Last updated: May 6, 2026

Treasure AI

DATA SECURITY ADDENDUM

This Data Security Addendum ("**DSA**") forms part of the terms of service, master service agreement or other agreement that governs the purchase of Services between Treasure Data, Inc. dba Treasure AI ("**Treasure AI**") and the counterparty thereunder ("**Customer**") and that references this DSA (the "**Agreement**").

1. Definitions

Any capitalized term not otherwise defined in this DSA has the meaning ascribed to it in the Agreement, including any data processing addendum or similar document attached thereto or incorporated therein by reference.

For the purpose of this DSA, the following capitalized words shall have the following meanings:

a) **"Security Incident"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data.

b) **"Availability Incident"** means any event which prevents or interferes with Customer's ability to use Treasure AI's Service.

c) **"Business Logic"** means the commands, operations, definitions, nomenclature, settings and configurations input by or on behalf of Customer that determine how the Service organizes, analyzes, enriches, displays, exports or otherwise processes Customer Data . Business Logic includes, without limitation, job and query definitions, data connector input and output definitions, segment definitions, database and table definitions, and workflow definitions.

d) "**Controls Reports"** means an independent assessment and report of Treasure AI's internal controls under global standards including International Standard on Assurance Engagements ("ISAE") No. 3402, Assurance Reports on Controls at a Service Organisation and Statement of Standards for Attestation Engagements ("SSAE") No.18, Reporting on Controls at a Service Organisation, and American National Standards Institute ("ANSI").

e) **"Removable Media"** means any portable or removable hard disks, Universal Serial Bus (USB) memory drives, zip disks, optical disks, CDs, DVDs, digital film, memory cards (e.g., Secure Digital [SD], Memory Sticks [MS], CompactFlash [CF], SmartMedia [SM], MultiMediaCard [MMC], xD-Picture Card [xD]), magnetic tape, and all other removable data storage media.

f) "**Service**" means the cloud-based service(s) hosted by Treasure AI and ordered by Customer, as described in the applicable Order Form and Documentation. For avoidance of doubt, "Service" shall not include any Beta Services or Customizations, each as defined in Treasure AI's Terms of Service.

g) **"Third-party"** means an individual, company, government agency or other legal entity that is not a party to the Agreement between Treasure AI and Customer.

h) **"Treasure AI Personnel"** means employees and individual contractors engaged by Treasure AI or any Treasure AI subsidiary.

2. General Security Measures

a) Treasure AI's security measures described in this DSA are designed to: (1) ensure the security, confidentiality, integrity, and availability of Customer Data; (2) protect against anticipated threats or hazards to the security or integrity of Customer Data; and (3) protect against unauthorized access to or use of Customer Data. This DSA outlines the Administrative, Technical, Physical, and Environmental security measures that Treasure AI will maintain.

b) Treasure AI will inform Customer in writing of any Security Incident promptly after its discovery, *provided* the notification is not prohibited by applicable law.

c) Treasure AI will investigate the cause of the Security Incident and take reasonable steps intended to mitigate the impact of the Security Incident and shall keep information (including logs) of actions undertaken until both parties reasonably agree the information is no longer needed.

d) Treasure AI may notify Third-parties of a Security Incident where required under applicable law or any judgment or ruling of or binding agreement with any governmental authority or court.

e) Where appropriate, Treasure AI shall develop and execute a plan aimed at reducing the likelihood of a recurrence of such Security Incident.

3. **Administrative Controls Requirements**

a) **Controls Reports**

(i) **ISO/IEC 27001:2022.** Treasure AI shall obtain an ISO/IEC 27001:2022 certification annually. The scope of the ISO/IEC 27001:2013 ISMS (Information Security Management System) shall include the Service(s) provided to the Customer and such certification shall be maintained for the duration of the Subscription Term; and/or

(ii) **SOC 2 Type 2.** Treasure AI shall undergo an independent SOC 2 Type 2 audit covering the Security, Confidentiality, Availability, and Processing Integrity Trust Services Criteria (TSCs) annually. The scope of the SOC 2 Type 2 audit shall include the Service(s) provided to the Customer and such certification shall be maintained for the duration of the Subscription Term.

b) **Policies and Training**

(i) Treasure AI shall establish and maintain formal, documented, mandated, company wide security policies, standards, and procedures, including acceptable use of Treasure AI computers and systems (collectively, "**Information Security Program**.") The Information Security Program will be communicated to all Treasure AI Personnel in a relevant, accessible, and understandable form.

(ii) Treasure AI shall require all Treasure AI Personnel who may access Customer Data to sign a confidentiality / non-disclosure agreement.

(iii) Treasure AI shall require all Treasure AI Personnel to acknowledge in writing applicable policies within the Information Security Program, initially during their onboarding process and thereafter on an annual basis.

(iv) Treasure AI shall supply Treasure AI Personnel with appropriate ongoing training regarding information security and privacy procedures, risks, and threats on an annual basis.

c) **Risk Assessment(s)**

(i) Treasure AI shall maintain an Information Security risk management program which includes policies and procedures regarding the continuous assessment of risks relating to the confidentiality, integrity, and availability of Customer Data. Without limiting the foregoing:

1. Treasure AI shall maintain a risk register to track risks identified.
2. Treasure AI shall maintain a process to analyze, treat, and/or mitigate risks.
3. Treasure AI shall maintain a formalized risk acceptance process.

d) **Third-Party Risk Management (TPRM)**

(i) Treasure AI shall maintain a TPRM program which includes policies and procedures regarding the assessment of new and existing Third-parties, as it relates to potential security or privacy risks to Customer Data.

4. **Technical Controls Requirements**

a) **Access and Monitoring**

(i) Treasure AI shall implement formal procedures to control logical access to the Service.

(ii) When accessing the Service, Treasure AI personnel are required to use unique access credentials and passwords for authorization.

(iii) The access privileges of Treasure AI Personnel to Customer Data are strictly based on the individual's job function, role and responsibilities, and any such access first requires internal approval.

(iv) Such access privileges shall be changed or removed as applicable upon role change or termination of the individual's employment or service.

(v) Treasure AI shall monitor access to Customer Data by Treasure AI Personnel. Access logs shall be retained for 12 months, at minimum.

(vi) Periodic reviews are conducted to ensure access permissions/privileges are not granted to Treasure AI Personnel who no longer need them, and to ensure that granted permissions/privileges are not provisioned beyond the account's day-to-day needs.

b) **Encryption and Cryptography**

(i) **At-rest.** Treasure AI shall utilize NIST-approved algorithms to encrypt Customer Data stored within the Service.

(ii) **In-transit.** Treasure AI shall use industry-standard strong encryption (e.g., TLS 1.2 or higher with NIST-approved algorithms) to encrypt Customer Data while traversing over public networks.

(iii) Treasure AI uses encryption keys for secure storage, secure transport, token generation, and authentication.

(iv) Access to in-scope keys is restricted to authorized Treasure AI Personnel only.

c) **Malware / Anti-virus / Host Intrusion Detection (HIDS) Protection**

Except to the extent senior management determines, in its reasonable judgement, that an exception is warranted (and such exception is approved and documented in accordance with Treasure AI's formal procedures for exceptions):

(i) Treasure AI shall run anti-virus/malware and/or HIDS on endpoints and servers used in the delivery of the Service(s) to the Customer.

(ii) The aforementioned software is kept configured without the ability to be turned off or disabled by the end-user.

(iii) The aforementioned software is configured to run reasonably up-to-date versions, evaluated and deployed on a risk-based schedule that accounts for security impact, compatibility, operational stability, and vendor support status.

d) **Removable Media**

(i) Treasure AI Personnel are not permitted to write Customer Data to any form of Removable Media.

(ii) Treasure AI has established strict security controls to detect and/or monitor the writing of Customer Data to any form of Removable Media.

e) **Vulnerability Management**

(i) Treasure AI shall conduct vulnerability scans at least monthly to ensure the Service is adequately protected.

(ii) At least once annually, Treasure AI shall engage an independent third-party to perform penetration testing services.

1. The scope of the penetration includes the externally facing production systems, networks, and infrastructure used in the delivery of the Service.
2. Upon request, Treasure AI will supply Customer with an Executive Summary of the most recent tests. The Executive Summary will include the test date/period, who conducted the test(s), an overview of the test results, and treatment plans for critical and high rated findings. For any critical or high risk findings that the Treasure AI has decided to accept, upon request, Treasure AI will provide the Customer with documentation of the exception.

f) **Patch Management**

(i) Treasure AI will use best efforts to implement and maintain an effective patch management process to ensure operating systems, software, and services are up-to-date. If a patch or update is not applied within a reasonable timeframe, Treasure AI will implement compensating controls as appropriate to mitigate the risk until remediation can occur. In the event Treasure AI accepts the risk of not applying a patch or update in a timely manner, Treasure AI will follow its formalized risk acceptance process.

g) **Network Security**

(i) Network access to both internal and external Service shall be controlled, including, but not limited to, the use of properly configured firewalls with a Demilitarized Zone (DMZ) to protect internal systems and services.

(ii) Connections over a public network into the Service must be protected by using a virtual private network (VPN) tunnel and two-factor authentication.

(iii) Treasure AI shall utilize an intrusion detection and prevention system (IDS/IPS) within Treasure AI's Service production network environment. Treasure AI shall actively monitor the IDS/IPS for traffic that correspond to attempts at breaking the security of the Service provided.

(iv) Treasure AI must have a separation between the production, development, and test/staging environments for the Service supplied to the Customer.

h) **Secure Software Development Lifecycle**

(i) Service production code additions or changes must go through the Treasure AI's formalized change control procedures. The change control procedures should include application security checks, such as, Static

Application Security Testing (SAST), Dynamic Application Security Testing (DAST), open-source scanning, secrets scanning, independent code reviews, testing, and documented approval to deploy in production.

(ii) Treasure AI will use commercially reasonable efforts to triage Service vulnerabilities by conducting a risk assessment (i.e. determine if they're false positives) to remediate vulnerabilities in a timely manner.

i) **Backups**

(i) Treasure AI's availability and backup strategy is designed to ensure replication and fail-over protections in the event of a Security Incident or an Availability Incident.

(ii) Customer's Business Logic stored within the Service is backed up for 30 days and maintained using at least industry standard methods. The aforementioned data is replicated in at least one separate physical location.

(iii) Access to such backups will be limited to authorized Treasure AI Personnel only and includes controls intended to prevent unauthorized deletion or modification.

j) **Disaster Recovery & Business Continuity**

(i) Treasure AI maintains a Business Continuity (BC) / Disaster Recovery (DR) program, including a recovery plan, sufficient to ensure the Service can continue to function through an operational interruption and continue to be used by the Customer.

(ii) The BC/DR program provides a framework and methodology, including a business impact analysis and risk assessment process, necessary to identify and prioritize critical business functions.

(iii) In the event the Treasure AI experiences an event requiring recovery of systems, information or services, the recovery plan will be executed promptly.

(iv) Treasure AI must conduct annual testing of the BC/DR plan and provide documentation to the Customer upon request. Annual testing should include relevant stakeholders, lessons learned, and action plans to address any lessons learned.

5. **Physical and Environmental Controls Requirements**

Treasure AI relies on an Infrastructure-as-a-Service (IaaS) provider for the performance of the Service and is responsible for ensuring the following requirements are in place, and for conducting annual Third-Party due diligence:

a) Implementation of formal procedures to control physical access to Data Center(s).

b) When entering a Data Center(s), authorized personnel are required to have individual keys and or keycards for access.

c) Access to Data Center(s) is limited to authorized personnel only, who require access for day-to-day purposes.

d) Entry logs and video camera footage is in place and retained for a minimum period of 12 months.

e) Data Center(s) must be composed of the following:

(i) Multiple active power and cooling distribution paths, with redundant components of each, that are currently maintainable, providing high availability;

(ii) Flexibility to enable planned activity without disrupting computer hardware operations, with unplanned events causing minimal outage and impact; and

(iii) Necessary floor configuration and sufficient capacity and distribution to carry load on one path while performing maintenance on another path.

6. Audits

6.1 Upon Customer's written request at reasonable intervals considering the circumstances, Treasure AI will make available to Customer such information in Treasure AI's possession and control as Customer may reasonably request for the purpose of demonstrating Treasure AI's compliance with its data protection and security obligations under the Agreement. In satisfaction of such a request, Treasure AI may provide an audit report prepared by a respected independent audit firm(s) which is not older than 12 months.

6.2 Customer may contact Treasure AI to request an audit at Treasure AI's and/or Treasure AI Subsidiaries' premises as and to the extent provided in the DPA. Any such audit shall be conducted in accordance with the terms and conditions of the DPA.

6.3 Any information or audit report shared in accordance with this Section shall be Treasure AI's Confidential Information.