieved at any time using the version of the Syngistix Enhanced Security software used to create the record.

It is the responsibility of the customer to establish secure policies and procedures for the archival and subsequent retrieval of archived data.

Q Is the Audit Trail available for review and copying by the U.S. FDA?

A The Audit Trail and Security Audit Trail can be printed using Syngistix Enhanced Security software.

11.10 f Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Q If the sequence of system steps or events is important, is this enforced by the system (e.g. as would be the case in a process control system)?

A Syngistix Enhanced Security software performs a large number of method and analysis checks to ensure that all settings are valid before analyses are performed. Methods can only be generated and modified by those operators that have been assigned appropriate permissions by the Syngistix system administrator.

Electronic signature points are utilized to ensure that the user is authorized to perform actions as appropriate. Other analytical problems are flagged using pop-up or warning messages.

Users are forced to provide their login credentials to save all files used to generate data records before an analysis can be started.

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.

Q **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?**

A Syngistix Enhanced Security software and the recommended computer/operating system it runs on meets the electronic record requirements of a closed system for 21 CFR Part 11 compliance.

Access to the software is password-controlled using a proprietary security module or integration with the company's Windows® Active Directory. If not using the Windows® login option, Syngistix Enhanced Security software can be used to force periodic password changes and render ID/password combinations inactive. If a user is deactivated, records of their activities are not removed and continue to be available for review.

User groups can be created and assigned different privileges consistent with their training. It is the responsibility of the customer to establish SOPs outlining data system training and user roles.

Electronic signatures and read-only access is used to enforce permissions and are applied to all pertinent operations.

Projects or studies may be organized by creating specific directory locations. Groups of users can then be assigned default access to different folders.

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.

Q **If it is a requirement of the system that input data or instructions can only come from certain input devices (e.g. terminals), 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).

A Syngistix Enhanced Security software is always configured for a single mass spectrometer and only one user can be logged into the system at any given time. The username and user ID are recorded as part of the data saved in each dataset file. User input can only come from the logged-in user or user that supplies their login credentials.

Information received from the instrument is in proprietary format and there is device polling for health status that identifies if the mass spectrometer is connected and operational.

Input files (Method, Conditions, MassCal, Sample) are checksummed and cannot be altered outside of the system. Their content is always validated against a password-protected version of these files.

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.

Q **Does the supplier have a quality management system?**

A PerkinElmer is ISO 9001 certified and develops all products under the ISO guidelines.

Q **Did the supplier train development staff on 21 CFR Part 11?**

A The development teams responsible for the implementation of Syngistix Enhanced Security software features receive training on the meaning and implications of 21 CFR Part 11. This training and subsequent understanding of 21 CFR Part 11 assures that the system has been developed in a manner consistent with the requirements of the regulation.

Q **What are the implications for the end users?**

A The end user is responsible for training their staff on 21 CFR Part 11 and for training their staff on the procedures and policies and intended use of the systems supporting 21 CFR Part 11.

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.

Q **Are there policies in place to hold individuals accountable for record and signature falsification?**

A It is the responsibility of the customer to implement policies describing the accountability and responsibility for the proper use of electronic signatures.

The customer is responsible for notifying U.S. FDA if they intend to use electronic signatures and will need policies and standard operating procedures and training for non-repudiation of electronic signatures.

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.

Q **Is the distribution of, access to, and use of systems documentation controlled?**

A Electronic documents furnished with Syngistix Enhanced Security software are present on the software media and cannot be changed by the user. The media has a part number, which identifies the version of the documents present.

The customer will require SOPs on versioning distribution and maintenance of systems documentation (this may include the vendor-supplied user manual and service manual as well as customer-created SOPs on the operation and use of the systems hardware and software).

The customer will require maintenance and systems configuration management SOPs and records of which the instrument maintenance log is a component.

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 electronic signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Q **Is data encrypted for transmission? Are electronic signatures applied?**

A Syngistix Enhanced Security software is a closed system.

11.50 Signature Manifestations

11.50 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.

Q **Do signed electronic records contain the following related information?**

- The printed name of the signer;
- The date and time of signing; and
- The meaning of the signing (such as approval, review, responsibility).

A Syngistix Enhanced Security software has the ability to apply electronic signatures. The Audit Trail within Syngistix Enhanced Security software saves all data records with the username, date/time of signing and the meaning of the signature.

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).

Q **Are the items identified in [11.50(a)] shown on displayed and printed copies of the electronic record? Are the items identified in [11.50(a)] subject to the same controls as for other electronic records?**

A Syngistix Enhanced Security software displays this information within the software as well as on printed copies of the Audit Trail.

All controlled activities require a two-component signature from a user with valid system permissions for that activity.

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.

Q **Are signatures linked to their respective electronic records to ensure that they cannot be excised, copied, or otherwise transferred by ordinary means for the purpose of falsification?**

A Syngistix Enhanced Security software uses a secure database to link and track all signature associations. This database cannot be accessed or modified by any user.

21 CFR Part 11 Subpart C – Electronic Signatures

11.100 General Requirements

11.100 a Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Q **Can more than one person use the same login information?**

A Syngistix Enhanced Security software provides the utility to use electronic signatures, however user access control should be established by company protocols.

11.100 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.

Q **Is the person's identity verified?**

A Syngistix Enhanced Security software provides the utility to use electronic signatures, however user access control should be established by company protocols.

11.200 Electronic Signature Components and Controls

11.200 a1 Electronic signatures that are not based upon biometrics shall:

Employ at least two distinct identification components such as an identification code and password.

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 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.

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.

Q **Is there control over signing requirements? In particular if there are a series of signings to perform?**

A Syngistix Enhanced Security software requires a unique username and password each time to utilize the electronic signature functionality.

All controlled activities require a two-component signature from a user with valid system permissions for that activity.

11.200 a2 Electronic signatures that are not based upon biometrics shall:

Be used only by their genuine owners.

Q **What are the requirements to electronically sign data/files?**

A Syngistix Enhanced Security software requires a unique username and password to utilize the electronic signature functionality. Corporate policy and user training is required to ensure no sharing of credentials occurs.

11.200 a3 Electronic signatures that are not based upon biometrics shall:

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.

Q **Can anyone log in as another user?**

A Syngistix Enhanced Security software requires a unique username and password to utilize the electronic signature functionality.

Syngistix Enhanced Security software provides the utility to use electronic signatures, however user access control should be established by company protocols.

11.200 b Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Q **Can biometric be ensured to be genuine?**

A Syngistix Enhanced Security software does not use biometric access systems.

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:

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.

Q **Does the system ensure that no two identical accounts can exist?**

A Syngistix Enhanced Security software requires a unique username and password to utilize the electronic signature functionality.

11.300 b Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Q **Does the system force passwords to be periodically changed and also enable ID/password combinations to be rendered inactive without losing the record of their historical use?**

A Syngistix Enhanced Security software uses two-component user ID/password authentication to limit application access. If using PerkinElmer login, Syngistix Enhanced Security software can be used to force periodic password changes and render ID/password combinations inactive. For new user creation, pre-expired passwords are used so that only the user can ever know the account password.

If a user is deactivated, records of his/her activities are not removed and continue to be available for review.

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.

Q **Does the system provide notification of attempted unauthorized access and take preventive measures (e.g. lock a terminal after a specified number of failed attempts, retain card)?**

A Attempted unauthorized access is detected by Syngistix Enhanced Security software and reported on screen at the next login. This event is also recorded in the Security Audit Trail. Syngistix Enhanced Security software can also be used to prevent system access after a specified number of failed attempts to log in.

PerkinElmer, Inc.
940 Winter Street
Waltham, MA 02451 USA
P: (800) 762-4000 or
(+1) 203-925-4602
www.perkinelmer.com

PerkinElmer®

For a complete listing of our global offices, visit www.perkinelmer.com/ContactUs

014657_01 PKI