

# DU<sup>®</sup> 800

## UV/Visible Spectrophotometer



# 21 CFR Part 11

## Compliance Booklet

Version 2.0



## Important Notice

The information in this booklet is provided by Beckman Coulter, Inc. for its personnel and as a convenience to its customers. It illustrates how the *DU 800 UV/Visible Spectrophotometer* and its *System and Applications Software at Version 2.0*, or later, address the compliance issues promulgated in 21 CFR Part 11. For more details on the DU 800 UV/Visible Spectrophotometer system, see the on-line Help file as well as the *DU 800 Installation and Operating Instructions* (512860AC) and the *DU 800 Applications Software Reference Manual* (390398) on the CD-ROM or the hard disk after installation of the software.

The information in this document is as accurate as Beckman Coulter could make it at the time of publication. Changes to the Federal regulations and Microsoft Windows may occur without our knowledge.

If you would like to comment on this document, find an error, omission, or problem of any sort please write to:

Beckman Coulter, Inc.  
Lab Products Organization  
Strategic Marketing  
4300 N. Harbor Blvd.  
Fullerton, CA 92834-3100

The contents of 21 CFR Part 11 are presented here, along with information explaining how Beckman Coulter complies with these requirements. Where procedures and actions are required on part of the organization that uses the system, we have made recommendations based on standard practices. However, because Beckman Coulter has no control over the end-user organization, it is the responsibility of the user's organization to put in place and follow its own procedures and action to comply with 21 CFR Part 11 regulations.

All information in this document is subject to change with notice.

For additional security, certain features of Microsoft Windows may be applied in addition to features already included in the DU 800 System and Applications Software. A good example is the use of an NTFS formatted drive as the destination drive for data files. As an example, the administrator or the MSI/IT group could determine directories in which files are protected against deletion.

Be aware that you may lose some of the convenience and the multi-user capabilities of the DU 800 System and Applications Software when applying certain Windows security features.

## **Contents**

Title 21 Code of Federal Regulations (21 CFR Part 11) Electronic Records; Electronic Signatures came into effect on August 20, 1997 and sets forth criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper. People using electronic signatures must certify to the agency that the electronic signature in their system is intended to be the legally binding equivalent of traditional handwritten signatures.

### **Part 11 – Electronic Records; Electronic Signatures**

#### **Subpart A – General Provisions**

- 11.1 Scope
- 11.2 Implementation
- 11.3 Definition

#### **Subpart B – Electronic Records**

- 11.10 Controls for Closed Systems
- 11.30 Controls for Open Systems
- 11.50 Signature Manifestations
- 11.70 Signature/Record Linking

#### **Subpart C – Electronic Signatures**

- 11.100 Requirements
- 11.200 Electronic Signature Components and Controls
- 11.300 Controls for Identification Codes/Passwords

## Subpart A – General Provisions

### 11.1 Scope

- (a) *The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.*
- (b) *This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.*
- (c) *Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.*
- (d) *Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with Sec. 11.2, unless paper records are specifically required.*
- (e) *Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.*

### 11.2 Implementation

- (a) *For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.*
- (b) *For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:*
  - (1) *The requirements of this part are met; and*
  - (2) *The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.*

### 11.3 Definitions

(a) *The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.*

(b) *The following definitions of terms also apply to this part:*

- (1) *Act means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).*
- (2) *Agency means the Food and Drug Administration.*
- (3) *Biometrics means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.*
- (4) *Closed system means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.*
- (5) *Digital signature means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.*
- (6) *Electronic record means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.*
- (7) *Electronic signature means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.*
- (8) *Handwritten signature means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.*
- (9) *Open system means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.*

## 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:*

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

All parts of the DU 800 System (instrument or optical bench, approved PC, and the DU 800 System and Applications Software) have been fully validated by Beckman Coulter, Inc. The instrument or optical bench ships with a Certificate of Compliance and, in addition, can be certified in the field by qualified service personnel after installation. The Operational Qualification (OQ) program from Beckman Coulter includes different OQ levels and ensures ongoing instrument certification, accuracy, and performance of the system.

When the DU 800 System initializes, a number of Self Diagnostic Tests are performed automatically. The user may continue and use the instrument when all test have passed.

The DU 800 also includes the Performance Validation software to verify specified performance and ensure accuracy and reliability on a daily basis. With the Performance Validation Scheduler, these tests can be scheduled to run automatically and provide a saved and/or printed report after completion. The tests, which are scheduled to be executed automatically, can be selected by the administrator.

Invalid or altered records (DUX data files) will be rejected by the DU 800 System and Applications Software.

- (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.*

The DU 800 System generates and accepts data or records in binary format, called the DUX (DU eXtended) file format. Data and results are viewed and printed in a human readable form. In order to verify Electronic Signature(s) and/or generate human readable records for inspection or review, the DU 800 System and Applications Software must be available. The software can be installed on any computer with a Window 2000/XP operating system and does not require a spectrophotometer to use the respective functions.

Data can also be easily converted to human readable electronic records in the form of CSV (Comma-Separated Values) files, which are compatible with Microsoft Excel and other commercial products. The CSV file contains the decrypted signature(s) and the associated information. Be aware that these records do not contain verifiable electronic signatures since they are designed for use outside of the closed system.

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

Records or DUX files are protected against tampering through their binary format and cannot be altered, falsified, or overwritten using ordinary means. The records are located in user-specific directories on the local drive or a network drive and can, therefore, be easily retrieved.

The System Audit Trail includes a log of all records that have been created on the system. The system audit trail (master) resides on the host computer. A mirror image will be maintained on the destination drive with the electronic records to facilitate retrieval at a later time.

(d) *Limiting system access to authorized individuals.*

Access to the system is limited to authorized individuals through the use of User Names and Passwords.

A. **User** – Level with individual user accounts, user log on, and password protection.

The administrator authorizes access for a user by creating a user account. He/she then informs the user and communicates the initial password. When the user then logs on for the first time, it is recommended that he/she changes the initial password. The user maintains his/her own password utilizing the Password Renewal/Aging feature.

B. **Administrator** – The administrator creates and maintains the User Accounts and controls all system and regulatory features. The administrator also assigns the initial password and the Electronic Signature Privilege(s), which are Author, Reviewer, and/or Approver.

The 'No <Generic User> Access' feature in the Regulatory tab must be activated by the administrator.

(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.*

The Data Audit Trail is embedded in the electronic record (secure DUX file). It is computer-generated, time-stamped and includes all user and method parameters. There can be no operator entries after the electronic record has been created. The record is protected and cannot be altered or overwritten. Any changes made when loading an existing record (e.g.; post-run analysis) must be saved in a “new” electronic record.

Because the content of a record cannot be changed after it has been created, the data audit trail information is considered a “one-time” audit trail and should not be confused with the system audit trail. The data audit trail is embedded in the electronic record while the system audit trail monitors system activity and provides additional information for the administrator.

The System Audit Trail records:

- User log on and log off, including failed log on attempts
- Passwords changes
- Data acquisition and creation of electronic records
- Loading and saving of records
- Copying of methods
- Saving and deleting of methods
- Backup and restoring of system parameters and methods

Each entry in the system audit trail includes a date and time stamp, description of the action, and identification of the user. The system audit trail can be viewed with the DU 800 Software. Checksums are used to protect the information in the audit trail file. The system can be customized in regard to alerts for the system audit trail backup.

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

The design and organization of the software is such that data collection must be preceded by a sequence of pre-requisites, such as operational instrument connection, a valid method, etc. Pre-configured applications can be created to provide “canned” applications that cannot be altered by users. This is accomplished by copying methods to the protected Custom Applications area.

- (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.*

As described earlier, only authorized users can access the DU 800 System and Applications Software through a log on and electronically sign a record or perform the operation at hand. Records cannot be altered. If a post-run analysis is performed on an existing record, a “new” record must be created.

- (h) *Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.*

It is the responsibility of the organization to ensure that all personnel are properly instructed in the operations of the system and that all samples being analyzed are properly identified and labeled.

In addition, the DU 800 System includes the Performance Validation software, which aids the operator in validating data integrity by verifying instrument accuracy and performance on a daily basis.

- (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.*

It is the responsibility of the organization to ensure that individual have the education, training, and experience to perform their assigned tasks.

Beckman Coulter offers operator training and system certification at installation or at the customer's request. The training is documented and performed by qualified and certified service personnel. Certificates are provided for each trainee after a successful training.

- (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.*

The organization must create and implement policies and procedures that specify what it means for people to electronically sign a document. These policies must be made available to the individuals. Administrative actions that will occur as a result of incorrect use of electronic signatures should be included as part of these policies.

- (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.*

All documentation from Beckman Coulter is subject to a rigorous validation process. Its distribution and use is defined in company policies. Sensitive documentation related to system security features are handled separately and are only available to assigned personnel.

The DU 800 System ships with on-line manuals in PDF format, as well as a printed version of the Installation and Operating Instructions. Also included is a context-sensitive HTML Help file. If the organization chooses to print the on-line manuals and/or Help topics or orders manuals, it is the responsibility of the organization to control access to the printed material.

- (2) *Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.*

All documents are under strict Engineering Documentation Control. The on-line manuals (PDF files) and the HTML Help file are updated as appropriate whenever the software or hardware changes. The latest documents are automatically put on the hard disk when new or updated software is installed. For printed documents, the organization must put procedures in place to ensure that the users obtain the proper printed manuals.

The latest DU 800 Software Validation Pack is included in the set of documents that comes with each software version (CD-ROM). A printed version can be obtained from Beckman Coulter.

### **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 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.*

The DU 800 UV/Vis Spectrophotometer system is not considered an open system.

### **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.*

The electronic signature consists of an encrypted form of the user name (identification code), the password, and the serial number of the system. Electronic signature(s) are embedded in the electronic record.

The following associations are included with each signature:

- 1) Printed name of the signer (full name)
- 2) Date and time when the signature was executed
- 3) Meaning of the signature (Author, Reviewer, or Approver)
- 4) Note or Annotation

Up to five electronic signatures can be included in a single record.

*(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).*

All human readable forms of the electronic record contain the decrypted electronic signature(s) as well as the associated information.

### **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.*

The electronic signature(s) are embedded in the electronic record and cannot be excised, copied, or otherwise transferred by ordinary means. A signature cannot be used by any other person, as long as the user's organization maintains proper security control of identification codes and passwords.

## Subpart C – Electronic Signatures

### 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.*

The administrator creates a user account in the User Account Manager and assigns the user name (identification code). The DU 800 System and Applications software only accepts unused or “new” user names. This method guarantees unique combinations of user names (identification codes) and passwords. A used or deleted user account cannot be reused or reassigned to anyone else.

To ensure unique signatures on a worldwide basis, the DU 800 serial number serves as a third part of the electronic signature.

It is the responsibility of the user’s organization to cancel the signature privilege(s) when the person to whom it was issued leaves the organization and/or is no longer authorized to use an electronic signature. In this case, the administrator of the system should remove the signature privilege(s) immediately.

- (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.*

It is the responsibility of the user’s organization to ensure the identity of the person to whom authority for using an electronic signature is granted. The method of identification depends on the organization and the type of work being performed.

- (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.*

- (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 document, which is sent to the agency, should state – for each person – that the electronic signatures are to be considered as legally binding as traditional handwritten signatures. The document should be signed (handwritten signature) by the person in the organization who is responsible for maintaining the uniqueness and security of the electronic signatures.

- (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.*

Such additional information shall be provided with the necessary information and in the format required by the agency. The agency may require this information to be notarized or externally certified in some other manner.

## 11.200 Electronic Signature Components and Controls

(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.*

In order to sign a record (or DUX file), the user must be logged on, using the user name (identification code) and password. In addition, the user account must have at least one of the available 'Signature Privileges', which are "Author", "Reviewer", and/or "Approver". It is the responsibility of the administrator (or organization) to grant the appropriate signature rights to the user.

An electronic signature can only be executed on the DU 800 system. Before executing a signature, the password must be confirmed.

The 'Auto Logoff' feature can be customized by the administrator. It ensures that the system is protected:

- a) if the user fails to log off after completing his/her task, or
- b) when the user leaves the system unattended for a longer period of time (e.g.; a kinetics run). When "idle", the systems logs off automatically after a specified time and the session is terminated. In this case, a new user log on is required. During an "open run", the system goes into a protected mode. In order to return to the application, end the run, and consequently sign the record, the password must be confirmed.

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

To execute the signing of the electronic record, the password must be confirmed.

The user's organization and its personnel are responsible that identification codes and passwords are kept secret and secure so that only authorized people will be able to use them.

(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.*

To use an electronic signature, the person must be logged on as a user with one or more signature privileges. Each user should change their initial password immediately upon first log on. This prevents the administrator (the person that created the user account), from being able to log on as the genuine user.

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

The DU 800 System is not based on biometric identification but three distinct components: the user name (identification code), the user's password, and the serial number of the instrument.

## 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.*

The administrator creates user accounts in the User Account Manager. The DU 800 System and Applications software only accepts unused or "new" user names. This method guarantees unique combinations of user names (identification codes) and passwords. A deleted user account cannot be re-used.

In addition and for unique signatures on a global basis, the DU 800 serial number serves as part of the electronic signature.

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

The Password Renewal/Aging feature of the DU 800 System and Applications Software requires the user to periodically change the password. The administrator can customize this feature to suit the requirements.

- (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.*

Beckman Coulter does not supply security with the DU 800 Spectrophotometer in the form of physical tokens, cards, or other devices.

If the user or any other person believes that a password has been compromised, they should immediately inform the administrator and change their password immediately. In this case, the administrator may also choose to set up a new user account.

- (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.*

As a measure of active prevention, each user should be trained to keep passwords secret and to change the password periodically.

The DU 800 System and Applications Software provides the Password Renewal/Aging feature to assist the users in periodically changing their passwords. After a given period of time, which is determined by the administrator, the user will be automatically reminded to change the password. In this case, the password must be changed in order to log on and use the system.

Three attempts are allowed for the user log on. Unsuccessful attempts to log on to the user level are recorded in the 'System Audit Trail'. The administrator should review the 'System Audit Trail' on a regular basis to detect any attempt of unauthorized use of passwords and identification codes. It is the responsibility of the user's organization to develop the protocols and procedures that determine the review period of the 'System Audit Trail' and to describe the actions that need to be taken to the system security in case of unauthorized use.

- (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.*

There are no tokens or cards as part of the system.

However, a standard bar code reader (not provided by Beckman Coulter) may be connected to the computer. In this case, it is the responsibility of the user's organization to develop the necessary protocols and procedures. If any other devices are added, it is the responsibility of the user's organization to perform the required testing.