**QUALITY EXHIBIT**

Between

|  |
| --- |
| ***<Customer Legal Entity as MSA>*** |

and

|  |
| --- |
| Veeva Systems, Inc. |
|  |
|  |

***<Note: This is a template (***[***QV-01663***](https://veeva-qms.veevavault.com/ui/#doc_info/1763)***). Please contact Veeva Quality Operations to make sure the latest template is used prior to engaging with customer. All blue (variable) text is to be replaced with specifics/details prior to final review and approval, and all template notes deleted.>***

Table of Contents

[1 Introduction 3](#_Toc141707111)

[1.1 Customer Focus and Quality Advocacy 3](#_Toc141707112)

[1.2 Support for Regulated Use of Veeva Software Solutions 3](#_Toc141707113)

[2 Scope of the Quality Agreement 4](#_Toc141707114)

[3 SaaS Shared Responsibility 4](#_Toc141707115)

[4 Definitions 4](#_Toc141707116)

[5 Requirements 5](#_Toc141707117)

[5.1 Quality Management System 5](#_Toc141707118)

[5.2 Personnel and Training 5](#_Toc141707119)

[5.3 Sub-contractors / Supplier / Vendors 6](#_Toc141707120)

[5.4 Incident Management - Complaints, Deviations, CAPA 6](#_Toc141707121)

[5.5 Change Management 7](#_Toc141707122)

[5.6 Operational Controls 8](#_Toc141707123)

[5.7 Document Control and Record Retention 9](#_Toc141707124)

[5.8 Validation and Periodic Review 10](#_Toc141707125)

[5.9 Right to Audit and Inspections 12](#_Toc141707126)

[6 Approvals 13](#_Toc141707127)

[Appendix A. Contact Information 14](#_Toc141707128)

[Appendix B. Product Scope 15](#_Toc141707129)

[Appendix C. Definitions and Acronyms 16](#_Toc141707130)

***<Note: Refresh TOC prior to final review and approval>***

# Introduction

This Quality Agreement (QAG) outlines the responsibilities of Veeva Systems Inc. (herein Veeva) and <Customer legal entity> (herein <Customer>) with respect to the quality of <Customer>’s use of the in-scope (see Section 2) Veeva Software Solutions and the interface between the companies. The terms of this QAG are intended to be supplemental, and not conflict with, the terms of the Master Subscription Agreement (MSA) between the parties and dated <TBD>. Upon execution, this QAG is incorporated into and forms part of the MSA as an Exhibit. To the extent that any provision of this QAG conflicts with the provisions of the MSA, (i) the terms of this QAG shall prevail with respect to all matters pertaining to, or governed by, the Quality Regulations; and (ii) in all other respects, the terms of the MSA shall prevail.

<**Note:** As this QAG is an “exhibit” to the MSA, the sections below avoid either duplication or contradictions with the MSA commitments, especially the Technical Addendum SLAs. Before introducing new requirements or expectations in this document, ensure these are not already addressed in the signed MSA. Consult Veeva Knowledge Article [28935](https://veeva-qms.veevavault.com/ui/#doc_info/41169) – *Quality Agreements for Multitenant SaaS Software Deployments* for additional limitations.>

## Customer Focus and Quality Advocacy

Veeva’s driving principle is to help produce results that achieve customer success in the Life Sciences domain, including pharmaceutical, biotechnology, medical device, and veterinary medicine. Veeva has established an independent Quality Assurance Unit (QAU) that monitors and tracks issues within the Veeva Quality Management System (QMS), including those that directly affect product, or potentially affect <Customer>’s use of Veeva Software Solutions. The QAU (owner of this document) seeks to maximize the ability of the business in order to satisfy the customer and does so by reviewing the processes, work products, and <Customer>’s feedback to assure that critical issues potentially affecting Veeva Software Solutions are addressed in a timely manner.

## Support for Regulated Use of Veeva Software Solutions

For regulated customers of Veeva Software Solutions, the FDA regulations such as 21 CFR 211 Current Good Manufacturing Practice (cGMP) for Finished Pharmaceuticals and/or FDA Quality System Regulations (QSR) 21 CFR 820 have applicable sections that are relevant to processes where Computerized Information Systems are utilized. In addition, the applicability of international standards may include the ICH Q9 (specifying management of risk), ICH Q10 (specifying the quality system), or ICH E6 (specifying clinical conduct). With respect to the application of Electronic Signatures to Electronic Records, 21 CFR Part 11 is applied in the US. In European markets, EudraLex Volume 4 Annex 11 requirements are relevant.

Veeva has adopted GxP-compliant practices while validating functions that have GxP applicability in one or more of the international markets. For some applications, not all system functionality will have GxP applicability as deployed at a customer site. Areas of GxP applicability are identified by Veeva for typical application intended use. However, each customer must define the areas of GxP applicability and configure the product to comply with their intended use, including any business processes that the customer requires the system to meet. As the regulated user, the customer is responsible for the configuration and system operation, including user provisioning. As the Data Controller, the customer is responsible for the integrity of the resident data. The parties' responsibilities for ensuring compliance of Veeva Software Solutions under the MSA is outlined below.

# Scope of the Quality Agreement

The scope of this QAG covers the quality aspects for <Customer>’s use of Veeva Software Solutions (listed in Appendix B) and describes the responsibilities and the channels of communication between the involved parties. The specific sections below are for clarification of certain domains of the Quality Regulations and as such are not meant to exclude or replace cGxP or other regulatory requirements.

This QAG defines the roles and responsibilities for each Party relating to the internal controls and auditing of Veeva’s provisioning of Veeva Software Solutions as implemented by <Customer> for supporting <Customer>’s GxP processes and to the extent such activities are regulated by 2001/83/EC Annex 11 (as amended), 21 CFR Part 11, as amended, and laws applicable to a company engaged in supporting <Customer>’s use of Veeva Software Solutions under the Master Subscription Agreement (MSA).

Exclusion: This QAG does not cover professional and/or managed services defined under separate SOW, where customer is responsible, as the regulated user, to perform quality oversight over the stated activities and deliverables: E.g., Customer specific project implementations and configurations, integrations with customer legacy systems, migration of customer data, and/or custom solutions.

<Note: This QAG is designed around Veeva Vault Products (e.g., eTMF, QualityDocs, RIM, CDMS, Safety). The controls described below apply to the Vault Product Suite. Please Consult with Veeva Quality if introducing non-Vault products in scope (e.g., CRM, Network) as the below controls do not universally apply to all Veeva Software Solutions. >

# SaaS Shared Responsibility

The Software as a Service (SaaS) multitenant deployment model imposes a shared responsibility between Veeva’s Quality Assurance Unit (QAU) and the customer’s QMS and quality function. Since Veeva Software Solutions are highly configurable (GAMP Category 4) and are not (with few exceptions) delivered Out-Of-The-Box (OOTB), it is the responsibility of the regulated user to ensure that the implementation is “fit for use” (aka intended use) within their regulated context (i.e., GxP). The comprehensive demonstration that a supplier and a software solution is “fit for use” is a layered process with shared responsibilities. In this SaaS engagement, Veeva is a “data processor” and <Customer> is the “data controller.” Although <Customer> bears the ultimate responsibility for the suitability of the system for its intended use, some activities are sub-contracted to Veeva as outlined in Section 5 below.

<Note: Consult the Knowledge Article [31685](https://veeva-qms.veevavault.com/ui/#doc_info/45547) – *Shared Responsibility of the Multitenant SaaS Model* for additional insight.>

# Definitions

For a list a terminology and acronyms referenced herein consult Appendix C.

# Requirements

## Quality Management System

The International Standards Organization (ISO) defines a Quality Management System (QMS) as a management system designed to direct and control an organization with regard to quality. Veeva’s QMS shall be focused on the software design, development, testing, deployment, maintenance, and product support service delivery for <Customer>’s use of Veeva Software Solutions, including document management, human resource management, audit/inspection management, and related quality management, such as incident and change management, and CAPA. Veeva’s processes shall be documented and available for <Customer> to review during audits (see Section 5.9 below). QMS requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish and maintain a Quality framework aligned against a recognized standard (e.g., ISO 9001) to ensure an independent Quality Unit (QAU) that is appropriately qualified to oversee, maintain and support the Veeva QMS. | X |  |
| 1. Establish a QMS by developing and maintaining approved Quality System documents such as policies, standard operating procedures, and/or work instructions.   The Quality System will include, but not be limited to, change and configuration management, supplier management, incident management, document management, self-inspection, and training of personnel (see sections 5.2 - 5.8 below). | X |  |
| 1. Perform periodic self-inspections of internal process domains that define and delimit the Veeva QMS. Audit findings and corrective actions are documented and brought to the attention of management for timely and effective resolution (see sections 5.4 & 5.9 below). | X |  |
| 1. Implement Key Performance Indicators (KPIs) or metrics to assess the effectiveness of controls related to QMS activities or processes within the Veeva QMS. Communicate these performance metrics to executive management through periodic quality reviews. | X |  |

## Personnel and Training

Veeva shall ascertain that its personnel are competent and have appropriate role descriptions, professional qualifications, training, and experience to support <Customer>’s use of Veeva Software Solutions. Additionally, during an audit and upon <Customer>’s written request, Veeva shall make available documentation to demonstrate that said qualifications are current and in order. Resource management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Ensure sufficient qualified resources are available for the performance of scoped solution. | X | X |
| 1. Establish and maintain a documented process (in any combination of electronic or written format) for the management of training for personnel that may impact the quality characteristics of the scoped solution. | X |  |
| 1. The training records will be maintained and include documented job descriptions with defined roles and responsibilities, training curriculum, collected evidence of completion/certification, and monitoring of training effectiveness for personnel engaged in the scoped solution. | X |  |
| 1. Ensure that the use of contracted staff performing an activity within the framework of the QMS is supported by documented verification that they have the sufficient education, training, experience, or any combination thereof, to perform the activities for which they are contracted. See 5.3 below. | X |  |

## Sub-contractors / Supplier / Vendors

If Veeva employs a third party to perform activities within the framework of Veeva’s QMS, Veeva shall assure that the third party has been fully qualified via the Veeva’s third party qualification process. A quality or service agreement shall exist between Veeva and any third-party contractor performing any QMS related activity. Veeva provides a list of subprocessors and notifications of any subprocessor updates on trust.veeva.com. Supplier management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a documented process to select, qualify, and audit critical suppliers. Establish and maintain a list of approved suppliers and vendors, subcontracted that perform an activity within the framework of Veeva’s QMS. | X |  |
| 1. Veeva reserves the right to select and subcontract services to meet its obligations outlined in the MSA and commits that any such change will not adversely impact the level quality and performance established in the MSA or in this QAG. | X |  |
| 1. Customer may, upon request, review a list of such parties during an audit pursuant to the Right to Audit section 5.9 of this QAG. Customer agrees to treat such information as Confidential and not to contact any such parties in connection with this QAG without Veeva’s prior consent. |  | X |

## Incident Management - Complaints, Deviations, CAPA

Veeva maintains a Trust Site accessed at [trust.veeva.com](http://trust.veeva.com/) which offers the most up to date information on Veeva Systems' service status and includes a link for customers to subscribe to an RSS feed specific to their production system(s). For Veeva Vault Safety, Vault CDMS, and Vault CP applications, customers who subscribe to Vault notifications will receive email update notifications. Veeva shall investigate and document within its QMS incidents impacting the Veeva Software Solutions. SLAs for response times are defined in the MSA. For critical incidents (which shall include any incident that has an adverse impact, or may potentially adversely impact, on the <Customer>’s GxP use of Veeva Software Solutions), Veeva will notify <Customer> promptly. Incident and problem management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a documented process to record, review, triage, analyze and resolve customer complaints associated with the design, testing, deployment, and/or maintenance of the scoped solution. | X |  |
| 1. Establish a documented process for notifying the impacted parties of a significant event, incident, deviation and/or deficiency impacting the integrity, confidentiality, privacy, or security of the scoped solution without undue delay and within 3 business days. | X |  |
| 1. For incidents that impact the integrity, confidentiality, privacy, security of resident data, or represent a deviation/deficiency from Regulatory Authority requirements (e.g. a serious compliance breach), a formal investigation (Incident Report) will document the root cause and define appropriate corrective/preventative actions. Final incident report will be issued within a maximum of sixty (60) days following detection of the incident. | X |  |
| 1. Review and assess the adequacy of the reported incident analysis, investigation, and proposed remediations with respect to the intended use of the system and its resident data. |  | X |

Corrective and Preventative Actions (CAPA) are defined to address process and product anomalies that are systemic in nature and thus warrant additional remediation attention. Not every deviation, deficiency, lapsus, bug, or gap warrant this level of analysis, however, where direct impact to the integrity, security, of confidentiality of system records is affected, a CAPA will be initiated. CAPA management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a documented process to record, triage, investigate, and perform a root cause analysis (RCA) of critical process and product deficiencies/deviations related to the scoped solution. | X |  |
| 1. Implement and monitor the effectiveness of any agreed upon corrective and preventive actions (CAPA) arising out of the completed investigation to prevent recurrence of similar issues in the future. | X |  |
| 1. Review and evaluate the effectiveness of proposed remediations on process control capabilities. Trend process and product deviations for each function of the QMS. | X |  |

## Change Management

Changes to Veeva Software Solutions come in a variety of forms, from General Releases of new features and applications (enhancements), changes on platform architecture and infrastructure, patches and fixes (corrective), as well as changes to operating environments. Change management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a documented process to scope, assess, test, and deploy changes to the scoped solution in a controlled, quality assured manner. | X |  |
| 1. Changes made to the scoped solution, whether corrective or perfective, will be communicated to the customer prior to implementation as outlined in the MSA, except for emergency changes required to restore service or address a critical security vulnerability. Such emergency changes affecting the scoped solution may be made by Veeva without prior notification following Veeva change management procedures.   Note: Customers will however be notified of any such emergency change post-implementation. | X |  |
| 1. Changes made to Customer-specific configurations or Customer-specific documentation relating to use or implementation of the scoped solution, will be processed by Customer per their internal procedures. | <X[[1]](#footnote-1)> | X |
| 1. Change records associated with the scoped solution can be reviewed under the auspices of an audit as defined below (Section 5.9). |  | X |
| 1. Veeva shall notify Customer no less than six (6) months prior to implementing any change of Infrastructure as a Service provider or geographical storage location of hosted data for scoped services. | X |  |

## Operational Controls

Operational controls include those necessary for the continued secure operation of the production environment, including physical and logical security, BCP/DR, ongoing maintenance, and monitoring, as well as data backup and recovery. Operational controls requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish and maintain an ISMS framework aligned to industry recognized standard (e.g., ISO 27001, Trust Services Principles) to ensure the security and confidentiality of environment and data. | X |  |
| 1. Ensure appropriate controls over the management of access to the physical areas (e.g., sites, buildings, rooms, and offices) where customer information is maintained, processed, and/or stored. | X |  |
| 1. Establish and maintain a Third-Party attestation/certification of controls to verify the security, confidentiality, and availability of the scoped solution (e.g., SOC2, ISO 27001). | X |  |
| 1. Establish and maintain written procedures describing user account authentication and authorization services including periodic security reviews to ensure access is properly authorized and that timely deactivation of user accounts occurs. | X | X |
| 1. Implement and manage a qualified infrastructure, to include but not limited to, environmental monitoring, patching, firewalls, security monitoring, antivirus/malware protection, intrusion detection, vulnerability scans, and penetration testing. | X |  |
| 1. Implement a backup and restore process for production environments. Establish a documented process for the periodic testing of backups to verify that backup data is complete and accurate. | X | <X[[2]](#footnote-2)> |
| 1. Develop a Disaster Recovery Plan (DRP) which describes how the computing environment will be recovered in the event of a disaster. Establish a documented process for the periodic testing of DR to verify that the DR architecture operates as designed. Tests will be performed annually. | X |  |
| 1. Develop a Business Continuity Plan (BCP) which describes how the business processes associated with the scoped solution will continue to operate in the event of a disaster. Establish a documented process for the periodic evaluation of BCP to verify that the support processes operate as expected. | X | X |
| 1. Maintain operational records, including system logs, BCP/DR reports, availability and performance reports to demonstrate that the system and its environment are maintained in a state of control. | X |  |

## Document Control and Record Retention

Document control includes those process documents (e.g., policies, procedures, work instructions) that define the activities described herein, as well as the quality records generated as output from these process documents. Document control requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a process for reviewing, approving, and controlling distribution of SOPs and associated records. | X |  |
| 1. Define a record retention and archival process for “essential documents” required by regulation covering the scoped solution. All such documents, records, and reports will be maintained in such a manner that they are: (i) readily retrievable and (ii) stored in an environment suitable to prevent damage or loss. | X |  |
| 1. Ensure that all data (electronic or paper) relevant to GxP activities conducted pursuant to this QAG are original, accurate, legible, controlled, and safe from intentional or unintentional manipulation or loss throughout the retention period for such data. | X |  |
| 1. Establish “*the ability to generate accurate and complete copies of such records in both human readable and electronic form suitable for inspection, review, and copying by the Regulatory Authority agency*.” | X | X |
| 1. Maintain records covering the “*validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records*,” where “validation” used here and elsewhere in this Exhibit (including “validate” and “validated”) means validation as required and defined by applicable regulations. | X | X |

Veeva provides and maintains an electronic reading room (Compliance Docs) where customer-facing documentation is available for customer self-service. User accounts can be requested at [www.veeva.com/services/support-and-community/docs-access-request/](https://www.veeva.com/services/support-and-community/docs-access-request/) to access and review key documentation related to the scoped service such as Veeva’s validation packages for GxP impacting products (5.8), operational reports (5.6), and certifications (5.6), plus regulatory assessments and process overviews in support of desktop assessment/audit (5.9).

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Maintain the Compliance Docs repository to provide customers with the latest customer-facing documentation relevant to Veeva process controls. | X |  |
| 1. Provide copies of product validation protocols, reports, and supporting documentation used to support the validation activities of the scoped solution. See Section 5.8 below. | X |  |
| 1. Where local retention periods differ from Veeva corporate 7-year period for quality documents, export binders and documentation for local retention. |  | X |

## Validation and Periodic Review

The comprehensive and conclusive demonstration that a system / software solution is fit for use (i.e., validated) is a layered process with shared responsibilities, which includes 1) the IT controls established by our IaaS / Infrastructure hosting vendor (e.g., AWS) at the data center level, 2) IT and Security Controls implemented by Veeva during the provisioning of the environment, 3) the design controls implemented during the SDLC and validated under the Computer System Validation program, and 4) the configuration of the customer solution during project implementation. Due to the highly configurable nature of Veeva Software Solutions, Veeva provides baseline validation of its GxP relevant products for customers to configure and implement in accordance with their intended use and regulatory requirements. SaaS is a shared responsibility model with respect to system validation as outlined below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Product validation proceeds in accordance with Veeva policies, procedures, and work instructions. The validation of a Production Release is formally documented, QAU reviewed and approved. The validation deliverables follow industry standard documentation, including:  * Requirement / Specification Document(s) * Project Plan * Qualification Protocol * Executed Qualification scripts * Regulatory Impact Assessment * Traceability Matrices * Summary Report | X |  |
| 1. Perform qualification of configured items such as enabled features, study specific configurations, custom integrations, to demonstrate the system meets its regulated intended use. | <X[[3]](#footnote-3)> | X |

Periodic review of system performance and operation is required to ensure a validated system continues to operate in accordance with its defined process control parameter and quality attributes. Periodic review covers a range of domains from system validation, incidents and changes, procedural controls, as well as access controls. While periodic review is the responsibility of the regulated user, Veeva can provide documentation to facilitate the review requirements. Periodic review requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| 1. Establish a process to record, maintain and retrieve information and records in support of customer’s periodic review obligations, including, but not limited to, change records, incident records, monitoring records, validation deliverables, that are relevant to the scoped solution. | X |  |
| 1. Perform risk-based periodic system reviews of GxP relevant products to evaluate the cumulative impact of changes on Veeva’s validation package. | X |  |
| 1. Perform validation impact assessment of Production Releases to assess and document the impact of system changes on the validated state of the configured system. | <X3> | X |
| 1. Perform periodic assessments of the project/study validation deliverables to ensure that system changes have been implemented in a manner to maintain the solution in a state of control. | <X3> | X |
| 1. Perform periodic assessments of user access and other system generated audit logs. | <X[[4]](#footnote-4)> | X |

## Right to Audit and Inspections

Veeva has established an external independent audit program that provides customers with an option to purchase GxP audit reports of Veeva. (Details on how to purchase can be found in Compliance Docs or by contacting [audits@veeva.com](mailto:audits@veeva.com)).

In accordance with the MSA, the customer has a Right to Audit. For the avoidance of doubt, Sponsors of the Customer may participate in the Customer’s annual audit for their organization. Veeva operates a remote/virtual audit program where Customer audits are limited to one audit per year (postal audit, desktop audit, or remote audit) unless customer reasonably believes Veeva has materially failed to fulfill its obligations hereunder, and that such failure would be a violation of any Laws and provided Customer can provide Veeva reasonable evidence of the same. In which case Customer shall be entitled to conduct a for-cause audit of Veeva. To request an audit of Veeva contact [audits@veeva.com](mailto:audits@veeva.com) or your Veeva account partner. The audit and inspection management requirements and responsibilities are itemized below:

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| * 1. Maintain a customer-facing reading room with timebound access to Veeva process documents (e.g., SOPs, WIs) for remote desktop self-service audit. | X |  |
| * 1. Upon request and with appropriate notification (as defined in the MSA), permit an audit/inspection of the controls relevant to the scoped solution for the purpose of a verifying compliance with the operational terms of the MSA and this QAG. | X |  |
| * 1. Following an audit, a formal report shall be drafted identifying any significant non-compliance findings. |  | X |
| * 1. Within 30 days from the receipt of an audit report, a written response to all audit observations agreed upon between the Parties will be provided identifying the proposed corrective actions to observations which are to be implemented within agreed timeframes. | X | X |

As a SaaS vendor, Veeva understands that it may be called upon to support customers during a regulatory inspection (e.g., biennial GMP, BIMO sponsor audit, Pre-Approval Inspection). To notify Veeva of an upcoming regulatory inspection which may require Veeva support, please contact [audits@veeva.com](mailto:audits@veeva.com) with the name of the agency and in-scope Veeva products, in advance of the inspection. Your Veeva point of contact for questions that cannot be answered by the information available in the Compliance Docs reading room is Veeva’s *Audit Management* team at [audits@veeva.com](mailto:audits@veeva.com) who will help answer supplemental questions and/or provide requested documented evidence.

| **Responsibility/Requirement** | **Veeva** | **<Customer>** |
| --- | --- | --- |
| * 1. Customers should be conversant with the artifacts posted in the Compliance Docs reading room as well as those customer specific deliverables posted in the Project (or PMO) vault as if they had performed the activities themselves. |  | X |
| * 1. If customer is inspected by a Regulatory Authority having authority over the industry (e.g., FDA, MHRA, EMA) (“Regulatory Authority”), Veeva shall provide backroom (war room) support during an inspection as is reasonably necessary in the circumstances. Veeva shall supply records limited to those required to respond to the Regulatory Authority’s inquiries directly related to the scoped solution, provide remote support, and/or permit a reasonable level of access to the Regulatory Authority to the extent required by Law. | X |  |
| * 1. Veeva will permit regulatory inspections of their business, either as a direct inspection request or in support of a Customer inspection. Veeva will notify customer if an inspection is directly scoped to customers implementation and provide a copy of correspondence related to the customers implementation promptly. | X |  |
| * 1. If Veeva is inspected by a Regulatory Authority, Veeva will promptly notify Customer of any FDA Form 483’s, Warning Letters or the like from applicable Regulatory Authorities and subsequent response(s) directly relating to the customer’s implementation of the scope solution. | X |  |

# Approvals

Any change to this QAG must be agreed by the QAU of both <Customer> and Veeva. If either party intends to change any part of this QAG, the party requesting such change will promptly inform the other party allowing such period of time for both parties to discuss and agree on such matters to be changed. The updated QAG will be signed and returned to the other party, a signed copy being retained for reference.

In witness whereof, the parties hereto have caused this QAG to be executed by their duly authorized representatives as of the date last signed below (“Effective Date”).

|  |  |  |  |
| --- | --- | --- | --- |
| **<Customer>** | | **Veeva Systems Inc.** | |
| Title: |  | Title: |  |
| Name: |  | Name: |  |
| Signature: |  | Signature: |  |
| Date: |  | Date: |  |

1. Contact Information

The contact names and respective contact details for the Parties’ contact teams are initially as established below. Either Party may replace any member of its contact team, at any time, by written notice to the other.

**<Customer>**

|  |  |
| --- | --- |
| **Name / Title** | **E-mail Address** |
| <Customer Quality representative> |  |
|  |  |

**Veeva**

|  |  |
| --- | --- |
| **Name / Title** | **E-mail Address** |
| <Veeva Quality representative> |  |
|  |  |

1. Product Scope

The Table below identifies the products in scope of this QAG

|  |  |  |
| --- | --- | --- |
| **Products** | **In Scope** | |
| **Yes** | **No** |
| Vault Core - Software solutions developed on the Veeva Vault Platform including Clinical Suite (e.g., eTMF, CTMS), Commercial (e.g., PromoMats, MedComs), Quality (e.g., QDocs, QMS, Training), and Regulatory (e.g., RIM Submissions). These products are itemized in the *Veeva Vault System Overview* ([QV-01873](https://veeva-qms.veevavault.com/ui/#doc_info/2021)). | <X> | <X> |
| Vault CDMS - Software solutions developed on the Veeva Vault Platform supporting Clinical Data Management (e.g., EDC, Coder). These products are itemized in the *System Overview for Veeva Vault CDMS* ([QV-12726](https://veeva-qms.veevavault.com/ui/#doc_info/15055)). | <X> | <X> |
| Vault CDB (Workbench) – Clinical DataBase software solution integrated with Vault CDMS and third-party source data for clinical data analysis and cleansing. The CDB capabilities are itemized in the *System Overview for Veeva Vault CDMS* ([QV-12726](https://veeva-qms.veevavault.com/ui/#doc_info/15055)). | <X> | <X> |
| Vault Safety - Software solutions developed on the Veeva Vault Platform supporting Safety Data Management (e.g., Case Management, Coder, Submissions). These products are itemized in the *System Overview - Vault Safety* ([QV-16049](https://veeva-qms.veevavault.com/ui/#doc_info/20463)). | <X> | <X> |
| Vault CP – Software solutions developed on the Veeva Vault Platform supporting the Consumer Products industry sector. Vault CP products are itemized in the *System Overview for Veeva CP&C* ([QV-15931)](https://veeva-qms.veevavault.com/ui/#doc_info/20153). | <X> | <X> |
| Digital Trials Platform - Software solutions developed to support Clinical Conduct and Operations (e.g., eConsent, ePRO, SiteVault). Digital Trials Platform products are itemized in the *System Overview for Digital Trials Platform* ([QV-21465](https://veeva-qms.veevavault.com/ui/#doc_info/29195)). | <X> | <X> |
| RTSM - Software solutions developed to support clinical study Randomization and Trial Supply Management operations. Software capabilities are defined in the *System Overview for Veeva RTSM* ([QV-34384](https://veeva-qms.veevavault.com/ui/#doc_info/49876)). | <X> | <X> |
| Multichannel CRM - Software solutions developed on the SalesForce.com platform supporting Customer Relationship Management for the Lifesciences. CRM suite of products are itemized in the *CRM System Overview* ([QV-02714](https://veeva-qms.veevavault.com/ui/#doc_info/2945)). | <X> | <X> |
| Network MDM - Software solutions developed to manage Healthcare Professional (HCP) and Healthcare Organization (HCO) contact information in a single master data management system (MDMS). Network MDM is described in the *System Overview for Veeva Network* ([QV-03074](https://veeva-qms.veevavault.com/ui/#doc_info/3379)). | <X> | <X> |

1. Definitions and Acronyms

| **Term / Acronym** | **Definition** |
| --- | --- |
| Applicable Laws | All laws, ordinances, rules and regulations within the Territories applicable to the customer’s use of the scope solution and associated obligations, as the context requires, including, without limitation, (i) all applicable federal, state and local laws and regulations. (ii) The U.S. Federal Food, Drug and Cosmetic Act, and (iii) the "GxPs." Applicable Laws shall also include all laws, ordinances, rules and regulations applicable in Territories added to this Quality Exhibit after the Effective Date of this Quality Exhibit; solely to the extent Customer or its designee has provided written copies of such laws to Veeva. Copies of all laws shall be in the English language. |
| BCP | Business Continuity Plan |
| Data Controller | Responsible for managing the data/records within Veeva Software Solutions by creating, editing, deleting, reviewing and approving resident data/records to ensure their accuracy and completeness (i.e., integrity). |
| Data Processor | Responsible for managing the system and environment that processes data/records associated with Veeva Software Solutions by designing, testing, monitoring, and maintaining the data/record system/environment to ensure confidentiality, security, and availability (i.e., integrity). |
| Facilities | Veeva facilities located at: 4280 Hacienda Drive Pleasanton, CA 94588 |
| Essential documents | Essential documents are those records predicated by regulation and required in support of a health authority inspection, and/or for a marketing authorization (e.g., ICH E6 Section 8, FDA Part 11 Section 11.1 Scope) |
| EMA | The European Medicines Agency is a decentralized agency of the European Union responsible for the scientific evaluation of medicines developed by pharmaceutical companies for use in the European Union. |
| ERES | Electronic Records Electronic Signature regulations define controls over electronic data used to satisfy predicate rule requirements (GxPs). These ERES requirements are codified in FDA 21CFR 11 regulation and in EU Eudralex Volume 4, Annex 11. |
| FDA | United States Food and Drug Administration, and any successor entity thereto |
| GxPs | Current Good [x = Manufacturing, Clinical, Pharmacovigilance, Laboratory, Distribution, etc.] Practices for Pharmaceuticals, Devices or Biologics promulgated by the FDA, international regulatory agencies and notified bodies, as amended from time to time. |
| IaaS | Infrastructure as a Service |
| Incident | Any event which is not part of the standard operation of a service and which causes, or may cause, an interruption to or a reduction in, the quality of that service. |
| Investigations | A detailed and thorough review of any atypical operation deviating from the qualified/validated configuration specifications (or any other matter that has potential impact to the electronically stored customer data contained in Customer Instance(s) of the scoped solution that is documented in a written report and approved by Veeva Quality Assurance. |
| ISMS | Information Security Management System, policies and procedures which manage an organization’s sensitive data in order to minimize risk. ISO27001 |
| MHRA | The Medicines and Healthcare products Regulatory Agency is an executive agency of the Department of Health in the United Kingdom, which is responsible for ensuring that medicines and medical devices work and are acceptably safe. |
| PMDA | Pharmaceuticals and Medical Device Agency, Japan oversees the public health and safety of pharmaceutical and medical devices in Japan. |
| Promptly | Typically, no more than three (3) business days. This period may be exceeded due to events or circumstances beyond the reasonable control of the responsible party. |
| QAG | Quality Agreement or Quality Exhibit to MSA |
| Quality Regulations | Regulations that specify the quality controls, parameters, procedures and/or attributes of a process or product (e.g., 21CFR820). |
| QMS | Quality Management System - A set of policies, processes and procedures required for planning and execution (production/development/service) in the core business area of an organization. The QMS enables the organization to identify, measure, control and improve the various core business processes that ultimately lead to improved business performance. (ISO 9000) |
| Record | Any document/data/metadata that is established and maintained to provide evidence of conformity to the requirements and of the effective operation of the Quality Management System. |
| Regulatory Authority | FDA and any other Regulatory Agency (e.g., EMA, PMDA, MHRA) within a Territory involved in regulating any aspect of the development and implementation of the scoped solution. |
| Scoped Solution | Veeva provides software solutions in a multitenant, SaaS, cloud-based engagement. The scoped solution defined herein is listed in Appendix B above. |
| SaaS | Software as a Service |
| SDLC | Software Development Lifecycle - A defined framework for computer system implementation and management that entails defining and performing activities in a systematic way from conception, understanding requirements through development, release, and operational use, to system retirement. |
| Serious Compliance Breach | As relates to clinical trials: Any deviation of the approved protocol version or the clinical trial regulation that is likely to affect the safety, rights of trial participants and/or data reliability and robustness to a significant degree in a clinical trial. |
| Software | Programs, procedures, code, algorithms, rules, and any associated documentation pertaining to the operation of a computerized system. |
| SOP | Standard Operating Procedures” (SOP) shall mean the standard operating procedures in effect at Veeva which have been approved by Veeva Quality Assurance department and which are applicable to the scoped solution. |
| SOW | Statement of Work – defines the activities and deliverables to be implemented for the scoped solution. NB. May also contain a formal Transfer of Obligation if required by GCPs. |
| Specifications | Quality standards, configuration, testing procedures that define, delimit, and contribute to the quality characteristics of the scoped solution as set forth in writing and referenced and/ or contained in the MSA and/or SOW. |
| Territories | United States of America, the Member States of the European Union, and any other country which the parties mutually agree in writing to add to this Quality Exhibit (QAG). |
| Validation | The process that establishes documented evidence that a computer system is developed according to quality software development principles, that it provides functional capability required by its users and that it will continue to do so over time. |

1. <Applies to RTSM and DTP products only. Remove if not in scope> [↑](#footnote-ref-1)
2. <Applies to CRM products only. Remove if CRM not in scope> [↑](#footnote-ref-2)
3. <Applies to RTSM and DTP products only. Remove if not in scope> [↑](#footnote-ref-3)
4. <Applies to RTSM when explicitly codified in a Transfer of Obligation. Remove if not in scope> [↑](#footnote-ref-4)