

White Paper

21 CFR Part 11 Compliance Position For the SoloVPE System

April 10, 2012

1.0 Abstract

The final version of the 21 CFR Part 11 regulation released by the FDA in March, 1997 provides a framework in which organizations are able to sign, create, store and provide secure access to electronic records. 21 CFR Part 11 provides the guidelines and rules related to copying, access and permissions, audit logs and tracking, version control and the application of electronic signatures to electronic documents. Compliance with 21 CFR Part 11 entails both procedural requirements and software requirements. The procedural requirements include validating the electronic records system, drafting and maintaining standard operating procedures for the use of the electronic records system and ensuring that users of the electronics records system have adequate training about its appropriate use, and administration and their role in maintaining compliance.

The intent of this document is to outline the capabilities available with the SoloVPE System that provide for compliance with the FDA's ruling on Electronic Records and Electronic Signatures (21 CFR Part 11). The document has been prepared with the understanding that Part 11 compliance requires both procedural and administrative controls to be put in place by the organization in addition to the technical controls that are available in the software packages. The capabilities and functions available in the software alone cannot guarantee a compliant implementation and therefore the software provided cannot be certified as compliant. Ultimately, the final decision concerning compliance of any application, including the software provided as part of C Technologies, Inc.'s variable pathlength line of products, rests with our customers and is subject to their interpretation and understanding of the Part 11 requirements.

2.0 Introduction

This guidance is intended to provide substantive information to customers considering the implementation of a 21 CFR Part 11 compliance installation about the tools, capabilities and functionality available in the software provided with the SoloVPE System that relate to a customers' overall compliance plan. The design of the software has taken into account the requirements of the regulation and numerous technical elements have been incorporated into the software to provide both the integrity to achieve compliance and the flexibility to adapt to unique procedures and policies of each customer and installation. Ultimate responsibility for achieving full compliance with the *21 CFR Part 11* requirements lies with the customer and their design, implementation and validation efforts. To the extent possible CTI will work with its customers to understand any perceived gaps in the capabilities of the system and options for implementation and at its discretion incorporation of possible enhancements.

3.0 Background

A successful implementation of the system requires a complete understanding of the capabilities of the software. A complete understanding of the software requires a comprehensive appreciation of the infrastructure of the software environment. In the case of the SoloVPE System, the software platform is constructed from three major components:

- (1) the computer operating system *Microsoft Windows*®
- (2) the spectroscopy environment: *Agilent Technologies Cary WinUV*
- (3) the variable pathlength application: C Technologies, Inc. SoloVPE™ Software

These three core components work cooperatively to create a complete interface for command and control of the SoloVPE Hardware. The Cary WinUV spectroscopy software suite is a complete spectroscopy workbench that was designed to control Agilent's (formerly Varian Inc.) line of Cary spectrophotometers. The platform provides for direct control and configuration of the various hardware systems and their respective accessories creating a common user interface for the development of methods and the acquisition, analysis, and presentation of data both graphically and in reports. It has an array of options that allow for the saving and retrieving data in a number of different file formats. The SoloVPE Software is seamlessly integrated with the Cary WinUV platform since the functional overlay of the variable pathlength capabilities was designed and engineered using Agilent's proprietary ADL (Advanced Development Language) spectroscopy authoring command set. It exists only and exclusively within the Cary WinUV software environment and leverages the core capabilities of the Agilent Cary WinUV platform.




For secured implementations of the SoloVPE System, C Technologies, Inc. recommends the implementation of optional security modules:

- (A) **GLP Administrator** (*Agilent Cary WinUV*)
- (B) **SecureVPE** (*C Technologies, Inc. SoloVPE*)

The use of these optional modules combined with the security options at the network domain and/or workstation level, create three levels of security. This stratification provides the individual or group assigned the task of implementing a compliant system with an array of tools that can be used to customize the overall security structure to support each organizations' policies, procedures and work flows as well as any companion historian, archiving or electronic notebook software in use at that company.

The balance of this document includes more detailed information regarding how these components and the modules work together, the specific roles they each play and some examples and options of how they can be used to achieve a compliant implementation.

In order to highlight which component or layer is being discussed, the following symbols are used throughout the document:

Icon	Layer	Component
	1	<i>Windows (Workstation / Network Domain)</i>
	2	<i>Agilent Cary WinUV – GLP Administrator</i>
	3	<i>SoloVPE – SecureVPE</i>

4.0 Detailed Information

This section of the document provides more detailed information as to how the tools available in the SoloVPE System can be applied to the relevant section of the 21 CFR Part 11 regulations by companies as part of an overall compliance plan.

Controls for Closed Systems

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

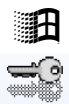


C Technologies, Inc. provides validation services in the form of Installation Qualification / Operational Qualification / Performance Qualification (IQOQPQ) of the SoloVPE System by trained service personnel. This service is included when systems are purchased through C Technologies in order to perform to ensure that the hardware and software is properly installed at the customer location. Following the IQOQPQ the customer's compliance implementation team can begin the process of developing the required policies and procedures and utilizing the tools available with the system in accordance with the compliance plan. C Technologies, Inc. does recommend periodic revalidation of the system and does offer periodic Preventative Maintenance services to SoloVPE owners.

Audit trails in the system provide detailed information regarding system access, performance, use and manipulation to help customer comply with the regulation. Audit trail information is available in all three layers of the system:

- Event Logs and Network Logging can be configured by the customer to control and monitor access.
- The Agilent Cary WinUV environment maintains a verbose audit trail that is saved with each data file.
- The *GLP Administrator* maintains a log of the User and Group Security Administration events.
- The *SecureVPE* software maintains an audit trail of the changes to user and group permissions.
- The SoloVPE Software maintains a log of system related events.

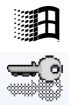
§ 11.10(b) The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.



The Agilent Cary WinUV environment is a complete spectroscopic software platform designed to work with the *Cary* line of spectrophotometers. It has within it the ability to capture, analyze, report and save spectroscopic data. There are a number of proprietary file formats (Batch, Data, Method, Report, and Grams) that the system can create electronically as well as more common files (CSV and RTF). Widely available programs that produce portable document formats such as PDF and XPS, can also be produced when they are installed on the computer system. Hard copy output is also an option when a physical printer is connected to the system.

The ability to create, save, modify and delete these electronic records can be controlled through the customers' appropriate and supportive use of workstation and network file and folder permissions. The customer is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures.

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






The ability to create, save, modify and delete electronic records created with the SoloVPE System can be controlled through the customers' appropriate and supportive use of workstation and network file and folder permissions. The customer is responsible for establishing proper user and group permissions and incorporating their use into the workflow and standard operating procedures. The Agilent Cary WinUV software contains a variety of options for creating output. Some of those options such as Agilent's proprietary Batch files may contain data, report, method, meta-data, audit trail and electronic signature information. Other options, such as a PDF or XPS files, mimic electronic paper and contain an electronic version of the hardcopy that could be produced using an attached printer. Customers must decide which formats are appropriate for their compliance plan and then develop a supportive file and folder permissions approach with the tools that are provided on the SoloVPE System and their own network infrastructure. Additionally, customers must establish the required policies and procedures that deal with appropriate means of storing, archiving, backup and retrieval of electronic records for the duration of the required retention period. This frequently will require consideration of the additional systems and tools that are used by the customer (e.g. document control software, historians, electronic notebook software, LIMS packages, etc.).

§ 11.10(d) Limiting system access to authorized individuals.



Access controls to the SoloVPE System can be set at all three levels of the software to some extent. While this may seem redundant, each layer does provide some unique options and functionality that the customer should consider when developing a compliance plan. While some redundancy exists, each layer does provide unique security tools to the compliance implementation team. The following table provides a basic overview of each layer and explores how they work together to give guidance to the compliance implementation team as to how to incorporate these features into the compliance plan.

Layer	Access Control Overview
	<ul style="list-style-type: none"> Access to the individual computer can be controlled at the local level on the workstation which will run either <i>Windows XP (Service Pack 3)</i> for legacy systems, or <i>Windows 7 (32-Bit)</i> system sold after November 1, 2011. NTFS permissions can be controlled on folders and files by setting User and Group permissions at the customers' discretion. Microsoft provides significant flexibility in establishing security profiles. Configuring these features requires the knowledge and experience of a trained IT professional, whose participation on the compliance implementation team will be invaluable. When customers choose to connect the SoloVPE System computer to a network domain, even more complexity and options for securing the system become available. A network administrator familiar with the compliance plan will be required to ensure that the policies and procedures that have been prepared by the customer are appropriately implemented. The security controls available in the operating system and network afford customers tremendous flexibility to controlling access to the SoloVPE System such as log on monitoring, password group policies such as complexity and expiration, log on attempt tracking and lock out. Additionally, the network framework is frequently the environment in which incorporation with other software packages and systems can be controlled and monitored.
	<ul style="list-style-type: none"> The <i>GLP Administrator</i> is the primary security component of the Agilent Cary WinUV software suite. The <i>GLP Administrator</i> allows users to create unique Users and Groups each with their own specific permission profiles. The permissions that are set in the <i>GLP Administrator</i> program are focused on access to the programs that are available in the Cary WinUV software suite and the authorization to perform certain types of activities in the Cary WinUV Software. Access to the <i>GLP Administrator</i> itself is password protected and an Administrator must be designated to be responsible for creating and modifying settings within the application. The <i>GLP Administrator</i> allows Users and Groups to be added, modified and deleted by the assigned Administrator. The <i>GLP Administrator</i> allows the Administrator to toggle Agilent Cary WinUV On and Off for the computer (Not User or Group specific). This option allows for running the system in fully secured or unsecured mode. When GLP Checks are Enabled, access to all Cary WinUV software application, including the SoloVPE Software is User Name and Password controlled and that user's security profile is enforced. When GLP Checks are Disabled, access control is disabled and the software is unaware of the operation using the system. The specific permissions that can be controlled are: <ul style="list-style-type: none"> Authorize Users/Groups permission to run specific applications. Authorize Users/Groups to Modify Methods they Own Authorize Users/Groups to Modify All Methods Authorize User/Groups to Modify Reports they Own Authorize Users/Groups to Modify All Reports

	<ul style="list-style-type: none"> • The <i>SecureVPE</i> application is an option companion product related to the SoloVPE System Software. As described earlier the SoloVPE functionality exists within the Cary WinUV environment. The <i>SecureVPE</i> application works with the <i>GLP Administrator</i> application in the Cary WinUV Suite to provide expanded security tools that related specifically to the SoloVPE Functionality. • The <i>SecureVPE</i> Software has access control built into it and works cooperatively with the GLP Administration software. The Administrator in the <i>GLP Administrator</i> is also the Administrator in the <i>SecureVPE</i> application. <i>Users and Groups with Administrative rights can be allowed access to the SecureVPE software at the customer's discretion to allow flexibility in customers' compliance plans.</i> • Access the SoloVPE System can be controlled at the operating system level or using the <i>GLP Administrator</i> at the Cary WinUV level. The <i>SecureVPE</i> application provides a third option for controlling access to the SoloVPE software. • The <i>SecureVPE</i> application rides on top of the <i>GLP Administrator</i> application. The system synchronizes Users and Group created in the <i>GLP Administrator</i> with the <i>SecureVPE</i> database. This synchronization is unidirectional from the <i>GLP Administrator</i> to the <i>SecureVPE</i> environment only. <i>SecureVPE</i> make no accommodation for adding or deleting Users and Groups. • The <i>SecureVPE</i> application provides a specific security matrix that relates specifically the SoloVPE Software running in the Cary WinUV environment. The permissions options have been designed to provide the customer and the Administrator control over access to specific features and functions in the SoloVPE environment. In some cases permission settings may toggle a button state between enabled and disabled, or visible and invisible. In other cases, permissions settings may provide for or revoke the option of performing a certain task, such as performing an electronic signature or whether the Auto Save functionality is enabled. • A complete exploration of the permission settings available in the <i>SecureVPE</i> application is beyond the scope of this document. However, it is critical to understand that the controls provided at this layer of the security structures relate exclusively to the SoloVPE Software and need to be configured in conjunction with the other layers to meet the goals of the compliance implementation team.
---	--

§ 11.10(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.



Extensive audit trails are recorded within the various levels of the SoloVPE Software environment. Customers have extensive options for the configuration of both the computer workstation and the network domain including the tracking of actions by user and the various Event Logs that exist within the *Windows* operating system. The extent to which a customer makes use of these capabilities must be decided by the compliance implementation team and be implemented with their own internal network experts and those decisions need to include their plan for maintain, backing up and archiving the data.

The *GLP Administrator* software maintains audit logs of all configuration changes made in that environment including changes to Users and Groups and changes to both specific and global security settings and permissions. The audit log can be viewed from within the *GLP Administrator* application and cannot be directly edited nor deleted. C Technologies, Inc. recommends that customers create policies and procedures that deal with the retention, backup and archiving of the audit information.

The *SecureVPE* software maintains audit logs configuration changes made to the security settings within the program that apply to the SoloVPE Software environment. Because the User and Group functionality is built on top of the *GLP Administrator* controls, the focus of the Audit Trail activity is on the changes to the permissions for the Users and Groups. The audit trail Reports can be viewed from within the *SecureVPE* Environment and reside within its database which prevents edits and deletion. C Technologies, Inc. recommends that customers create policies and procedures that deal with the retention, backup and archiving of the audit information.

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

C Technologies, Inc. recommends the customers' compliance implementation team develop policies and procedures that utilize the capabilities and functions within the SoloVPE System software to enforce the permitted sequencing of steps and events through the use of operational system checks. The security features of the SoloVPE software, particularly the *GLP Administrator* and the *SecureVPE* package allow customers to setup up users and group with specific permissions to be allowed to create methods, modify methods or simply run methods. When permissions are properly configured users are constrained by the parameters of the method and their specific permissions. Proper configuring of permissions combined with the automatic electronic signature capability allows the customer to ensure the integrity, and authenticity of the electronic record.

§ 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.

The SoloVPE System can be configured to require authority checks to gain access to the system, control the system, make configuration or record changes, electronically sign records and authorize various types of operations. The customers' compliance implementation team is responsible for designing the policies and procedures around the system's capabilities in order to meet their organization's compliance goals. Because there are multiple layers of security features, it is important to consider the specific features available within each layer when designing the security plan, because each can be configured to secure specific types of access, control and data.

In integral part of any security plan must start the computer workstation and the network domain when the system is connected to a computer network. There is a tremendous amount of power and flexibility that can be used within the *Windows* operating system and the network architecture. The power and flexibility comes with a cost however and that cost is the complexity involved with configuring a security configuration that supports the overall goals of the compliance implementation team. It is here that customers must involve their IT Staff to successfully design and implement their computer/network security structure. Issues such as controlling the read and write and modify permissions within the NTFS file system both on the work station and any accessible file servers will be critical to ensure that records can be created, secured and archived correctly. C Technologies, Inc. provides specific information regarding the security requirements of its software packages; however, it cannot provide guidance on the overall network security due to the complexity and variability that exists in the industry. At the most basic level however, *Windows* allows customers to configure unique User ID's (Accounts) that are password protected that can control both access to the computer/network and an overall profile of permissions for that user. When implemented in this fashion the *Windows* login creates a first line of defense for securing the computer system at the time of login and if a logged in user walks away from the computer for a period of time. It can also be used to control where and how file data is created and saved and whether it can be modified, deleted or overwritten.

The *GLP Administrator* is the second security threshold that uses authority checks to secure the SoloVPE System. As described earlier the *GLP Administrator* creates a security structure that relates specifically to the Cary WinUV software suite. The *GLP Administrator* allows unique Users ID and password combinations to be created that are used to secure access to and permissions within the Cary WinUV Software applications including the SoloVPE Software. The user specific permission profiles that are configured constrain which users can access the system and what tasks they can perform when they are working in the Cary WinUV applications including which applications can be access and whether the user as the ability to modify methods or reports. When enabled, the *GLP Administrator* login prompt requires a valid User ID and password combination to be entered in order to successfully access the Cary WinUV applications. Once logged in, the user's specific profile will control what actions they can in the software and with the system.

The final and most focused level of security is controlled by the *SecureVPE* software. The *SecureVPE* software enabled customers to configure a SoloVPE specific permissions matrix for each *GLP Administrator* User ID that works that applies to the SoloVPE Software environment to work in conjunction with the *Windows*, and *GLP Administrator* security profiles. The permissions that can be set using the *SecureVPE* software toggle access to specific features and functions within the SoloVPE software environment providing Administrators the flexibility to control what actions users' can perform when they are using the system. Additionally, the e-signature capability within the SoloVPE software are configured from with the *SecureVPE* environment thus prompting the user to provide authenticated credentials to authorize critical steps in the process.

§ 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.



The *GLP Administrator* and *SecureVPE* software security layers can be configured to prompt the logged in user to record an e-signature through an authentication prompt that requires the logged in user to provide their password before and after critical operations to ensure the validity of the input and output.

§ 11.10(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems has education, training, and experience to perform their assigned tasks.

C Technologies, Inc. has been supporting fiber optic based spectroscopy equipment in the bio-pharmaceutical industry for well over a decade. As part of its implementation of the SoloVPE System, an organization can contact C Technologies, Inc. to request and review aspects of its development policies, processes and procedures as well as employee training and experience.

§ 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.



C Technologies, Inc. recommends the customers' compliance implementation team develop policies and procedures that describe and govern the actions that administrators and end users must perform using the SoloVPE system. For administrators, policies and procedures should be developed for system-related actions such as user and group management, password management, and audit trail configuration and purging. For end users, policies and procedures should be developed for actions such as document and folder creation, data naming conventions and e-signature application, review and approvals.

**§ 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.**



The documentation that C Technologies, Inc. provides with the SoloVPE System, including both the Agilent Cary WinUV Software and the SoloVPE and *SecureVPE* software, is updated and distributed with each version of the software. Each set of documentation are uniquely identifiable as applying to its specific version.

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 confidentiality of electronic records from the point of their creation to the point of receipt.



C Technologies, Inc. recommends the customers' compliance implementation team implement appropriate policies and procedures, given the capabilities and constraints of the SoloVPE System to satisfy this requirement. The SoloVPE System and security capabilities provide specific functionality intended to support compliance as it relates to user authentication, data integrity and confidentiality as follows:

Authentication: System access can be controlled through both the *Windows* operating system / network domain access controls as well as through the configuration and implementation of the *GLP Administrator*.

Integrity: Customers can configure the various security levels in a tiered and complimentary way to constrain the generation, modification and storage of data by specific user ID and through the use of the electronic signatures capability for critical operational steps during system use.

Confidentiality: To ensure confidentiality, C Technologies, Inc. recommends that customers establish appropriate workstation and network security profiles, including local and group policies, that can control what information is visible and accessible based upon authenticated User IDs. Appropriate documented policies and procedures also need to be part of the implementation plan for the organization.

Digital Signatures: The *SecureVPE* software system allows for the implementation of electronic signatures that are User ID and password authentication prompt events that occur at critical points during the use of the system. In addition to the automated prompts, the system can be configured to allow users to initiate electronic signature events at their discretion (for reviews and approvals) and in compliance with customer created policies and procedures.

§ 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.



Electronic signatures are executed by the user through the SoloVPE Software application interface, whereupon the user is required to enter her username and password. The electronic signature is stored with the data in the batch file along with the name of the unique identifier of the document, the signer's full name, the date and time the signature was executed, and the meaning of the signature. The user also has the option to append comments to the electronic signature when at the time it is executed. A human readable text block indicating that the document is digitally signed will be appended to the existing report in the software environment.

§ 11.50(b) The items identified in (a) shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of electronic record (such as electronic display or printout).

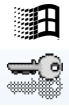


The SoloVPE Software appends a human readable text block with the details of each electronic signature. This information is saved in the batch file and as part of the auditable activity. Because it co-exists with the data, the security and control structure is identical.

§ 11.70 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.

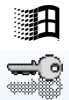
C Technologies, Inc. recommends that the customers' compliance implementation team create the necessary policies and procedures, given the capabilities and constraints of the SoloVPE System to achieve compliance with this requirement of the regulation.

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



C Technologies, Inc. recommends that the compliance implementation team implement policies and procedures to ensure that user names are assigned to only one individual and that each individual agrees not to divulge their password under any circumstances. These policies and procedures must be applied to both the *Windows*/network domain User names and the *GLP Administrator* user names given the capabilities and constraints of those systems. *Note: User names cannot be managed (created, modified or removed) in the SecureVPE software since SecureVPE uses the Users and Groups created in the GLP Administrator application.*

§ 11.100(b) Before an organization establishes, assigns, or certifies an individual's electronic signature, the organization shall verify the identity of the individual.



C Technologies, Inc. recommends that the customers' compliance implementation team incorporate policies and procedures to ensure that usernames are assigned to individuals with proper authorization and approval given their role and responsibilities at the organization and position in the organization structure.

§ 11.100(c) Persons using electronic signatures shall certify to the FDA that they are using electronic signatures intended to be the legally binding equivalent of a traditional handwritten signatures, and may be required to provide additional certification that a given electronic signature is the equivalent of the signer's handwritten signature.



C Technologies, Inc. recommends that the customers' compliance implementation team implement policies and procedures to be able to comply with the certification requirements of this regulation given the capabilities and constraints of the software components of the SoloVPE System. The software components and output options of the system as they relate to for user identifications provide for certifying that the electronic signatures do create legally binding equivalents to traditional handwritten signatures as part of the customers' implementation plan and execution.

§ 11.200(a) Electronic signatures that are not based upon biometrics shall:

(1) 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.

(2) Be used only by their genuine owners; and

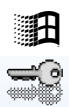
(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

§ 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.

The SoloVPE System does not use biometric authentication techniques. Instead, a user of the system enters her username and password combination to authorize a signature.

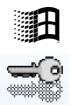
§ 11.300 Controls for identification codes/passwords. Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

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.



C Technologies, Inc. recommends that the customers' compliance implementation team create policies and procedures to ensure the uniqueness of the identification code and password combinations. The *Windows* operating system and network domain management capabilities provide for extensive types of password policies including, complexity, aging, change requirements, lock out, reuse prevention and expiration. Customers' should involve their IT departments to define policies that support their overall implementation plan. These policies should also be applied to the User ID maintenance that takes place in the *GLP Administrator*.

§ 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).



C Technologies, Inc. recommends that the customers' compliance implementation team create policies and procedures to ensure that identification codes and passwords are periodically reviewed and managed as required. The *Windows* operating system and network domain management capabilities provide for extensive types of password policies including, complexity, aging, change requirements, lock out, re-use prevention and expiration. The *GLP Administrator* does not have the same level of sophistication as the *Windows* systems with respect to the creation and monitoring of policies that relate to User ID's and passwords, therefore periodic reviews must be achieved through the proper implementation of administrative policies and procedures.

5.0 Conclusion

C Technologies, Inc., the originator of *Slope Spectroscopy*™ and inventor of the SoloVPE variable pathlength spectroscopy system is committed to working with its customers to achieve the successful implementation and deployment of its technologies. The utility and broad applicability of UV-Vis measurements is reflected in the diversity of our customers and installation sites which range from academic institutions, governmental agencies and companies across a wide range of industries around the globe. Many of our customers are in the bio-pharmaceutical industry and are subject to a variety of regulatory constraints from different nation's agencies and pharmacopeias. C Technologies, Inc. is committed to working with our customers to ensure the capabilities and functionality of its system enable customers to design and implement a compliance installation. Due to the variability and complexity of our customers' regulatory environment, C Technologies, Inc. does not provide a certified turn-key installation service. Instead C Technologies, Inc. through its close relationship with Agilent Technologies and its technical staff provide support services to assist each customers' compliance implementation team fully understand the tools and capabilities and requirements of the SoloVPE System and its software, to help successfully craft a compliance plan that meets their organizational and compliance goals. Ultimately, compliance remains the responsibility of each customer at each install site.

6.0 References

- (1) *Guidance for Industry: Part 11, Electronic Records; Electronic Signatures – Scope and Application* (Office of Compliance in the Center for Drug Evaluation and Research [CDER], FDA August 2003)
- (2) *Federal Register/ Vol. 62, No. 54 / Thursday March 20, 1997 / Rules and Regulations 21 CFR Part 11* [Docket No. 92N-0251] http://www.fda.gov/ora/compliances_ref/part11/frs/background/11cfr-fr.htm

For additional information, please contact:

C Technologies, Inc.
Direct Dial: + (US) 908 707 1009
Solo Service Direct: + (US) 908 707 1201
info@solovpe.com
solovpe.com

Copyright© 2012 by C Technologies, Inc.

The copyright to this material is owned by C Technologies, Inc. This material may not be copied in whole or part without the express, written permission of C Technologies, Inc. The information in this document is subject to change without notice. All rights reserved. All other products or company names are used for identification purposes only, and are trademarks of their respective owners.

* *Slope Spectroscopy*® and *SoloVPE*™ are claimed as trademarks of C Technologies, Inc.

Windows® is a registered trademark of the Microsoft Corporation

Agilent Technologies ® is a registered trademark of the Agilent Corporation

For more information about the SoloVPE and related products, please visit the website at: www.solovpe.com