INSTABASE

Information Security Addendum

TABLE OF CONTENTS

Revised: Apr 28, 2023

1. INTRODUCTION

1.1 Purpose & Scope

This Information Security Addendum describes Instabase, Inc. and its affiliates' ("Instabase") security program, security certifications, and technical and organizational security controls to protect: (a) Customer Data from unauthorized use, access, disclosure, or theft; and (b) Instabase Platform products and services ("Instabase Service'' or "Services"). For purposes of this Addendum, "Customer Data" means any electronic data or information, including text, sound, video and image files, that: (i) Customer processes using either the Customer-hosted version, or the SaaS version of the Instabase Service; and (ii) is provided to Instabase by or on behalf of a Customer, pursuant to the applicable Customer agreement.

As security threats change, Instabase continues to update its security program and strategy to help protect Customer Data and the Services. As such, Instabase reserves the right to update this Information Security Addendum from time to time; provided, however, any update will not materially reduce the overall protections set forth in this Information Security Addendum. The then-current terms of this Information Security Addendum are available at https://trust.instabase.com/security/. This Information Security Addendum does not apply to any Services that are identified as alpha, beta, evaluation software or services, not generally available, limited release, developer preview, or any similar Services offered by Instabase.

2. INFORMATION SECURITY MEASURES

2.1 Security Certifications and Attestations

Instabase holds the following certifications and attestations:

- SOC 2 Type 2 (Trust Service Principles: Security, Availability, and Confidentiality)
- Health Insurance Portability and Accountability Act (HIPAA) – Attestation of Compliance

2.2 Corporate Identity, Authentication, and Authorization Controls

Instabase maintains industry best practices for authenticating and authorizing personnel access, including the following measures:

- Instabase uses single sign-on (SSO) to authenticate its personnel requiring access to third-party applications. Role Based Access Controls (RBAC) are used when provisioning access.
- Mandatory multi-factor authentication is used for authenticating to Instabase's identity provider. Device certificates are required as an additional authentication factor when authenticating personnel to sensitive services.
- Unique login identifiers are assigned to each user.

- Password requirements follow NIST 800-63B guidance, and as such, our policy is to use longer and complex passwords, with multi-factor authentication, but not requiring frequent changes.
- Established review and approval processes for any access requests to Services storing Customer Data.
- Quarterly access audits designed to ensure access levels are appropriate for the roles each personnel performs.
- Established procedures for promptly revoking access rights upon separation.
- Established procedures for reporting and revoking compromised credentials such as passwords and API keys.
- Established password reset procedures, including those designed to verify the identity of a user prior to a new, replacement, or temporary password.

2.3 Customer Identity, Authentication, and Authorization Controls

Instabase maintains industry best practices for authenticating and authorizing its Customers' access to Services. Such measures include:

- SSO integration via Security Assertion Markup Language (SAML 2.0).
- Instabase offers a built-in username and password user management system. All password-based logins are verified through MFA and we provide support for any 2FA app, such as Authy, Duo Mobile, or Google Authenticator.

2.4 Cloud Infrastructure and Network Security

Instabase maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:

- Instabase hosts its SaaS offering on Amazon Web Services ("**AWS**") and is protected by AWS's security and environmental controls. The production environment within AWS where Instabase's SaaS offering and Customer Data are hosted are logically isolated in a virtual private cloud ("**VPC**"). More information about AWS security is available at: https://aws.amazon.com/security/.
- Separate development, staging, and production environments.
- Primary backend resources are deployed behind a virtual private network ("**VPN**"). Obtaining a VPN certificate requires multi-factor authentication. Certain Services require additional authentication and authorization beyond the VPN as part of a defense-in-depth architecture.
- Routine audit of Services for security vulnerabilities. Dependencies are automatically scanned for security vulnerabilities as part of the development lifecycle of the Services.
- Instabase conducts third-party penetration tests at least annually and employs Offensive Security (OffSec) Certified Professionals.

- Application secrets and service accounts are managed by a third-party secrets management service. Non-*User* service accounts and resource configurations are audited for least-privilege.
- Network security policies and firewalls are configured for least-privilege access against a pre-established set of permissible traffic flows. Non-permitted traffic flows are blocked.
- Services’ logs are monitored for security and availability.

2.5 Change Management

Instabase maintains industry best practices to administer changes to the production environment–including to its Software, applications, and systems–using the following measures:

- Changes are carefully reviewed and evaluated in a test environment before being deployed into the production environment.
- Changes, such as, an evaluation of the changes in a test environment, are documented using a formal, auditable system of record.
- A rigorous assessment is carried out for all high-risk changes to evaluate their impact on the overall security.
- Plans and procedures are implemented in the event a deployed change needs to be rolled back to preserve the security of the Services.

2.6 System and Workstation Control

Instabase maintains industry best practices for securing Instabase’s corporate systems, including laptops and its own on-premises infrastructure by utilizing:

- Endpoint management of corporate workstations via an industry standard endpoint management service.
- Endpoint management of personnel-owned mobile devices via industry standard “bring-your-own-device” management service and associated policies.
- Automatic application of security configurations to workstations. For example, aligning to CIS benchmark standards for OSX workstations, an EDR agent, firewall rules, etc.
- Mandatory patch management.
- Tooling to defend against phishing, malware, and other risks borne from general web activity.
- Password requirements for workstations to align with CIS MacOS Benchmark—including minimum length, complexity and forced changes of password.
- Maintaining appropriate security logs including, where applicable, the initiating identity and timestamp.
- Synchronizing clocks with Network Time Protocol (NTP).

2.7 Data Access Control

Instabase maintains industry best practices for preventing authorized personnel from accessing data beyond their authorized access rights. Additionally, measures are deployed to prevent unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:

- By default, Instabase does not have access to the Services. If the Customer requires support or assistance with solution building, the Customer can either: (a) request a screen-sharing session; or (b) provision Instabase's authorized personnel with access via the Customer's identity provider, or in case of its SaaS offering–through its secure user management service.
- Personnel access to the Services follows the principle of least privilege. Only personnel whose job function involves supporting the delivery of Services are credentialed to the Services environment. Data access is authorized to personnel whose job function requires such access.
- All activities of Instabase personnel at the Services layer, including its infrastructure, are logged and auditable.

2.8 Disclosure Control

Instabase maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, as well as for securing and logging all transfers. Such measures include:

- Encryption of data at rest in production datastores using AES-256.
- Encryption of data in transit between Customers and Instabase using TLS version 1.2.
- Cryptographic standards are reviewed periodically, with selected technologies and ciphers being updated in accordance with assessed risk and market acceptance of new standards.
- Audit trail for all data access requests for production datastores, including but not limited to date and time of event, type of action performed, and name of files accessed.
- Full-disk encryption required on all corporate workstations.
- Device management controls required on all corporate workstations with the ability to remotely wipe the device of data.
- Restrictions on use of portable or removable media.
- Customized Customer Data retention policies can be implemented upon request.
- Customer Data can be deleted upon request.

2.9 Availability Control

Instabase maintains industry best practices for maintaining Services' functionality in case of an accidental or malicious event.

- Ensure that systems may be restored in the event of an interruption.

- Ensure that systems are functioning and faults are reported.
- Anti-malware and intrusion detection solutions installed on corporate workstations, which perform real-time analysis of machine and network behavior.

2.10 Segregation Control

Instabase maintains industry best practices for separate processing of data collected for different purposes, including:

- Instabase's SaaS offering includes deploying and hosting its Software in a dedicated, single-tenant environment in Instabase's cloud service provider account.
- Restriction of access to data stored for different purposes according to staff roles and responsibilities.
- Segregation of business information system functions.
- Segregation of testing and production information system environments.

2.11 Risk Management

Instabase maintains industry best practices for detecting and managing cybersecurity risks, including:

- Threat modeling to document and triage sources of security risk for prioritization and remediation.
- A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.

2.12 Personnel

Instabase maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:

- Background checks, where legally permissible, of personnel with access to Customer Data or supporting other aspects of the Services.
- At least once a year, Instabase personnel must complete a security and privacy training which covers Instabase's security policies, security best practices, and privacy principles.
- Instabase's dedicated security team also performs phishing awareness campaigns and communicates emerging threats to personnel.

2.13 Physical Access Control

Instabase maintains industry best practices for preventing unauthorized physical access to Instabase facilities, including:

- Physical barrier controls including locked doors and gates.
- 24-hour on-site security guard staffing.

- 24-hour video surveillance and alarm systems.
- Access control systems requiring photo-ID badge for entry to all Instabase facilities by Instabase personnel.
- Visitor identification and sign-in protocols.
- Logging of facility exits and entries.

2.14 Third-Party Risk Management

Instabase maintains industry best practices for managing third-party security risks, including with respect to its subprocessors or subcontractors to whom Instabase provides Customer Data. Such measures include:

- Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data.
- Vendor Security Assessments: All third-party vendors undergo a formal vendor assessment process maintained by Instabase's Security team.
- Periodic review of vendors in light of Instabase's security and business continuity standards, including the type of access and classification of data being accessed (if any), controls necessary to protect data, and legal or regulatory requirements.

2.15 Security Incident Response

Instabase maintains a security incident response plan for responding to and resolving events that compromise the confidentiality, availability, or integrity of the Services or Customer Data (each, a "**Security Incident**") including the following:

- Instabase deploys monitoring across its computing resources, with alert notifications sent to the Security Incident Response Team (SIRT) for triage and response. The SIRT employs an incident response framework to manage and minimize the effects of unplanned security events.
- Instabase aggregates system logs for security and general observability from a range of systems to facilitate detection and response.
- If Instabase becomes aware that a Security Incident involving Customer Data has occurred, Instabase will notify Customer within 72 hours, the time period required by applicable law, or the time period as provided in the appropriate agreement with a Customer.

2.16 Security Evaluations

Instabase performs regular security and vulnerability testing to assess whether key controls are implemented properly, and are effective as measured against industry security standards, its policies and procedures. Such testing also ensures continued compliance with obligations imposed by law, regulation, or contract with respect to the confidentiality, integrity, availability, and security of Customer Data, as well as the maintenance and structure of Instabase's information systems.

3. CONTACT US

Please direct your inquiries about Instabase's security, compliance, and privacy programs to compliance@instabase.com.