Reference to the Part 11 Ruling / Requirement		*Comments*
General		
11.10 (a)	Is the system able to detect invalid entries where applicable? (ex. Out of range values, wrong data type etc).	All input, from users or files, are checked for validity.
Records Availability for Inspection		
11.10 (b)	Can the system generate accurate and complete copies of the records in both paper and electronic format (This includes metadata and Audit Trails)	It is possible to display and to print reports including audit trails generated by Peak Spectroscopy Software applications.
11.10 (b)	Can the data from the system (including Audit Trails) be converted into a common format (ex Excel, word ASCII etc).	It is possible to convert all data including spectral data, reports, calibration files, method files and audit trails to common formats including Excel, Word, HTML, PDF, and ASCII.
Records Retention & Retrieval		
11.10 (c)	Can records including Audit Trails be quickly (within 24 hrs) retrieved (electronically) throughout their retention period.	There are no limitations regarding retrieval in Peak Spectroscopy Software applications. It is in the responsibility of the System Administrator to archive the records and Audit Trail properly.

11.10 (e)	Is this Audit Trail secure from being modified/deleted by the user (User can have read only access)	The Audit Trail is embedded in the document. Entries are made automatically. The user is not able to modify the entries. It is only possible to view the content. Any attempt to tamper with the audit trail is detected.

11.10 (e)	Is it impossible to disable the Audit Trail function?	The Audit Trail is permanent and cannot be disabled.
11.10 (e)	Does the Audit Trail record the date and time of the user action, identity of the individual performing the action and reason for the action/change (if required).	YES. All audit trail entries are time-stamped and include the user name and the reason for the change.
11.10 (e)	Is the user restricted from changing the clock that writes to the Audit Trail	Peak Spectroscopy Software uses the security tools of the Windows operating system. If the system is set up properly, YES. The setup of the Windows operating system is in the responsibility of the system owner.
11.10 (e)	Is there a mechanism to ensure that the time and date on the system are correct.	Peak Spectroscopy Software uses the security tools of the Windows operating system. If the system is set up properly, YES. The setup of the Windows operating system is in the responsibility of the system owner.

11.10 (e)	When data is changed or deleted are all the previous values still electronically available.	In a properly configured system, it is not possible to delete or change sample prediction and diagnostic data.
Automatic System Checks		
11.10 (f)	If the process controlled by the system requires sequenced steps, does the system ensure that the actions are performed in the correct sequence.	For routine operation the EZ module is used. With this application it is only possible to follow a predefined sequence of actions. This SOP can be defined by the supervisor/administrator.

11.10 (h)	If it is a requirement of the system that data input or instructions can only come from specific devices (e.g. instruments, terminals) does the system check for correct device.	The software has internal controls to check that only correctly installed and configured devices can be used.
Education of persons involved		
11.10 (i)	Do the persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.	Software development is done by experienced engineers who have the appropriate education. Additionally they are trained on a regular basis. Service is done by experienced engineers who in addition are trained on a regular basis. It is the responsibility of the system owner to ensure that operators have adequate training to operate the instrument and software.
11.10 (j)	Are there written polices that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	This is the responsibility of the system owner.
Documentation Control		
11.10 (k, 1)	Are there adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.	This is the responsibility of the system owner.
11.10 (k, 2)	Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.	New software versions will have a new version number and a new set of documentation and/or documentation describing the changes compared to the previous version. Versions are archived in the Mercurial system, which guarantees time-sequenced documentation. Internal handling of the system owners documentation is in the responsibility of the system owner.

11.10 (k)	If the documentation is created and maintained electronically are changes to the document audit trailed.	Changes to internal documentation are the responsibility of the system owner. Changes to documents are not possible if the operating system is configured properly.
11.70	Are there procedures in place that require the signatory to re-sign the electronic record if it is modified after the signatory has signed the record.	Any changes to documents generated by the system will remove the document signature, requiring re-signing. This function will be audit trailed.
Controls for open systems		
11.30	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 Sec. 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.	Peak Spectroscopy Software is considered to run in a closed system, i.e. the user needs authorization to log into the system. If Peak Spectroscopy Software is used in an open system, it is the responsibility of the system owner to prevent unauthorized access to the system.

Signature Manifestations		
11.50 (a)	Is the following information displayed when a record is signed electronically: 1) Full name of the signer, 2) date and time of the signature, 3) meaning (reviewed, approved etc) of the signature. Is this information stored in the record and displayed immediately after the signature is executed.	YES, the signature of the operator is always associated with a measurement. A signature consists of the date, the name of the signer and the signer's role (reviewed, approved). The information is stored within the signed document.
11.50 (b)	Does the above information appear in all human readable forms (electronic and paper) of the record	YES.
11.50 (b)	Does the information contained in the electronic signature meet all the electronic record requirements (Audit Trail, authority checks etc)	YES, the operator must log on before using the system and authenticate using the User name and Password. Before signing an electronic record the user has to enter his Password again. Both actions are audit trailed.
Signature/Record Linking		
11.70	Does the system ensure that the electronic signatures are linked to the electronic record on which they are executed to ensure that the signature cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	YES. In addition all electronic records are tagged with a MD5 signature (a kind of checksum) that is embedded in the document itself. Any modification of the record is detected by checking the MD5 signature. Signed records are automatically checked for tampering when they are accessed.
11.70	Does the system require the signatory to sign again if the record is changed after the signatory has signed the record.	YES. Any change to a record removes signatures. The record must go through the review and approval process to be re-signed.
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	Unique user logins are assigned to individuals by the system administrator using the 'userAdmin' program that is part of Peak Spectroscopy Software.

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.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
11.100 (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.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
11.100 (c, 1)	The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
11.100 (c, 2)	Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer`s handwritten signature.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
Non-Biometric Electronic Signature Components & Controls		
11.200 (a,1)	Is the signature made up of at least two distinct identification components (ex user id and password)	YES, operators must log-on before using the system and authenticate using the user name and password. Before signing an electronic record the user has to enter the Password again. Both actions are audit trailed.

11.200 (a,1,i)	When an individual executes a series of signings during a single continuous period of system access: a) Does the first signature require all the electronic signature components, b) do the subsequent signings require at least one electronic signature component that is only executable by and designed to be used only by the individual. **Note:** The single electronic signature component should be known only to the owner of the electronic signature (ex password)	YES. A user must enter their username and password when signing a document. This action is audit trailed. The administration of the user names and the Password is the responsibility of the system owner using the supplied userAdmin program.
11.200 (a,1,ii)	When an individual executes one or more signings not performed during a single continuous period of system access: Does the system require that all the signatures be executed using all the components of the electronic signature.	YES.
11.200 (a, 2)	Be used only by their genuine owners.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
11.200 (a, 3)	Be administered and executed to ensure that attempted use of an individual`s electronic signature by anyone other than the genuine owner requires collaboration of two or more individuals.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation.
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.	Peak Spectroscopy Software has been designed for the use of Username and Password for authentication. Biometric systems are not supported.

Controls for Identification Codes/Passwords		
11.300 (a)	Are controls/procedures establishes to ensure the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	YES. This is enforced through the userAdmin program.
11.300 (b)	Are controls/procedures established to ensure that identification codes and passwords are periodically revised	This is enforced through the userAdmin program.
11.300 (c)	Are loss management procedures established 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 enforced through the userAdmin program.
11.300 (d)	Are transaction safeguards established 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.	This is in the responsibility of the system owner. It is recommended to have a clear internal regulation. After a configurable number of invalid login attempts, the user account is frozen until the administrator takes action. The number of invalid attempts can be set by the administrator.
11.300 (e)	Are controls/procedures established for 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.	Peak Spectroscopy Software has been designed for the use of Username and Password for authentication./