# Security Addendum

This Security Addendum ("**Addendum**") is incorporated into the Master Agreement between Customer and Veeva ("**Agreement**"). In the event of any conflict between the terms of this Security Addendum and the Agreement, the terms of this Security Addendum will control solely with respect to the terms set forth herein. Any capitalized terms used herein, but not defined, have the meaning set forth in the Agreement.

## 1 Technical and Organizational Measures

Veeva implements the technical and organizational security measures specified herein. Veeva regularly reviews and modifies its security measures to reflect changing technology, laws and regulations, risk, industry and security practices and other business needs. Veeva may make changes to its security measures, so long as the changes do not materially decrease the standard of security.

## 2 Security Standards

**Policy and Standards.** Veeva applies information security policies across the enterprise to protect Customer Data, Veeva systems, information assets and infrastructure. Veeva maintains a security program that is appropriate for the Software, systems, data, and physical locations being protected. Veeva maintains third party certifications on certain Veeva Software as applicable and as reflected in Veeva's audit summaries, certification reports, and in the Veeva compliance documents repository which is made available to Customer. Veeva's security organization and management align with the following standards as applicable or as described:

2.1(a) ISO 9001:2015 – Quality Management Systems

2.1(b) ISO/IEC 27001:2022 – Information Security Management

2.1(c) SOC2 Type II – System and Organization Controls

2.1(d) SEI Capability Maturity Model Integration (v1.3)

2.1(e) IT Infrastructure Library ITIL version 3

2.1(f) ICH Q9 – Quality Risk Management.

Further information regarding third-party audits and certifications Veeva obtains in relation to its security measures may be found at veeva.com/trust/. Audit and certification reports may be viewed in Veeva's compliance documents repository that Customer may request access to at Veeva Document Repository Request.

**Security and Architecture.** Veeva applies a security architecture across its information resources. The architecture comprises a defined set of security mechanisms and supporting standards. Veeva's architecture supports information resources requiring different levels of protection; enables the secure flow of information within and between technical environments; provides authorized users with an efficient means of gaining access to information resources in different technical environments; enables access privileges for individual users to be revoked efficiently when users leave or change jobs. Veeva maintains an accurate and complete inventory of its critical information assets and the applications used to process them.

## 3 Personnel Security

**Veeva Personnel**. Veeva employs appropriate measures to supervise information processing by Veeva personnel. Where legally permissible Veeva screens applicants for security sensitive positions to the extent allowed under the law. Veeva logs and monitors activity by Veeva personnel engaged in the handling and processing of information assets. Veeva has an internal team dedicated to security and has appointed an Information Security Officer. Customer may contact Veeva security at security@veeva.com.

**Endpoint Security.** Veeva uses established processes and controls designed to protect software installed on Veeva-issued laptops, desktops, or other devices that process Customer Data ("Endpoints") from malware and malicious activity. Veeva applies available security patches to address vulnerabilities in software installed on any Endpoint. Veeva laptops are provisioned and built by authorized personnel from a known baseline (gold image) and include standardized software including disk encryption and security tools designed to prevent and detect malicious activity.

## 4 Physical and Environmental Security

**Veeva-controlled Equipment and Facilities.** Veeva maintains processes designed to protect Veeva-controlled equipment and facilities against loss or damage. Measures include limiting access to physical structures to authorized personnel only. Veeva conducts due diligence on cloud providers that it leverages in providing in-scope Software and Services to verify that providers maintain industry standard safeguards.

**Specialized Equipment used in the Production Environment.** Veeva uses specialized equipment in its production environment to protect from a wide variety of known hazards.

**Third-party controlled Equipment and Facilities.** Veeva requires subcontractors used in our operations or that help Veeva provide our services to Customer to enter into appropriate contracts based on the type of services they provide, the type of information they have access to, and their risk profile. Veeva ensures contractual controls are in place that require subcontractors that house or process Customer Data to employ measures to protect against loss of or damage to the equipment and facilities used to host Customer Data. Veeva conducts risk assessments to determine the competency and appropriateness of each subcontractor's self-maintained security program. Subcontractors must maintain adequate security programs for the services and products they provide

## 5 Malicious Activity

Veeva deploys up to date software and procedures for the purpose of detecting and preventing the proliferation of viruses and other forms of malicious code. Veeva uses network and host-based intrusion detection services to protect critical systems, especially internet connected systems. Veeva utilizes a qualified, independent third party or in-house team of experts to perform technical penetration testing on Veeva information systems that are accessible from the internet regularly (at least annually). Veeva deploys industry standard firewall technologies. Veeva separates informational resources used for production environments from system development and testing environments.

## 6 Access Control

**Access Control and Authentication.** Veeva assigns access to systems, applications, and associated information in accordance with Veeva's documented access policies, which are risk-based and incorporate the principles of least privileged access and are enforced by automated means. Veeva logs all system access (including access by system administrators, operators, development, or audit staff).

**Authorization Safeguards.** Veeva uses industry standard practices to verify and authenticate authorized users before access to systems and data is granted.

## 7 Incident Prevention and Management

**Information Security Awareness and Training.** Veeva provides all Veeva employees and contractors engaged in the handling of Customer Data and Veeva systems with information security awareness training annually. New employees receive information security training and certification.

**Vulnerability Assessment.** Veeva performs regular, automated vulnerability and configuration scanning across all IT environments and assets, where findings are risk-assessed, prioritized by severity, and remediated accordingly. Veeva also commissions annual security assessments from an independent third-party provider of national repute in the business of assessing web applications for security risks. Upon request, Veeva will provide a letter of attestation that the assessment was performed and include a summary of findings.

**Incident Response and Notification.** Veeva maintains Incident Response processes that include annual testing and approval of Veeva's Incident Response Processes. "Security Incident" means an occurrence that materially impacts the Customer and actually jeopardizes the confidentiality, integrity, or availability of Veeva's information systems or Customer Data, or that constitutes a violation of Veeva's security policies, procedures, or acceptable use policies. In the event of any Security Incident Veeva will notify the Customer of the Security Incident without undue delay and not to exceed seventy-two (72) hours after becoming aware of the Security Incident. Veeva's notification of a response to a Security Incident is not an acknowledgement by Veeva of any fault or liability with respect to the Security Incident.

## 8 Data Availability and Integrity

**Data Availability.** Veeva has procedures to maintain data integrity and availability. Standard Operating Procedures are in place to handle occurrences including but not limited to, Security Incidents, equipment and/or Software malfunctions, loss of power and/or communication services, overloads, user mistakes, and access violations.

**Data Integrity.** Veeva uses an industry standard encryption method to encrypt Customer Data while it is in transit across an untrusted network. Communication between user(s) and server(s) are protected by TLS encryption. Veeva uses firewalls and antivirus software designed to protect application servers. Veeva maintains an audit management program to (i) perform periodic self-assessments of its Software and (ii) monitor the performance of its subcontractors.

**Data Retention and Destruction.** In accordance with Veeva's data retention and data destruction policies and in accordance with Customer's Agreement, Veeva uses industry standard processes and technologies to permanently delete Customer Data when it is no longer reasonably needed or authorized.

**Business Continuity and Disaster Recovery.** Veeva maintains backup and recovery, disaster recovery and business continuity processes and procedures as detailed at veeva.com/trust/.

## 9 Software Development Lifecycle

Veeva has software development lifecycle processes and controls ("SDLC Process") governing the development of and changes to Veeva Software, including updates, upgrades, and patches. The SDLC Process includes industry standard secure software development practices and application security analysis and testing on Software, according to industry standard verification requirements (such as the OWASP Application Security Verification Standard (ASVS)).