21 CFR Part 11 Compliance Assessment

Veeva delivers regulated content management applications for key areas of a life sciences company, from R&D, to clinical trials, quality and manufacturing, and global regulatory approvals.

Veeva R&D applications are built on the Vault Platform, and are designed to manage controlled documents for life sciences organizations, as well as produce secure and compliant audit trails and electronic signatures in accordance with the FDA's 21 CFR Part 11, EU Annex 11 (Europe), and other industry compliance standards.

These standards define regulatory compliance requirements for the validation and maintenance of computer systems used for managing the regulated records that are mandated as part of life sciences product development and marketing activities.

As a modern cloud provider, Veeva deploys and maintains software applications that satisfy predicate rule requirements such as those found in GLP (Good Laboratory Practices), GCP (Good Clinical Practices), and CGMP (Current Good Manufacturing Practices).

About this Document

The purpose of this document is to provide clarification and guidance for customers regarding the applicability of the 21 CFR Part 11 requirements to Veeva processes, personnel, and products. Each section and sub-text of FDA 21 CFR Part 11 was evaluated for relevance to Veeva practices and Veeva Vault. Where applicable, a statement of compliance is provided.

Customer responsibilities have been highlighted where applicable. Full compliance may require a function or feature implemented in Veeva software products, or a service Veeva performs in support of customers' predicated activities.

About 21 CFR Part 11

On **March 20, 1997** (Federal Register Vol. 62 No 4), the Food and Drug Administration (FDA) published a set of regulations that define "*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."*

The regulation is divided into three subparts that cover:

a) General Provisions

b) Electronic Records

c) Electronic Signature

In **2003**, the FDA published guidance on the application of Part 11, indicating agency intent to enforce "*all predicate rule requirements, including predicate rule record and recordkeeping requirements*," but that "*fewer records will be considered subject to part 11;"* and further noted that Part 11 would be *"interpreted narrowly."*

The following controls were highlighted as critical:

- Limiting system access to authorized individuals.
- Use of operational system checks.
- Use of authority checks.
- Use of device checks.
- Determination that persons who develop, maintain, or use electronic systems have the education, training, and experience to perform their assigned tasks.
- Establishment of and adherence to written policies that hold individuals accountable for actions initiated under their electronic signatures.
- Appropriate controls over systems documentation.
- Controls for open systems corresponding to controls for closed systems bulleted above.
- Requirements related to electronic signatures.
- Indication of who (Veeva or Customer) must act, and the mechanism of action (behavior, procedural, or an application design element) that must be in place in order to satisfy the regulation.

Description of Controls

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
Subpart B – Electronic Records					
§11.10 Controls for Closed Systems					
§11.10 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:					
§11.10(a)	Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.	Veeva has implemented a comprehensive Computer Systems Validation (CSV) program codified in policy and further detailed in procedure. CSV deliverables are reviewed and approved by the Veeva Quality Unit.	—	X	—
		Customers are responsible for demonstrating that the system has been configured to their business requirements and is fit for use. This demonstration may come in the form of a PQ or UAT and must be performed under the customer's QMS.	—	—	X
§11.10(b)	The ability to generate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.	Veeva Vault provides system records in human readable form suitable for inspection, review, and copying by the agency. Configurable reports and exports permit review of records and associated metadata. In addition, an API is available for custom access to all stored records.	X	—	—
§11.10(c)	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	Veeva Vault's scalable architecture ensures all records (even archived records) are retained and can be retrieved from the production environment throughout the record retention period. No separate offsite or archive storage is required.	X	—	—
		Veeva hosts and operates its software on servers located in secure data centers. Customer data is protected through incremental and full backups and a routinely tested disaster recovery policy.	—	X	—
§11.10(d)	Limiting system access to authorized individuals.	Veeva Vault limits system access to authorized individuals through the use of user ID and password combinations. Role-based security configurations control all access to system functions.	X	—	—
		Veeva has implemented policies and procedures to control its employees'	—	X	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
		access to company business systems and customer applications.			
		Customers may configure Veeva Vault to conform to their security policies and define roles and privileges to align with their business requirements. Customer administrators are responsible for managing accounts and ensuring compliance with this section of the regulation.	—	—	X
§11.10(e)	Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.	Veeva Vault has a secure, system-generated audit trail that captures user entries and actions associated with the creation, modification, and deletion of system records. The audit trail information is available to system administrators for review, download, and archival outside of Veeva Vault.	X	—	—
§11.10(f)	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	All documents within Vault are governed by a lifecycle containing a sequence of states that control security, available actions, and other behavior. Veeva Vaults document lifecycles and workflows are designed to control the sequencing of events. Veeva Vault ensures that “required” data is completed prior to allowing the user to proceed with the next process step.	X	—	—
§11.10(g)	Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.	Veeva Vault has controls to ensure that only authorized individuals can use the system.	X	—	—
		Veeva has implemented policies and procedures for account management. All critical business systems leverage user accounts to limit access to authorized users.	—	X	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure that Veeva Vault user roles and profiles are configured to conform to their company’s security requirements.	—	—	X
§11.10(h)	Use of device (e.g. terminal) checks to	As a cloud-based solution, Veeva Vault may be accessed from multiple	X	—	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
	determine, as appropriate, the validity of the source of data input or operational instruction.	device platforms (PCs, mobile devices, and tablets). The validity of the source of data input or operational instructions is controlled through the authentication process and is systematically assured throughout the user session.			
§11.10(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.	Veeva has implemented policies, procedures, and training processes to ensure the qualification of staff who develop and maintain Electronic Records and Electronic Signatures (ERES) systems. Training records are maintained and demonstrate the qualification of individuals in relation to their assigned tasks.	—	X	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X
§11.10(j)	The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.	Veeva's written policies explicitly state that all individuals are personally accountable for actions initiated under their electronic signature. Falsification of signatures or records is grounds for termination of employment. All Veeva employees fulfill 'Read & Understood' training on this policy.	—	X	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X
§11.10(k)	Use of appropriate controls over systems documentation including: (1) adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance;	Customers can access system documentation (user and administrator help, release notes) from a secure website within Veeva Vault.	X	—	—
		Veeva has implemented policies and procedures on the control and distribution of system documentation.	—	X	—
	(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation	Veeva Vault user documentation is kept current and maintained cumulatively.	X	—	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
§11.30 Controls for Open Systems					
§11.30	Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 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.	Veeva Vault uses encryption to secure all data transfers and digital certificates to ensure authenticity.	X	—	—
§11.50 Signature Manifestations					
§11.50(a)	Signed electronic records shall contain information associated with the signing that clearly indicates all 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	Signature manifestation within Veeva Vault includes (a) the printed name of the signer; (b) the date and time when the signature was executed; and (c) the meaning of the signature. The system enforces the consistent application of these components.	X	—	—
§11.50(b)	The items 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).	The signature manifestation associated with signed records in Veeva Vault is subject to the same controls as the individual record to which it is attached. When selected, the electronic signature is manifested within all human readable forms of the record (display and printout).	X	—	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
§11.70 Signature/record linkage					
§11.70	Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.	Vault prevents all system users, including administrators, from excising, copying, or otherwise transferring electronic signatures through ordinary means.	X	—	—
Subpart C – Electronic Signatures					
§11.100 General Requirements					
§11.100(a)	Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.	Veeva Vault ensures unique user accounts by systematically prohibiting new accounts with an existing user name.	X	—	—
		Veeva has implemented policies and procedures on how the uniqueness of user accounts is prescribed and managed.	—	X	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X
§11.100(b)	Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.	Verification of identity is an integral part of the Veeva HR onboarding process.	—	X	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
§11.100(c)	Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.	Veeva Systems has notified the FDA, pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, that all electronic signatures executed by its employees, agents, or representatives, located anywhere in the world, are the legally binding equivalent of traditional handwritten signatures.	—	X	—
		Customers must notify the FDA of their own intent to use electronic signatures in order to comply with this section of the regulation.	—	—	X
§11.200 Electronic Signature Components and Controls					
§11.200 Electronic signatures that are not based upon biometrics shall:					
§11.200(a)	(1) Employ at least two distinct identification components such as an identification code and password.	Electronic signatures applied within Veeva Vault require a user ID and password.	—	X	—
	(1i) 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.	All signings within Veeva Vault require a user ID and password. Veeva Vault does not provide single component signing.	X	—	—
	(1ii) 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	We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
		Veeva has implemented policies and procedures to enhance user awareness regarding the appropriate use of their electronic system accounts.	—	X	—
	(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.	Passwords are encrypted in Veeva Vault to ensure that no one, including system administrators and database administrators, can view them. New users and users requesting a password reset receive a system-assigned temporary password that must be changed on the next login.	X	—	—
§11.200(b)	Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.	Veeva products do not currently employ biometric authentication for electronic signatures.	—	—	—
§11.300 Controls for identification codes/passwords.					
§11.300 Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:					
§11.300(a)	Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.	Veeva Vault ensures that user IDs cannot be duplicated or reused.	X	—	—
§11.300(b)	Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).	Veeva Vault allows customers to set the password aging controls in accordance with their security policies.	X	—	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X
§11.300(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	Veeva products do not currently employ any devices to assist with authentication.	—	—	—

21CFR11 Section	Part 11 Requirements	Veeva IT Controls & Processes	Applicability		
			Product	Process	Customer
	code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.				
§11.300(d)	Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and 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.	Veeva Vault has been developed to prevent and detect unauthorized access, and assist customer system administrators in reporting on unauthorized attempts. An audit log of all user login attempts is maintained.	X	—	—
		We advise customers to review their policies and procedures and modify them accordingly to ensure full compliance with this section of the regulation.	—	—	X
§11.300(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.	Veeva products do not currently employ any devices to assist with authentication.	—	—	—

Terms and Definitions

Term	Definition
API	Application Programming Interface
CFR	Code of Federal Regulations (US)
Cloud	Remote computing via the Internet with little local resource use
CSV	Computerized System Validation
ERES	Electronic Records and Electronic Signatures
GCP	Good Clinical Practice
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
QMS	Quality Management System
HR	Human Resources
PQ	Performance Qualification
UAT	User Acceptance Testing
Vault	Veeva's Regulated Content Management System

References

FDA 21CFR 11 Electronic Record; Electronic Signature - Final Rule (20Mar1997)

FDA Guidance for Industry Part 11, Electronic Records; Electronic Signatures - Scope and Application (Aug. 2003)