# Force.com and the FDA CFR 21 Part 11 Requirements

## Overview of Capabilities to Enable Compliance

Version 4, Nov '14

Last Updated: November 10, 2014

# Disclaimer

This statement does not confer legal advice, and should not be taken as a substitute for advice, nor consent by qualified counsel. Nothing in this document is a warranty or guarantee for compliance with U.S. Food and Drug Administration (FDA) regulations, including 21 CFR Part 11, the U.S. Food, Drug & Cosmetics Act (the “Act”), or U.S. Code or predicate rules.

# TABLE OF CONTENTS

# Overview

This document delineates how the Force.com platform can provide companies the necessary tools to achieve and maintain compliance with 21 CFR Part 11[1] (hereto thereafter termed as “Part 11”) requirements in their regulated applications built with Force.com.

Life Sciences firms face the challenge of not only following exacting GxP regulations in their operations, but to do so with electronic systems conforming to Part 11 regulated requirements. The intent is to reduce paperwork burdens and speed regulated product approvals by eliminating wet-ink signatures, while lowering the costs of review, approval and transmission of critical, regulated documents.

21 CFR Part 11 is a regulatory requirement for firms which want to use electronic records and electronic signatures in record-keeping of their regulated information. Examples of firms using these technologies which must comply are those involved with the manufacture, distribution, handling or warehousing of biologics, drugs and medical devices.

Other entities that use electronic record keeping and electronic signatures increasingly include commercial manufacturers (for clinical or approved drug batches) and contract research organizations (CROs) that provide essential services as part of clinical trials management services.

To assure the use of electronic signatures and electronic record-keeping are at least equivalent in authenticity and attributability to their hard-copy counterparts, it is the responsibility of firms using these technologies to comply with Part 11 requirements.

Part 11 does not apply to systems which have no application whatsoever to FDA-regulated products, such as most financial or human resources applications[2]. While Part 11 provides general guidelines for meeting FDA requirements for the validation of computerized systems, it does not provide hard and fast rules for every situation with regard to exactly how compliance can be achieved. For this, each company must rely on their own interpretation, industry guidelines and best practices, and apply these to their internal systems and procedures.

Computerized systems that maintain electronic records must provide assurance that:

- The information stored in the system is valid and reproducible
- The responsible party has certified the entirety of the records
- Dates cannot be altered and signatures are irrefutable representations of the person’s affirmation of their legal, binding signature where applicable

Force.com has features which together provide the capabilities for companies to achieve and maintain compliance with Part 11 in their applications, which will be described below for each section of Part 11. The proper configuration, deployment and management of these features are the responsibility of the Salesforce customer and system developer, and this will be indicated in more detail in the sections below.

[1] The term 21 CFR Part 11 refers to the Code of Federal Regulations <CFR>: Food and Drug Administration Title 21 Chapter 1, Part 11- Electronic Records; Electronic Signatures.

[2] Few exceptions exist. For human resources, in an example where GMP training of manufacturing personnel is recorded in a system and affirmed through the use of electronic signature, Part 11 requirements must be followed.

# Background of 21 CFR Part 11

Part 11 provides requirements for life sciences firms wishing to certify that electronic records and electronic signatures are trustworthy, reliable and equivalent to paper records and “wet ink” signatures. These two requirements are defined here:

Electronic records - defined as “any combination of text, graphics, data, audio, pictorial, or other information in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.”[3] These records are those regulated by the FDA which are in electronic form, whether or not submitted to the FDA but required to be maintained by predicate rules (see below).

Electronic signatures - defined as “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.”[4]

Part 11 applies to records and signatures required by predicate rule. Predicate rules are requirements set forth in applicable regulations which require records and/or signatures, and where those regulated records and signatures are to be originated in electronic form. Examples of requirements are those set forth by the Act, the Public Health Service Act, CFR, or any regulations which form the basis for Good Manufacturing Practices, Good Laboratory Practices, or Good Clinical Practices. These rules mandate what records must be maintained, including the validity of the content and any required approvals.

To be clear, Part 11 does not make electronic record keeping or signatures mandatory, but rather describes the technical and procedural requirements that are to be met if that route is chosen.

The latest guidance for Part 11 which was issued in 2003 clarified the scope and application and identified the aspects of enforcement discretion which can be exercised. Currently, these regulations are under review for amendment. FDA-regulated firms who maintain data using electronic recordkeeping, for example, must ensure that the system functions as designed, and in a manner in which data integrity is maintained. These regulations also require that firms shall have procedures and processes which govern these electronic systems to achieve and maintain compliance. By utilizing Part 11, life sciences companies can demonstrate compliance by deploying systems where the records provide assurance of authenticity, are of high integrity and are confidential and auditable. Part 11 compliance also means that these systems can only be accessed, manipulated and signed using authorization schemes that ensure security and authenticity of the data.

# 21 CFR Part 11—Electronic Records; Electronic Requirements

Summarized below is a detailed point-by-point evaluation of Part 11 sections, and the manner and extent to which the controls associated with Force.com supports compliance with the regulation.
Authority: Secs. 201-903 of the Federal Food, Drug, and Cosmetic Act (21 U.S.C. 321-393); sec. 351 of the Public Health Service Act (42 U.S.C. 262)

[3] Federal Register Vol. 62, no. 54/Rules & Regulations/Part 11, sec. 11.3(6) Electronic Records
[4] Federal Register Vol. 62, no. 54/Rules & Regulations/Part 11, sec. 11.3(7) Electronic Signatures

# 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 § 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.*

*Force.com applications capture and store records in a centralized secured database. These records are maintained and controlled in a secure environment with strict physical and logical access controls, which are detailed below in their respective sections.*

*(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.*

*The Force.com platform provides the infrastructure to support the transmission of electronic records, which can be tailored to each customer's regulatory submission requirements. Our AppExchange (https://appexchange.salesforce.com/) partners can also provide solutions to our customers requiring to perform electronic submittals. Force.com developers also have access to a wide range of reporting and formatting tools to enable output of data to meet varied regulatory format requirements.*

## 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 mean 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 content of electronic records that are on the system.*

*(5) Digital signature means an electronic signature based upon cryptographic methods of originator authentication that is 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 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:

Based on Section VI Definitions (§ 11.3) 41.- the agency states that the most important factor in classifying a system as closed or open is control of the access to the system by the party responsible for the system's electronic records. A system is closed if access is controlled by the party responsible for the contents of the records. The Force.com platform meets this critical criterion by default since only the customer has configuration and data access to their instances, and as such may be qualified as a closed system.

A customer can also configure their instance to only allow specific IP ranges to access the system thus keeping access secure within the customer's network.

Salesforce recommends to our Life Science customers that procedures be implemented which detail any provisioning of access for support by Salesforce or any AppExchange partner to maintain compliance with this definition of a closed system if required.

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

*Several third-party organizations specialize in cloud system validation and provide professional services to Salesforce life science customers.*

*AppExchange partners have created Qualification and Validation Accelerator Packages for the Force.com platform, as well as applications currently being used by our Life Science customers.*

*Conformance with this requirement is the responsibility of the 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.*

*The Force.com platform provides extensive reporting capabilities, which can be tailored by customers to satisfy business and regulatory requirements. Reports can be generated in both electronic and hard copy form. All customer data stored within the platform can be exported in a variety of formats for the purposes of review, audit, and archive and electronic transmittal.*

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

*All Force.com supported transaction records, as well as audit trail logs, are maintained in the secure multitenant database of the Force.com platform. Access to the data is limited to specific individuals or groups based on user defined security configurations. The modification and/or deletion of records is restricted, to ensure integrity throughout the record retention period. All records and associated audit trails are available for retrieval until they are purged from the* *repository by an authorized user or when the records are removed from the recycle bin. Your Recycle Bin record limit is 25 times the Megabytes (MBs) in your storage. For example if your organization has 1 GB of storage then your limit is 25 times 1000 MB or 25000 records. If your organization reaches its Recycle Bin limit Salesforce automatically removes the oldest records if they have been in the Recycle Bin for at least two hours.*

*User Access and Setup Audit Logs can be downloaded by an authorized user. The logs only contain data for the past six months and should be downloaded based on customer's policies.*

*Salesforce recommends that customers develop policies and procedures covering records retention (i.e. how long a record should be maintained) and disposition (i.e. what is done with the record at the end of its lifecycle). The policy should include specific rules for deleting, purging, or archiving records at the end of their lifecycle. Salesforce can assist in the development of these policies and procedures as well as in system configuration. The AppExchange also offers third party solutions for data archiving from Salesforce partners.*

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

*All Force.com supported electronic records, as well as audit trail logs and any reason for change records, are maintained in the secure multitenant database of the Salesforce platform. Record access is controlled by use of a unique sign-in (username) and password pair or other authentication methods: Sing Sign On or LDAP. Multiple levels of security and limitation of access to records are based on user roles and responsibilities. Salesforce recommends that customers implement policies and procedures to control the circumstances under which system access is granted as well as the user roles that define such access.*

*The Force.com platform monitors and logs all access attempts, recording the username used, the date and time of the access attempt, the application connecting, IP network address and whether the attempt was successful or not.*

*(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 as long as it is required for the subject electronic records and shall be available for agency review and copying.*

*All Force.com electronic records (objects) contain a minimum of two date and time stamps: creation date and last modified by date and time. Also, all electronic records contain information identifying the user who created or modified the record. When an electronic record is changed on an audited field, the date, time, and action are recorded, along with both the previous and changed field values, which are recorded in fields flagged for audit history. All audit trail records are maintained and can be archived for maintenance and stored for the required time periods.*

*Change-history tracking provides for automatic data and user name assignment to entries and edits in the transaction history log, enabling tracking and accountability. These records are not modifiable by normal means.*

*The Force.com audit trail is sufficient for meeting many Life Science application requirements, but it has some limitations. For example, the audit trail performs an audit on a maximum of twenty fields, and it does not perform full audits on long text fields (>255 characters), in which case it provides audit information no more detailed than “Field is changed.” Our AppExchange partners have created life science audit trail solutions that address these limitations if required by a customer.*

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

*The Force.com platform data collection and update operations are governed by a robust workflow engine embedded in Force.com. Application developers define these workflow steps to implement required business processes, which limit operators or users to specific functions and controlled entries or responses based on their defined role and security profile in the system. Force.com workflows can be used to ensure that the sequence of events prescribed in the customer's policies and procedures for a given business requirement is strictly observed and documented.*

*(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 Force.com service maintains a list of users, roles, access rights, user licenses, and permission sets within its multitenant database. User authentication is provided by a unique sign-in and password maintained within the database (user configurable).*
*When a customer is using the Force.com authentication service and not Single Sign-On (SSO):*

- *Only secure hashes of user passwords are stored within the database*
- *Password complexity requirements inhibit the use of weak passwords*
- *Password aging forces users to change passwords after a specified period of time*
- *Password recycling inhibits users from reusing a password for a specified period of time*
- *Automatic account lockout guards against unauthorized use*
- *Automatic session sign-out after a specified idle period forces an additional sign-in to continue system access*

*Single Sign-On (SSO) can be implemented as well, allowing our customers to leverage the access and security policies already in place within your corporation.*

*It is the customer's responsibility to configure the above authority checking features in accordance with their security policies to ensure compliance.*

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

*Data input validation requirements can be configured by the customer/developer in their applications to protect against the entry of unreasonable data—thereby guarding against obvious data entry errors.*

*In addition, a customer's instance can be configured to permit only certain IP addresses (terminals) to access the system, and to challenge an unidentified terminal access attempt via a required special access code supplied by Force.com either by SMS or email to a pre-authenticated user address.*

*Mobile device access can be controlled as well, and an authorized user can grant or revoke access to any device or terminal depending on the customer's unique configuration.*

*Salesforce recommends that customers develop security policies and procedures for both remote (e.g. by applications or integrations) and programmatic access modes (e.g. API) to their data repositories.*

(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.*

*A wide variety of training and educational services tailored to meet the requirements of the various categories of users who will utilize the Force.com platform are offered by Salesforce. Additionally, Salesforce works closely with clients to customize training classes based on their specific needs.*

*Conformance with this requirement is the responsibility of the customer. Customers can document the use of Salesforce training classes or media within their learning management processes, in accordance with their internal quality system, to comply with this requirement.*

(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.*

*Salesforce recommends that customers implement policies and procedures to cover the actions that administrators and end users must perform when using the Salesforce 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 data archiving and purging among others.*

*For individual users, policies and procedures should be developed for actions such as account and data security, electronic signatures, data entry and data updates unique to each workflow.*

*Conformance with this requirement is the responsibility of the customer.*

(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.*

*Salesforce provides and maintains documentation for the Force.com platform and the Salesforce applications in electronic form. This documentation should be included or referenced in part or in whole with the customers' own specific systems documentation. The Force.com platform can also be configured to support customized or application specific electronic help tools within the customer's application interface.*

*Salesforce has internal processes in place for the versioning and release of the manuals and release notes for the Force.com platform and associated Salesforce applications.*

*Salesforce recommends that customers develop policies and procedures covering the versioning and control of their Force.com custom and package application system operational documentation, system maintenance schedules and application update activities.*

## § 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in § 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Based on Section VI Definitions (§ 11.3) 41.- the agency states that the most important factor in classifying a system as closed or open is control of the access to the system by the party responsible for the system's electronic records. A system is closed if access is controlled by the party responsible for the contents of the records.

The Force.com platform meets this critical criterion and may be classified and qualified as a closed system since by default the customer is the only party authorized to access and control its instance and transaction records within the Force.com database.

However, in certain circumstances, the Force.com platform may also be classified and qualified as an open system. When a customer has Premier support with dedicated administration, the system can be qualified and classified as open. In these cases, the additional controls required by open systems are required for the Force.com platform.

The Force.com platform has provisions which addresses the controls required for either open or closed systems. Salesforce recommends that an organization implement usage policies and procedures to satisfy this requirement for open systems. The Force.com platform provides user authentication, data integrity, and confidentiality features as follows:

- Authentication: System access is controlled through the use of usernames and passwords. For more information, see the response to Requirement 11.10 (d).

- Integrity: Users with appropriate permissions may add and update records as allowed by their level of permissions as defined in their assigned user profile for a customer's application. Each activity is audited, and the values of the record prior to an update are recorded in the audit history for that record. The ability to delete an object can be strictly controlled through the use of record- and field-level permissions. Change-history tracking provides for automatic data and user name assignment to entries and edits in the history log, enabling tracking and accountability.

- Confidentiality: To ensure confidentiality, Force.com is deployed in a secure communications network employing the Secure Sockets Layer (HTTPS) security mechanism, which encrypts the data stream between the browser and the server. Configuration access can be limited to a specific, predefined set of users and associated IP addresses. Access permissions are extremely granular and extend to individual fields within any record in the system. Authorized administrators can modify the permissions to restrict access to confidential records. For more information, see the response to Requirement 11.10 (g).

- Digital Signatures: Salesforce has AppExchange partners which provide a component that supports digital signatures. This component can be installed into a customer's Salesforce account. For more information, see the response to Requirement 11.50. The Force.com platform does not directly support biometric devices such as fingerprint recognition and retinal scanning.

### § 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.*

(b) *The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).*

### §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 Force.com platform provides the tools (e.g. APEX, VisualForce) to manifest, print/or display and link the electronic signature to meet the requirements of §11.50 and §11.70, but would require custom development by the customer to fulfill.

Our AppExchange Partners have provided package solutions to meet this requirement for our Life Science customers. Salesforce recommends that any such solution leverage the many electronic account security and record control features provided by the Force.com platform previously described.

## 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.*

---

*Should electronic signatures be implemented by the customer, the solution should incorporate the Force.com username and authentication methods implemented by the customer based on their security policies. As such, each Force.com user is identified by a unique identifier in the database that cannot be deleted or removed, and whose further use can be disabled by an authorized administrator. These identifiers are linked, thereby uniquely identifying the user who created or modified a record. As a further security measure, if SSO is not being implemented, new users are required to specify a unique password during their first use of Salesforce. This ensures that the user, and no one else (not even the administrator), have access to their password.*

*Salesforce also recommends that customers implement policies and procedures to ensure that a given username is assigned to only one individual, that all individuals set their own password at the first login, and that all individuals agree not to divulge their password, and users formally* *acknowledge the equivalence of electronic signatures to a handwritten signature where applicable. For more information, see the response to Requirement 11.10 (d).*

*(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.*

*Salesforce recommends that the deploying organization implement policies and procedures to ensure that usernames are assigned to individuals only with proper authorization and approval from their superiors in accordance with their internal account security administration policies. Customer training programs should also be established to document the user's agreement to these policies.*

*Conformance with this requirement is the 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 and equivalent to traditional handwritten signatures.*

*(1) The certification shall be signed with a traditional handwritten signature and submitted in paper form to the Office of Regional Operations (HFC–100), 5600 Fishers Lane, Rockville, MD 20857.*

*(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.*

*Conformance with this requirement is the responsibility of the customer.*

## § 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.*

*(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.*

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

*The Force.com platform provides the tools (APEX, VisualForce, Workflow and Approval Processes) to meet this requirement but would require custom development to accomplish.*

*Our AppExchange Partners have provided solutions to meet this requirement for our Life Science customers.*

*As mentioned above, Salesforce does not directly support biometric devices such as fingerprint recognition and retinal scanning.*

## § 11.300 Controls for identification codes/ passwords.

Persons who use electronic signatures based upon the 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 Force.com security service will only allow unique usernames within any instance of Salesforce. A user cannot have a duplicate account username in any Salesforce instance as only one security controller is used and each username is identified only to one instance.*

*It is the Customer's responsibility to control the administration of accounts and respective usernames to ensure accounts are issued only to authorized users and conform to the customer's security and compliance policies.*

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

*If properly configured by the customer, all passwords must be changed immediately upon first use by a newly authorized Force.com user.*

*Password aging requires users to change their password after a specified period of time (user-configurable).*

*Password reuse/recycling is managed so that a user may not reuse a previous password for a specific amount required password changes (user-configurable).*

*If a customer is using SSO then the authenticating system shall control the password policies for the Force.com instance.*

*Conformance with this requirement is based on the customer's proper configuration of the account security administrative configuration based on their security policies.*

(c) ***Following loss management procedures*** *to electronically de-authorize 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.*

*If a customer has configured the instance to only allow access from the corporate network and is using a VPN authentication device for example, then it is the customer's responsibility to have procedures in place for reporting lost or stolen authentication devices. If tokens are used, Salesforce recommends that the customer have documented procedures or policies in place to address this requirement.*

(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.*

*All records of system access attempts are maintained in the login history list within the Force.com database. This information includes:*

- *User to whom access is being granted (username)*
- *Login time of access*
- *Source IP address of the computer where access occurred*
- *Login type for which access is being granted*
- *Outcome of the login attempt*
- *Browser program used for access to the application*
- *Computer platform used for access*
- *Application name*
- *Client version of the login application*
- *API type and version if the login is programmatically based*

*All records of access violation are maintained in the Force.com database and may be displayed online by an authorized Administrator. Additionally a trigger can be set and workflow rules created to notify appropriate individuals when a lockout occurs due to a pre-set number of failed sign in attempts. If SSO is used the customer should have procedures in place to address this requirement.*

*Salesforce recommends that the customer have procedures in place for the review/audit of the security logs on a periodic basis.*

*Salesforce encourages all of their customers to report any security concerns to security@salesforce.com immediately; any known issues are also available to be viewed at trust.salesforce.com.*

(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.*

*If a customer has configured the instance to only allow access from the corporate network and is using a VPN device for example, then it is the customer's responsibility to have procedures in place for the testing or maintenance of these devices. If tokens are used, Salesforce recommends that the customer have documented procedures or policies in place to address this requirement.*

# Summary and Conclusions

This white paper has demonstrated that the Force.com platform natively provides Salesforce customers with a wide array of best in class security, data management, data reporting and audit trail capabilities which together enable compliance with FDA 21 CFR Part 11 requirements.

Certain specialized capabilities which may be required by regulated customers (such as electronic signatures, archiving and audit trail tracking for long field lengths) can either be custom developed using the Force.com development tools, or acquired from a host of Salesforce partners on the AppExchange.

As for any sophisticated IT system development and operations platform, compliant use of the Force.com capabilities is dependent upon customers taking responsibility for the understanding of the platform, and proper configuration and management of their Force.com instances within the documented quality and IT policies for their organization. It is recommended that any deployment of a regulated system by a Salesforce customer be executed in concert with the organization's quality and validation units to ensure compliance with internal and regulatory compliance policies.

Salesforce and its compliance and our Independent Software Vendor (ISV) partners are available to assist you in the assessment, design, implementation and validation of the custom or packaged solutions you deploy on the Force.com platform to ensure your compliance with Part 11 and other regulatory requirements.