Ocean Data Systems

FDA 21 CFR Part 11 Compliance Statement For Dream Report™ 4.x

Revision	Date	Written By	Reviewer By	Approved By	Approved By
1	23.12.2010	I. Tchernogouz Signature	A. Shklyarov Signature	A. Mazal Signature	

Author	Date	Version	Revision	Module
I. Tchernogouz	15.12.2010	4.0	1	Dream Report FDA 21 CFR Part 11 Compliance

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

Table of Contents

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

1. INTRODUCTION

Effective August 20, 1997, the U.S. Food and Drug Administration (FDA) released and published a new rule to enable companies to approve their results with electronic signatures and to transfer paper-trail documentation into electronic records. This rule is known as 21 Code of Federal Regulations, Part 11 (referred to as 21 CFR Part 11) and applies to all industry segments regulated by the FDA. The impact of this rule on current work practices and data handling in various industries has been much higher than expected. "The industry wanted to have a rule on electronic signatures, but what they got was a rule on electronic records" (Martin Browning, former FDA inspector, during a validation seminar in Washington, D.C.)

The requirements on electronic records of 21 CFR Part 11 is not new to the industry as they only summarize several predicate rules. But, 21 CFR Part 11 places high emphasis on the implementation of all measures to protect and secure electronic records. Besides all uncertainties and changes that 21 CFR Part 11 requires in the behavior of the vendors of reporting and analysis software, it is well worth implementing in today's laboratories because it can help the industry with one of the most important issues in pharmaceutical research—bringing new drugs faster to market. The major benefits of this shift towards electronic data management are in the potential productivity increase for the industry. The industry can decrease its data output on paper, speed up the data review and approval process, and benefit from new automation technology based on computerized system control.

The main requirements of 21 CFR Part 11 are data security, data integrity, traceability/audit trails and electronic signatures. Data security and data integrity are maintained by requiring users to login with a valid user name and password. There are then permission tables that delineate what a user has access to and what that user has the ability to do. Anything that is done with the data is logged to the audit trail, thus maintaining the integrity of the data. Capturing the - who, what, when and why of data modifications is the requirement of the traceability/audit trails requirement. This data is captured automatically and includes the user id, the date and time, and what was modified. The data that is not captured is why the data was modified. This data cannot be modified. It is all permanent and readily available in human readable format.

1.1 Purpose

This document describes the Dream Report v 4.0 compliance with the US Food and Drugs Administration's Code of Federal Regulations, chapter 21, part 11 (aka FDA 21 CFR Part 11).

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

Dream Report™ is reporting software. The design and development of the Dream Report™ project and its compliance with the initial requirements or any sort of regulations remains the responsibility of the project developer and does not transfer to Ocean Data Systems.

FDA compliance embraces complete systems including hardware, software, documentation, file & user management, user rules of conduct, company security standards, etc. Taken that into consideration Dream Report™ is only one element in this system chain, Ocean Data Systems (or any other Reporting tool vendor) cannot solely guarantee full compliance; this is dependent upon the environment and methodology with which it is deployed.

Despite that fact, Ocean Data System Company guarantees that, providing the project that follows to these written guidelines will not in itself create any breaches of FDA compliance.

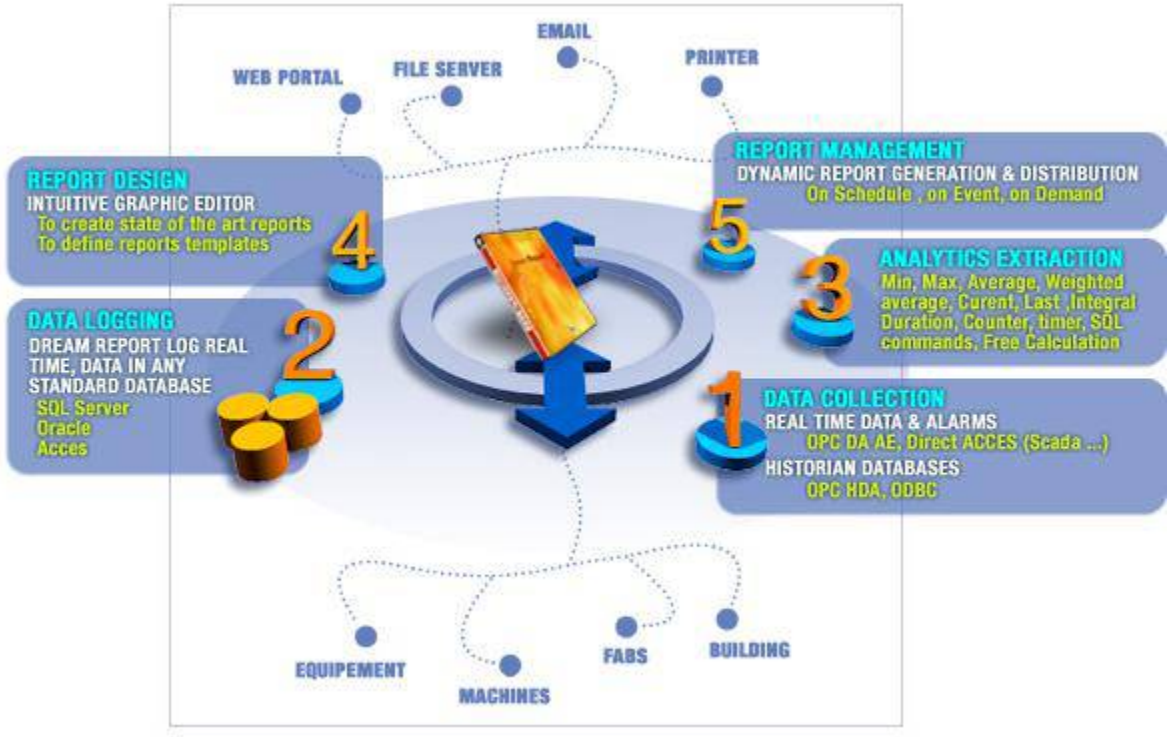
2. ABOUT DREAM REPORT™

Dream Report™ is a real time reporting generator solution based on a configurable End User interface. Its unique concept combines 5 key functions, and positions Dream report™ as the most convenient reporting solution for the industrial automation.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net



2.1 Data Collection

Dream Report™ integrates a robust and secured communication kernel to collect data and alarms from multiple real time and historian sources. It uses OPC, OLE and ODBC standards to securely connect and collect Data from different suppliers. Moreover, ODS develops custom drivers to leverage native history from SCADA systems, DCS, RTU and exclude unauthorized access to that systems.

2.2 Data logging

Dream Report™ integrates a powerful historian module to log clean and accurate data in any standard password protected databases such as SQL Server, Oracle, MySQL, Access. This unique feature position Dream Report™ not only as a reporting tool, but also as the ideal solution of field Data integration for enterprise applications.

2.3 Data extraction & analysis

Dream Report™ integrates a user friendly object library to extract Data statistics and analysis to be displayed in multiple views like tables, Bars, Pies, Charts and more…

2.4 Report Design

Dream Report's studio integrates an intuitive graphical editor to create and save state of the art reports as templates.

2.5 Report Generation & Distribution

Dream Report enables to generate reports manually and automatically. The automatic mode enables to execute report on event and on schedule. When ready, reports can be automatically printed, emailed, stored as secured and encrypted PDF file as well as published over the web.

3. DREAM REPORT USER MANAGEMENT

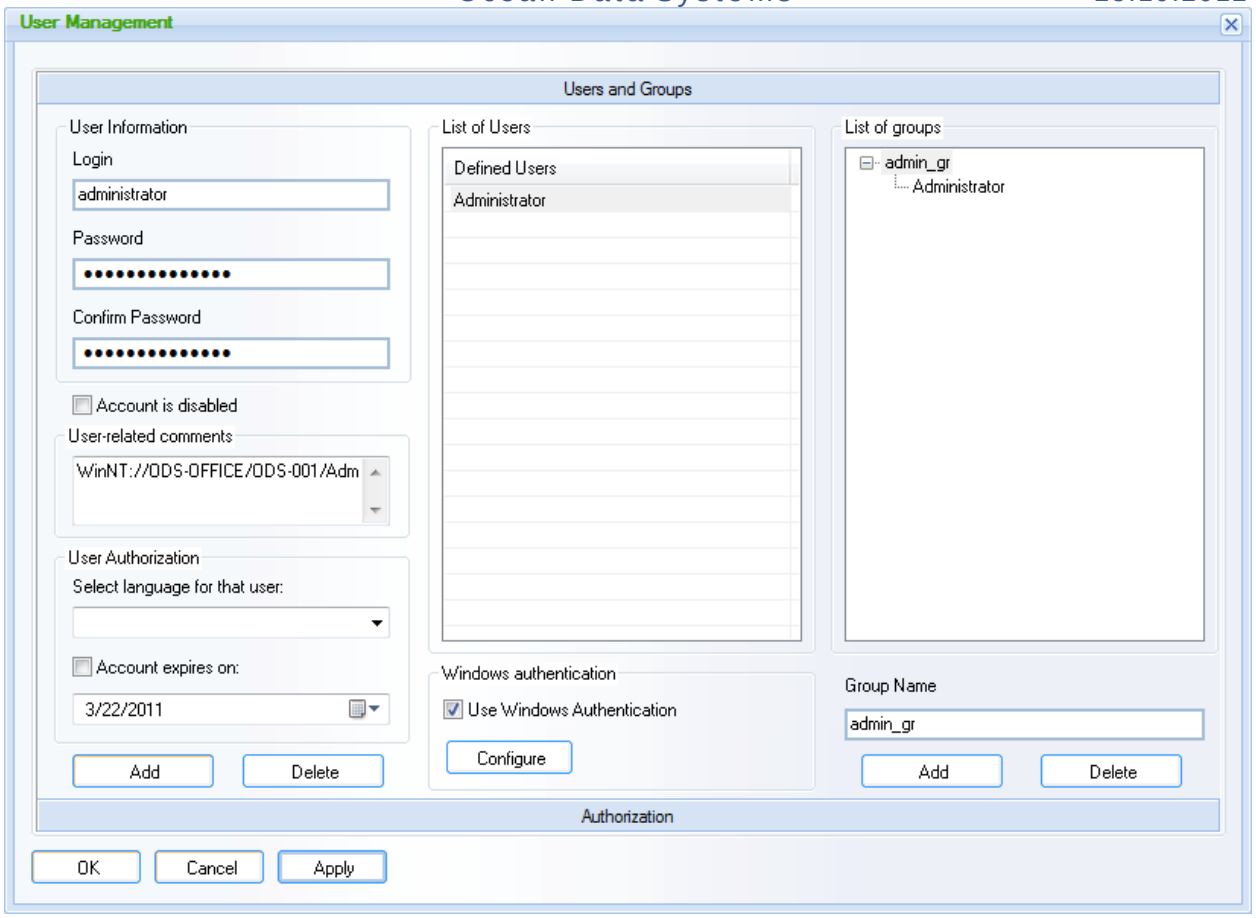
3.1 *Introduction to User's Management of Dream Report.*

Following requirements of FDA 21 CFR Part 11 Dream Report includes two independent identification components: User name and password that gives uniqueness combination to access different project modules, reports or protect stored data.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

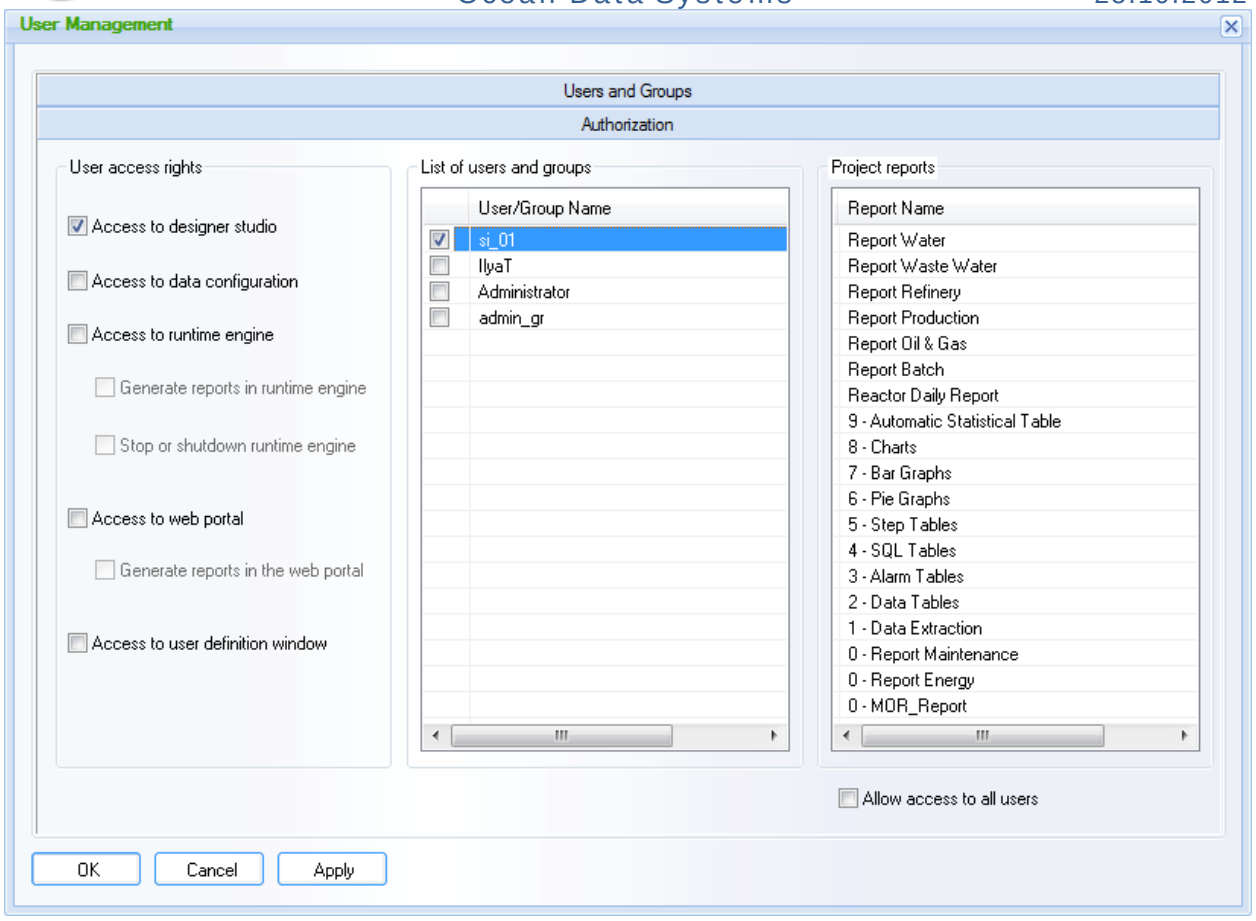


While doing configuration for the authorization access level, user can be limited to get access to different modules of Dream Report as well as to different reports. This configuration can apply to sole user or to complete user's group. It remains the sole responsibility of the project manager to protect those modules from being accessed, modified or renamed, by not properly authorized users.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net



Users must be created by a user that has rights to access UM consol (administrator)

Upon 3 consecutive failed login attempts Dream Report™ studio will be closed and Dream Report™ runtime will continue project launching process without giving any permission to access runtime or to see loaded reports.

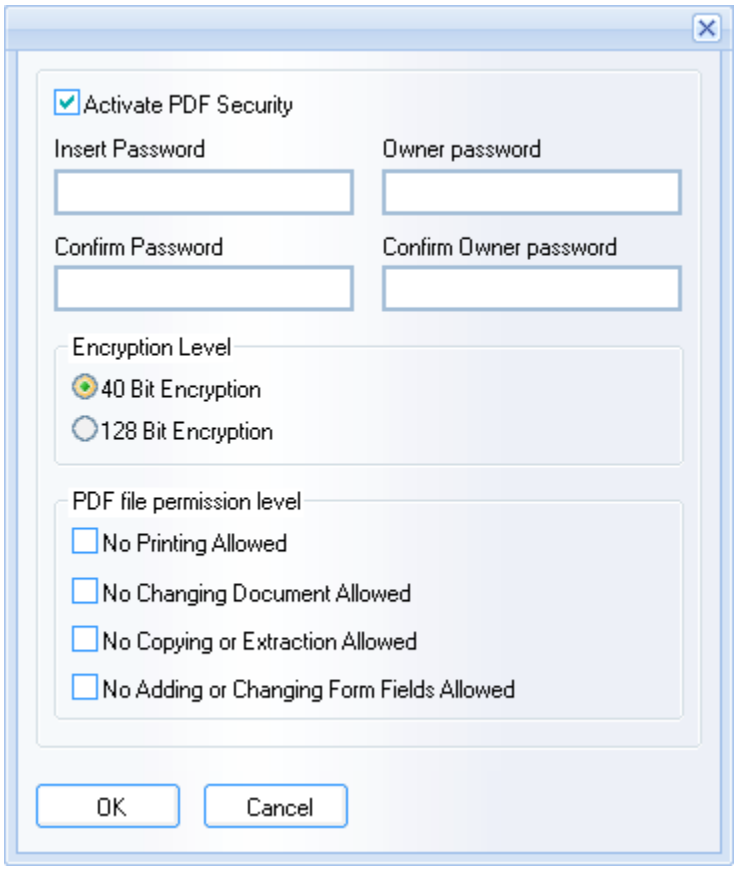
3.2 Implementation of Access rights in Dream Report project.

Users can have a limited access to reports in Dream Report™ project that only that users are allowed to see.

Reports can be generated in PDF file format:

- PDF files, generated by Dream Report™ comply with both PDF security standards: ISO 19005-1:2005, PDF/A-1a and PDF/A-1b. PDF report files can be encrypted (40-bit or 128-bit encryption levels) and/or

- Password protected for observation.
- Password protected for doing any manipulations with pdf file



It remains the sole responsibility of the project manager to keep the configuration tune in a proper way.

- For every report template defined in Dream Report project user can select in which location to store report PDF files, so using that feature user can automatically save PDF reports into separate folders that have different user access rights.

3.3 Implementation of Access rights in Dream Report embedded Web portal.

Dream Report™ has an embedded web portal that allows users to browse and manages their reports over the internet. The web portal can run in fully secured mode under https web access and with full support of SSL certificates. Please note that the configuration of IIS (Internet Information Services) feature inside Windows is sole responsibility of Company IT department where Dream Report™ project is installed.

4. FDA 21 CFR 11 - SUBPART A

General Provisions

4.1 Section 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.

(f.) This part does not apply to records required to be established or maintained by Sec. 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

4.2 Section 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.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

4.3 Sec. 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 (section. 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 writing in a permanent form. The act of signing with a writing or marking instruments 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.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

5. FDA 21 CFR 11 - SUBPART B

Electronic Records

5.1 Sec. 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.

Product compliance: Ocean Data Systems provides all needed tools for generation, development and maintenance of Reporting projects. The design and development of any report project by use of Ocean Data Systems products as well as the verification of its compliance with the FDA requirements and its final validation remain the sole responsibility of the project designer, systems integrator and of the end customer.

(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.

Product compliance: Dream Report™ provides historical data points and historical alarm records in relational and password protected (if set by user) format - as "standard database", any ODBC compliant relational Database is supported.

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

Product compliance: Dream Report™ historical data are stored in password protected relational format, to avoid alteration and falsification it remains the sole responsibility of the user to protect those databases from being deleted, moved, and renamed or from any other actions which could harm the stored data.

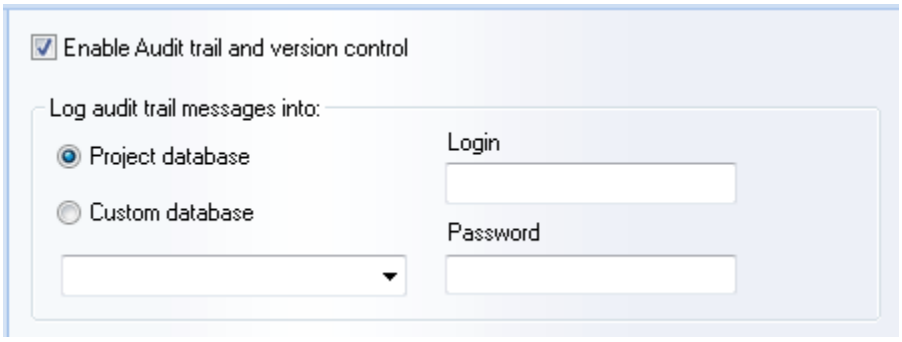
Ocean Data Systems Company recommends taking advantage of Microsoft's integrated User Management to limit access rights to these files.

(d.) Limiting system access to authorized individuals.

Product compliance: Dream Report™ provides an advanced user management defining access rights to the project as described in the Chapter 1 of this document. As required by FDA21 CFR11.200.1, Dream Report™ employs two distinct identification components such as a unique combination of password and login. Regarding general access limitation to the Operating System, Dream Report™ also provides an advanced user management which has direct interaction with Microsoft Windows security mechanism thus enabling the use of the Dream Report™ project only. The use of the above feature is optional, general access limitation can also be achieved using Microsoft's integrated User Management. If it is decided to implement the standard Microsoft user management mechanism for general access limitation it remains the sole responsibility of the customer's IT department to configure, manage and maintain these settings.

(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.

Product compliance: When using Dream Report™ there is no way to alter, falsify or delete a record of the historical data while the database is password protected. However, it remains the responsibility of the customer to protect those files from being corrupted, damaged, deleted, moved or renamed, or from any other actions which could harm the stored data. In case of using an external ODBC compliant relational Database it is the sole responsibility of the Compliance customer's IT department to manage this Database. In case of Ms SQL and records not being encrypted for this type of database, Ocean Data Systems strongly recommends activating the Ms SQL Audit Trail feature in order to trace any manual changes to the records. All user operations in the Dream Report™ project such as report generation on demand, login/logout into/from the Designer studio or Runtime or to the Web portal, are tracked by Dream Report's audit trail mechanism.



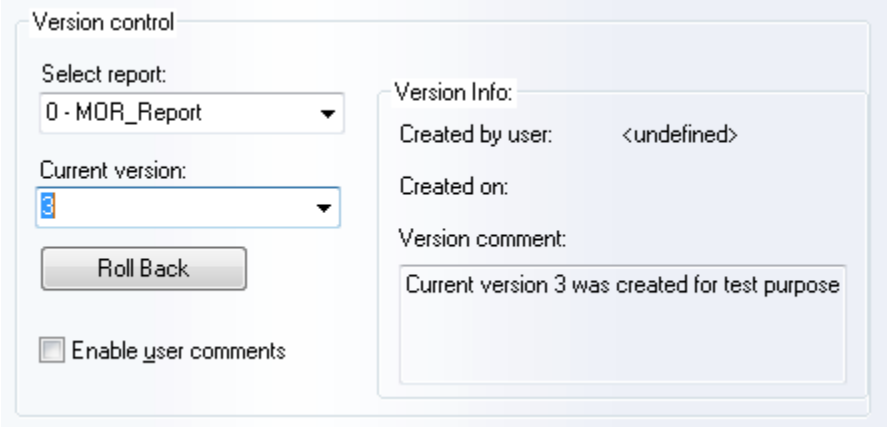
Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

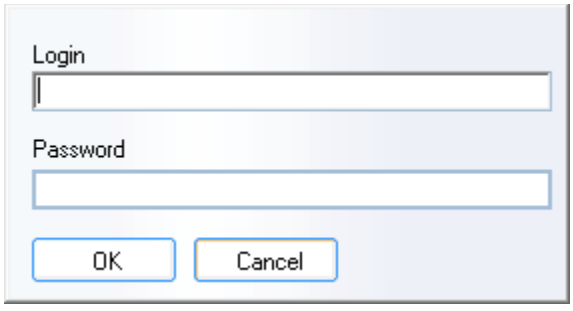
(f.) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Product compliance: Enforcing permitted sequencing of steps and events, as appropriate, can be achieved by implementing sequential Dream Report™ project validation test. It remains the sole responsibility of the customer using various methods to design its project in order to provide the appropriate operational systems checks. As soon as Dream Report™ project had been validated by end customer it can be stored in version control system for future recovering if needed.



(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.

Product compliance: Dream Report™ provides an advanced user management as mentioned in the p 3.1 of this document, defining access rights to the project modules (Dream Report™ Studio, User's Management, DRT runtime, Dynamic Report Generator, Web portal, etc…). As required by FDA 21 CFR 11.200.1, Dream Report™ runs two distinct identification components such as a unique combination of password and login.



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

Product compliance: In addition to the "normal" user login and password required, some installations require specific limitations for terminal. In practice, there can be a limitation when using a Web Client in terms of terminals that are allowed to access the system.

The simplest way to implement this limitation is to use a firewall listing the IP or MAC addresses of the allowed terminals and their actions. It remains the sole responsibility of the customer to chose, configure, manage and maintain these firewalls or/and set VPN connection.

(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.

Product compliance: Dream Report™ user management consists of Users that are assigned to User Groups as described in the p 3.1 above. Usually, access rights in projects are defined at a User Group level. It remains the sole responsibility of the customer to verify that the users configured as being member of a User Group will have the education, training, and experience that corresponds to the tasks assigned to this User Group.

(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.

Product compliance: It's the sole responsibility of the customer to establish and maintain the adherence to such written 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.

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

Product compliance: The customer/systems integrator who has developed a project using Dream Report™ is responsible for writing its own project documentation and maintaining it.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

5.2 Sec. 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.

Product compliance: Dream Report™ is designed for collection and representation of electronic records in a document format only. Modification, maintenance and transmission of such records are not part of the scope of Dream Report™. The establishment of written procedures and controls 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 remains the sole responsibility of the customer.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

6. FDA 21 CFR 11 - SUBPART C

Electronic Signatures

6.1 Sec. 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.

Product compliance: All electronic signatures are composed of a unique set of login and password. It is the customer's sole responsibility not to give an already used set of login/password to another or different operators.

(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.

Product compliance: The verification of the operator's identity before establishment, assignment or certification of an electronic signature (login/password) is the sole responsibility of the customer.

(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.

Product compliance: The certification to the agency by the person using electronic signature that this signature (login/password) are intended to be a legally binding equivalent to traditional handwritten signatures remains under the direct responsibility of the customer. Customer can also add an electronic signature by features available in PDF reader tool.

(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.

Product compliance: The submission in paper form of the certification to the Office of Regional Operations remains under the direct responsibility of the customer.

(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.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

Product compliance: Providing additional certification or testimony upon agency request remains under the direct responsibility of the customer.

6.2 Sec. 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.

Product compliance: Dream Report™ has an implementation of two distinct identification components such as a unique combination of password and login.

(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.

Product compliance: In Dream Report™, the first and all subsequent signings are always composed by the two identification components (login/password).

(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.

Product compliance: In Dream Report™, the first and all subsequent signings are always composed by the two identification components (login/password).

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

Product compliance: Verification and certification that a unique combination of identification components is not used by different individuals is the sole responsibility of the customer.

(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.

Product compliance: It is strongly recommended that the customer shall prohibit the use of an individual's electronic signature by anyone other than its genuine owner.

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

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

Product compliance: Dream Report™ has an option to be configured to integrate the Microsoft Windows user management mechanism which could include the support of electronic signatures based on biometrics equipment to get an access to the system, but it is the responsibility of the application integrator to design, develop and validate the system.

6.3 Sec. 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.

Product compliance: Dream Report™ User Management mechanism prohibits the coexistence of identical sets of signature identification components.

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

Product compliance: Dream Report™ has an option to be configured to integrate the Microsoft Windows user management mechanism which could include mechanism to ensure the periodical checking, recalling and revision of the identification code and password issuance.

(c.) Following loss management procedures to electronically unauthorized 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.

Product compliance: The implementation of such controls as to remove from the system or republish a combination of signature components that has become compromised remains the sole responsibility of the customer or customer's IT department .

(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.

Product compliance: Dream Report™ generates an audit trail log message upon the third failed login attempt and locks the project. The configuration of an urgent reporting (par fax, E-mail, SMS…) linked to such an event remains the sole responsibility of the project designer.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

(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.

Product compliance: Dream Report™ has an option to be configured to integrate the Microsoft Windows user management mechanism which can provide the ability to use SmartCard and eToken or Fingerprint readers. Initial and periodic testing plan for these components remains the sole responsibility of the customer.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net

7. REFERENCES

1. "Electronic Records, Electronic Signatures 21 CFR Part 11," Department of Health and Human Services, Food and Drug Administration Docket No. 92N-0251RIN 0910-AA29. From: *www.gpoaccess.gov/cfr/index.html*
2. Oracle is a U.S. registered trademark of Oracle Corp.

Israel:
19, Idelson str.
Tel Aviv, Israel
Tel: +972 545 742 411
Fax: +972 77 541 06 98

France:
24 Chemin de Verrieres,
Charbonniere Les Bains, 69290
Tel: +33 (0) 4 78 19 83 88
Fax: +33 (0) 9 58 03 39 30

Web site: www.dreamreport.net Email: contact@dreamreport.net