WHITE PAPER

Veeva SiteVault

Technical and Operational Security

Copyright © Veeva Systems 2022

CONTENTS

Copyright © Veeva Systems 2022

1 Executive Summary

Data security is a critical consideration for any company evaluating cloud-based software providers. Veeva is fully committed to ensuring the confidentiality, integrity, and availability of customer data managed by its platform and applications. Our teams utilize established information security frameworks and always employ secure software development best practices.

All of Veeva's applications are compliant with the strictest security regulations, including U.S. FDA's Title 21 CFR Part 11 and European Commission's Annex 11. Having achieved ISO 27001 certification, Veeva integrates security into every phase of product development and daily operations. Compliance with the ISO 27001 framework and regulations on electronic data and systems has enabled Veeva to meet and often exceed rigorous vendor assessment requirements in hundreds of customer audits.

This paper describes the technology, practices, and controls that Veeva uses to keep your data secure in Veeva SiteVault.

2 Application Security

Application security ensures the protection of SiteVault customer data. The security policies and profiles defined within SiteVault are enforced through authentication, authorization, and audit safeguards.

SiteVault makes content easily accessible in the cloud while ensuring customer data is only accessed by those with valid credentials and proper access rights.

2.1 Access Control and Identity Management

2.1.1 User Authentication

In SiteVault, Veeva creates the customer's first Regulatory user. Additional user accounts are set up and maintained by the customer's Regulatory user(s). Each user added will have their own SiteVault user account. Once user accounts have been created, users must be authenticated before they can access any data.

2.1.2 Login Policies

SiteVault is configured with strong user password strength, including complexity, a default session duration, and password length requirements based on industry's best practices. All access attempts are logged.

In order to protect login credentials, user passwords are salted and then hashed using a multiple-iteration algorithm. This one-way hash function cannot be reverse engineered back to the original password. Even when two identical passwords from different users are stored in the protected authentication servers, the encrypted password strings are different.

2.1.3 Session Management

SiteVault issues a session-specific cookie that keeps users logged into their accounts for a limited duration as configured by the Veeva SiteVault administrator. This cookie uses a secure random number hash algorithm and expires after the duration set by the Veeva SiteVault administrator, requiring users to re-authenticate their session upon expiration. Before rendering a webpage that corresponds to an application request, Veeva confirms that the calculated user hash value in the session-specific cookie matches the user hash value that was set during the login phase. For Cross-Site Request Forgery (CSRF) protection, Veeva leverages CSRF tokens associated with the user's current session.

Copyright © Veeva Systems 2022

2.2 Audit Trails

SiteVault automatically logs all user activity against a record in audit logs. The audit logs provide visibility into user activity and are a key requirement for compliance with Electronic Records and Electronic Signature (ERES) regulations. SiteVault users can view audit log information such as date and time stamp, username, and the event or activity being processed for documents and objects. For example, if a field value is updated, the before and after values are visible in the audit log for the record.

2.3 User Authorization

Veeva SiteVault administrators configure user access and activities down to the “atomic” level within the application. They specify access ranging from user administration and application functionality down to individual documents and their associated fields. SiteVault application is pre-configured with three user types: Regulatory, Study team, and External. Every customer user in SiteVault must be assigned to one of the pre-configured user types.

2.3.1 External Access

Customer’s SiteVault regulatory users can easily add External users to provide seamless collaboration with sponsors, contract manufacturers, auditors, regulatory authorities and other partners. To view any customer data, an External user must also be assigned (by a customer’s Regulatory user) to one or more studies.

Copyright © Veeva Systems 2022

3 Data Security and Protection

SiteVault is designed as a multi-tenant cloud application - all customers use a shared pool of computing resources. All communication and data are also protected using industry standard encryptions.

3.1 Customer Data

There are five types of customer artifacts that are stored:

1. Metadata
2. Annotation data
3. Application configurations
4. Content files
5. Full-text search indexes

The first three are stored directly in the database. The content files and full-text search indexes are stored on a file server. Content files are encrypted, and file location pointers are calculated using a value stored in the database; therefore, individuals must have access to the database in order to locate a piece of content.

SiteVault prevents customers from accessing each other's data by leveraging "atomic" security as noted in section 2.3.

3.2 Data in Motion Encryption

All network communication to SiteVault, from the initial login prompt to document transfer and the viewing of reports, uses industry standard Transport Layer Security (TLS) encryption.

Veeva uses an industry leading, external certificate authority for its TLS digital certificates with 2048-bit asymmetric keys and SHA-256 signatures and enforces a minimum of 128-bit symmetric key encryption.

3.3 Data at Rest Encryption

Customer documents are stored in the SiteVault file system using AES 128-bit encryption. Documents are also stored in Amazon Web Services' (AWS) S3 buckets, where an additional AES-256 layer of encryption is applied.

3.4 Backup and Recovery

Veeva has implemented a backup and recovery strategy with a four-hour recovery point objective (RPO) and a 24-hour recovery time objective (RTO).

Customer data is protected to ensure high availability (HA). Data is replicated from the primary site to a disaster recovery (DR) region at regular intervals, by storing the documents in AWS S3 with cross-region replication. DR site data is backed up to AWS S3 nightly and stored for 2 years. Backups are verified using automated daily restore scripts, with fully rehearsed disaster recovery tests performed every month and restore tests at least twice per year.

3.5 Data Protection and Retention Policies

3.5.2 Employee handling of data

Veeva company policies and procedures explicitly prohibit any caching of customer data on company computers, with the exception of those employees who require access to customer data to perform activities in their job role (e.g., Professional Services implementation or Customer Support). Data destruction and revocation of system access are explicitly stated as responsibilities of those personnel working with customer data.

Copyright © Veeva Systems 2022

3.5.2 Administrator access to customer data

‘

Only Veeva administrators providing support or addressing technical issues, and handpicked members of the Veeva product development team have the ability to access select customer data. Access is only granted in accordance with the Veeva Terms of Service (ToS) and is limited by policy to allow the least access necessary to provide support or measure product performance, following the principle of least privilege.

Copyright © Veeva Systems 2022

4 Infrastructure Security

4.1 Physical Security

4.1.1 Data Center

Customer data is stored in industry-leading ISO 27001 certified data centers around the world that issue SOC2 Type II reports. All facilities feature 24-hour manned physical security, mantraps, biometric access control, and video surveillance. Veeva does not have direct access to servers, which are managed by the data center providers' or managed services' personnel. All data centers are audited annually by an independent third party.

Veeva data centers are designed to protect customer data from hardware and environmental risks. Infrastructure is maintained in a strictly controlled environment to ensure optimal performance and protection. This includes the ability to withstand regional natural disasters. To ensure uninterrupted data access, infrastructure components are powered by redundant electrical supplies (e.g. breakers), UPS modules, and generators. Veeva and the data center operations personnel are continually monitoring system and network performance to ensure maximum service availability.

4.1.2 Operational Access

Only data center personnel can physically access servers. Data center personnel therefore perform all hardware maintenance. All operational activities, including facility access and replacing hardware components or removable media, are monitored, tracked, and audited.

Within Veeva, only a small number of technical operations administrators can access production infrastructure and perform system maintenance tasks. Veeva continually monitors access logs to verify all administrator activities.

Operating system level security is provided using continuous monitoring tools, such as host based intrusion detection software, which instruments the kernel and monitors all network and process activity. This allows automated detection of unauthorized access attempts, including any suspected network connections, file access or suspicious processes that are launched.

4.1.3 Amazon Web Services (AWS) Security

Veeva has a shared responsibility with AWS based on the standard AWS Shared Responsibility model. Veeva is primarily responsible for network management, AWS Console access, and AWS resources, and are secured using a variety of tools, including cloud configuration monitoring software, that continuously monitors and remediates any issues that arise. This allows Veeva to monitor how networks are configured within AWS – to trigger immediate alerts in case of policy violations or suspicious network traffic, as well as track user behavior of AWS accounts and associated access keys. Finally, these automated tools also inspect how AWS resources, such as S3 for object storage, or EC2 for compute instances, are configured to ensure they follow best practices.

Access to Veeva's internal corporate network is controlled through user accounts, which require eight-character minimum length passwords with password complexity requirements, multifactor authentication for remote access, and auto-expiration. SiteVault is housed on a separate production network in AWS which has stricter controls, including continuous monitoring by the security team. Access to the production servers and operations network is controlled through VPN access to a hardened jump host with two-factor authentication.

4.1.4 Asset Management

Veeva maintains an inventory of its critical information assets in an Enterprise asset inventory system and has identified all applications that process sensitive data. Veeva also tracks IT assets assigned to employees and ensures retrieval as part of the employee exit process.

Copyright © Veeva Systems 2022

4.1.5 Malware Protection

All company laptops have malware protection that are managed and monitored by Veeva IT Operations. Users are trained on security best practices and malware prevention as part of their security awareness training.

4.1.6 Media Handling

Operating procedures are defined to protect documents and computer media containing customer data or any other type of sensitive information. Media is properly sanitized or securely disposed in compliance to NIST SP 800-88, Guidelines for Media Sanitization.

4.1.7 Mobile Device Security

Customer data is stored on laptops only for specific purposes such as implementation or troubleshooting, and all files are encrypted using AES 256-bit keys.

4.2 Network Security

4.2.1 Firewalls

External facing systems, including servers hosting customer data, are protected by firewalls. Changes to firewall rules are reviewed and approved, and the firewalls are monitored 24/7 by the data center provider's security operations center.

Production servers only have two services directly accessible to the Internet: secure web (ports 80/443) and a series of secure FTP ports (56000 range). Port 80 is only open on login/authentication servers which immediately redirect communications to a TLS encrypted session on port 443. Periodic penetration testing helps ensure there are no known vulnerabilities at the application layer of these two services.

Monitoring of network traffic is provided by a combination of AWS Shield, AWS GuardDuty, AWS VPC Flow logs and a cloud-native Security Information and Event Management (SIEM) solution.

4.2.2 Jump Hosts

Production servers are not directly accessible from external networks for maintenance and support activities. Technical Operations access is routed through hardened jump hosts that are secured behind a second set of redundant firewalls. Jump hosts have full console logging and file integrity monitoring.

4.2.3 Log Management

Security relevant logs such as application and operating system event logs from servers hosting customer data are centrally aggregated to secure S3 log buckets for long term storage, which are then fed to a cloud native SIEM solution for real-time monitoring and alerting. The S3-based log buckets are only accessible to select security, engineering, and technical operations team members, with security having a separate copy that is not accessible to any other team. Automated log monitoring alerts designated personnel of security events via a Security Orchestration and Automated Response (SOAR) solution.

4.3 System Security

4.3.1 Change Management

Copyright © Veeva Systems 2022

Changes to IT facilities and systems are managed using a documented change control process which requires adequate testing, review, and approval prior to releasing changes to production servers. Servers have file integrity monitoring to detect unauthorized changes to critical system files.

4.3.2 Vulnerability Management and Penetration Testing

Systems undergo periodic vulnerability and penetration testing by industry-recognized, third-party security specialists, using multiple overlapping enterprise-class security solutions to ensure that any vulnerability is identified and mitigated in a timely fashion. See Section 5.2 for additional details.

4.3.3 Third-party Service Delivery Management

Security requirements, ongoing monitoring, and change management clauses are in place for Veeva's service level agreements (SLAs) with each data center provider. Third-party suppliers are also assessed and audited based on risk.

4.3.4 System Planning and Acceptance

Technical Operations conducts periodic capacity planning and monitoring to ensure adequate system performance, taking into account planned customer growth. Servers undergo burn-in testing and are qualified for production use following standard configuration and hardening checklists as well as automated "smoke tests" to ensure the SiteVault application functions as designed.

Servers are hardened following a standard build checklist. Unnecessary ports and services are disabled, password policies are configured, and patches are periodically reviewed and installed. Server hardening minimizes the attack surface on production servers.

4.3.5 Monitoring

Application, database, and system monitoring are in place using centralized log aggregation and monitoring solutions (e.g., SIEM) tools. Responsible personnel are notified via email and SMS when alerts are triggered using automated log monitoring systems. Logs are secured using centralized syslog servers accessible only to a limited number of Technical Operations personnel. Performance monitoring is conducted using representative systems in multiple geographic locations throughout the world.

4.4 Veeva Internal Corporate Security

4.4.1 Wireless Security

The wireless network is secured using WPA2-Enterprise encryption, with new wireless deployments supporting network access control security that enforces malware protection and network monitoring.

4.4.2 Network Access Control (NAC)

Access to customer data on servers and other network services is controlled and requires either physical access to Veeva offices or an IPsec VPN connection.

SiteVault application production servers, including all servers hosting customer data, are in a separate logical network domain from the standard Veeva network accessed by Veeva employees. Access to the production servers requires two-factor authentication through a VPN and all communication is encrypted.
Veeva has a logical network segment for QA and development activities. Application developers and product management cannot access production systems.

Copyright © Veeva Systems 2022

5 Software Security Practices

5.1 Secure Software Development

Veeva performs a combination of automated and manual code reviews and provides training for developers on secure software development. Veeva maximizes system protection by testing security measures throughout the software development lifecycle. Veeva also procures software from software vendors (i.e. ISVs and CSPs) with SLAs or security clauses that specify prompt security patches and updates.

5.1.1 Design Phase

Automated and manual security control requirements are analyzed and documented during the design phase. This includes cryptographic controls for digital signatures, management of keys, and digital certificates.

5.1.2 Coding Phase

Secure coding practices are defined and reviewed, and access to source code and test data is controlled. Secure coding practices include session management security, as well as the prevention of vulnerabilities. Top 10 software vulnerabilities including malformed XML or HTTP requests, XSS, CSRF, and SQL injection. Automated and manual code reviews are also performed in this phase.

5.1.3 Testing Phase

Application software is tested for security vulnerabilities during this phase. Identified vulnerabilities are documented – including remediation plans – and monitored to ensure each vulnerability is addressed appropriately. Full application penetration testing is conducted for each major release.

5.2 Application Change Management

Changes to production systems follow a documented change program which includes clear scope definition, technical and regulatory impact assessment, requisite approvals prior to implementation, and testing commensurate with criticality of change. Change documentation follows standard operational procedures, and corresponding quality records are maintained in a validated Electronic Document Management System (EDMS). The change control program is designed to ensure that GxP production systems (i.e. Veeva software solutions) are maintained in a validated state upon changes to software and hardware configuration items (CIs).

5.3 Application Vulnerability Assessments

In any web application, including online banking websites or personal email, unauthorized attackers may find ways to access customer data by piggybacking through a user's computer while he or she is logged in. Veeva follows industry best practices, such as the guidelines provided by the Open Web Application Security Project (OWASP), to identify such vulnerabilities and defend against them. For example, if another website attempts to access SiteVault through a foreign computer using cross-site scripting (XSS) and cross-site request forgery (CSRF), the unauthorized request is recognized, and all attempts are automatically blocked. This is accomplished by validating user input to prevent cross-site scripting, and CSRF uses HTTP security headers.

Veeva conducts periodic vulnerability assessments on its software using automated and manual methods. These assessments are performed on production systems testing contemporary attack vectors. Activities include threat modeling, vulnerability classification using CVSS, and automated scanning to find potential SQL, LDAP, XPATH, or JQUERY injection paths and prevent against denial of service (DoS) attacks. Testing is performed with a combination of manual penetration tests and ongoing private bug bounty programs.

Copyright © Veeva Systems 2022

Examples of application vulnerability tests include: spoofing of user identity, tampering, repudiation, information disclosure (privacy breach or data leak), denial of service, and elevation of privileges.
Veeva uses a variety of third-party services for vulnerability management, private bug bounties, and penetration testing. Penetration testing is performed once a year and is full coverage and source code assisted.

Copyright © Veeva Systems 2022

6 Compliance

6.1 Legal Requirements

Veeva is committed to complying with applicable legislation including predicate rules, copyright, data protection, protection of financial data and other vital records, cryptography restrictions, rules of evidence, and other applicable laws. This commitment has been codified in an “acceptable use” policy document shared with all employees.

6.2 Privacy Requirements

Veeva complies with the European Union (EU) Data Protection Directive 95 / 46 / EC and the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) through the EU-US and Swiss-US Privacy Shield certifications as set forth by the U.S. Department of Commerce and the EU Commission regarding the collection, use, and retention of personal data from citizens of the European Union and Switzerland. Veeva’s Global Data Protection Officer (DPO) resides in the EU and reports independently to Veeva’s General Counsel and ultimately, the Board of Directors. The DPO measures the privacy program using a regular privacy impact assessments (PIAs) against the Generally Accepted Privacy Principles (GAPP), developed by the AICPA, and manages the remediation plan.

The EU Data Protection Directive and General Data Protection Regulation (GDPR) prohibits transfer of European citizens’ personal data to non-European Union nations that do not meet EU’s “adequacy” standard for data protection. The U.S. Department of Commerce, together with the European Commission, developed a “Privacy Shield” that allows U.S. companies to legally transfer and access personal data if they abide to a set of Privacy Shield principles. The framework gives abiding companies assurance that the EU and Switzerland will consider their practices “adequate” for privacy protection of EU and Swiss citizens. For more information about Veeva’s certifications, please see https://www.veeva.com/privacy/.

Whenever possible, Veeva complies with provincial and statutory data protection and privacy regulations such as CA SB 24. Veeva is also certified to ISO 27018, which are the privacy controls for cloud providers. An independent attestation report is available upon request.

6.3 Service Organization Control Reports (SOC 2)

Veeva has developed a set of IT controls that are mapped to an IT Risk Control Matrix, which fulfills the requirements of SOC 2. Veeva initially completed a SOC 2 / Type II Report in Q1 2014 and renews the report annually. For additional information on the SOC 2 standard, please see www.aicpa.org.

6.4 ISO 27001:2013

Veeva’s information security management program is certified ISO 27001:2013 compliant and provides an independent attestation report for ISO 27001 compliance as part of its certification. The Information Security Officer measures the information security program using a gap assessment against ISO 27001, Annex A, and manages the remediation plan.

6.5 21 CFR Part 11

Veeva has conducted an internal compliance assessment to document compliance with the ERES regulations, such as 21 CFR Part 11 and EU Annex 11. For customer data, Veeva has implemented the required 21 CFR Part 11 controls for open systems, including document encryption at rest.

6.6 EU Annex 11

Copyright © Veeva Systems 2022

Veeva has conducted an internal compliance assessment to document compliance with the EU Annex 11 regulation. For customer data, Veeva has implemented the required EU Annex 11 controls, including security controls for data, data storage, audit trails, incident management, electronic signatures, and business continuity.

6.7 Sarbanes Oxley (SOX) - Section 404 (IT)

Veeva has developed a set of IT controls that are mapped to an IT Risk Control Matrix, which fulfills the requirements of SOX-IT.

6.8 Governance, Risk, and Compliance (GRC) Framework

As stated, Veeva uses ISO 27001 / 2 as a GRC framework that combines the IT system controls from the various certifications and attestations mentioned above. Assessments of this framework are scheduled on a periodic basis and are planned to minimize disruption to operational systems. Remediation plans for findings from these assessments are monitored by Quality & Compliance.

6.9 Business Continuity / Disaster Recovery

Veeva has implemented a business continuity policy that outlines Veeva's Business Continuity Plan (BCP). The validity of Veeva's BCP is tested on an annual basis.

Copyright © Veeva Systems 2022

7 Information Security Policies

7.1 Policies and Practices (SLAs)

Veeva has implemented numerous policies to deliver the highest quality of service and security to our customers, including:

- Application Security Management Policy
- Business Continuity Policy
- Computer Systems Validation Policy
- Data Privacy Policy
- Information Security Policy
- IT Asset Management Policy
- Risk Management Policy
- Security Incident Management Policy

As new risks are identified, Veeva addresses these using analysis and risk reduction mechanisms. When appropriate, new requirements are added to the body of existing policies as updates or entirely new content. To deliver the highest level of service, Veeva has adopted industry-leading practices for security standards and guidelines using a risk-based approach to assist in the implementation goals stated in our security policies.

This includes the ISO 27001 / 2 and selected NIST SP 800 series standards including NIST SP 800-30, Guide for Conducting Risk Assessments.

7.2 Security Organization and Management

Veeva has a dedicated security team reporting to the Chief Information Security Officer and a Data Protection Officer to ensure our products are compliant with security and privacy requirements worldwide. The Information Security and Data Protection Officers help business managers, users, IT staff, and others fulfill their information security and privacy responsibilities. Plans, policies, and procedures are in place to ensure that there is accountability for the security and use of information assets.

3.5.2 Information Security Officer

Veeva's Chief Information Security Officer (CISO) function reports directly to the head of Operations. Security personnel receive ongoing training in all aspects of enterprise security from leading vendors and industry experts. The Security team reporting to the CISO consists of 3 teams: Security Operations (SecOps), Security Engineering (SecEng), Security Audit&Compliance.

The Chief Information Security Officer assesses external parties for information security compliance based on industry standards such as ISO 27001, Trust Service Criteria, or shared assessments.

Veeva maintains relationships with various security related organizations, such as InfraGard, the Northern California Regional Intelligence Center (NCRIC), NH-ISAC.

3.5.2 Security Operations

The Security Operations team is responsible for monitoring the Veeva Corporate and Veeva customer-facing solutions for signs of possible mis-use or compromise along with the health of the security solutions used to secure the environments. Critical security alerts are forwarded immediately, 24/7, to a rotating on-call resource.

Copyright © Veeva Systems 2022

3.5.2 Security Engineering

The Security Engineering team primarily works with Veeva product teams to provide guidance early in the product development phase (Security by Design). This team is also responsible for the maintenance of the tools such as the code security analysis solutions (SAST/DAST) and internal/external penetration testing.

3.5.2 Data Protection Officer

The Data Protection Officer (DPO) reports directly to Veeva's general counsel, and ultimately, the Board of Directors. Certifications include EU DPO Privacy Training and International Association of Privacy Professionals (IAPP) CIPP/E exam. In addition to overseeing product compliance, the DPO engages directly with our customers to explain Veeva's transparent approach to privacy and how we are managing requirements from governmental authorities.

7.3 Veeva Personnel Security and Training

All Veeva personnel undergo security training, and per Veeva's logical access policies, employees and contractors are granted systems access based on the principle of least privilege. Access is added during onboarding and removed per employee exit procedures. An access review is also triggered whenever personnel change job functions, and at least once per quarter for privileged accounts. Access is terminated on the last day of employment or prior for departing personnel.

3.5.2 Security background checks

Where permitted by law, all Veeva employees are subject to criminal background check and identity verification prior to commencing employment.

3.5.2 Veeva Employee Security and Awareness Training

Veeva has an information classification scheme to ensure such information has adequate protection of confidentiality, integrity, and availability. The Information Security & Privacy Procedures policy specifies security controls including multi-factor authentication, replication, encryption, and monitoring requirements, by content category.

All new hires must undergo information security awareness training within their first week of employment. Subsequent security awareness training is required annually for all active employees and contractors.

Personnel are assigned training on policies and procedures based on job function, and their compliance to training requirements is monitored.

7.4 Data Breach

All personnel are trained to immediately report security incidents. Such breaches are handled via documented procedural controls and reporting mechanisms. Timely customer notifications are part of this process.

Security incidents are documented, classified, investigated, escalated, and contained per the Security Incident Management Policy, and triaged by the Security Operations (SecOps) team. The investigation and collection of evidence is managed through the corrective and preventative action (CAPA) system, which includes a continuous improvement process.

As previously mentioned, Veeva automates the incident management notification process. Customers are typically notified via email, which is escalated to phone if a reply is not received in a timely manner.

Copyright © Veeva Systems 2022

8 Conclusion

In order to serve customers in highly regulated industries, Veeva adheres to the same rigorous requirements as our customers. This includes the vital need to secure data in an increasingly open and networked environment.

And as an industry-leading cloud software provider, Veeva invests significant time and resources in cutting-edge security, providing companies of all sizes a safer way to manage and share information both internally and across their partner ecosystem.

If you have any unanswered questions about Veeva's technical and operational security policies and procedures, please contact us at sitevaultsupport@veeva.com.

Copyright © Veeva Systems 2022

About Veeva Systems
Veeva Systems Inc. is a leader in cloud-based software. Committed to innovation, product excellence, and customer success, Veeva has more than 550 customers, ranging from the world's largest companies to small businesses. Veeva is headquartered in the San Francisco Bay Area, with offices in Europe, Asia, and Latin America. For more information, visit **www.veeva.com**.

Veeva Systems
Global Headquarters
Pleasanton, California, USA
4280 Hacienda Drive
Pleasanton, California 94588
+1 925 452 6500 | info@veeva.com | veeva.com

Copyright © Veeva Systems 2022