SaaSDossier

SOURCE-LINKED EVIDENCE RECORD · SAASDOSSIER

OpenAI

Independent Security Evidence Dossier

PUBLIC EDITION · No. 003

Source-linked · Reviewed before release · Every line traceable to vendor-published sources.

47	8	55
DOCUMENTED	QUESTIONS SURFACED	CONTROL FIELDS REVIEWED

Evidence date	22 Jun 2026	Dossier ID	SD-OPENAI-20260622	SHA-256	2eb5eb954b76…	Reviewed by	A. Vale · SD-R01

SaaSDossier

CONTENTS

00

Executive summary

This dossier records what OpenAI publishes about its security, privacy, and compliance posture, compiled from 14 vendor-owned sources reviewed before release on 22 June 2026. Across the 55-field SaaSDossier framework, **47 fields are Documented** — each supported by a cited, vendor-published source — and **8 are surfaced as questions for review**, where the reviewed sources did not address the field.

A question surfaced does not establish absence of a control — it marks a precise, ready-to-send follow-up for your vendor conversation. Nothing in this record is a score, rating, audit, or certification. It is an evidence record you can read in minutes and act on: before you sign, renew, integrate, or recommend.

> Independent and unaffiliated — SaaSDossier is not affiliated with, endorsed by, or sponsored by OpenAI. Every finding traces to the vendor's own published pages, listed in the source register (§06).

COVERAGE AT A GLANCE

Documented fields by domain

A count of documented fields per domain — this is counting, never scoring. There is no grade, risk meter, or verdict here.

Documented 47 Questions surfaced 8 55 fields reviewed

01

How to read this dossier

Every field in the evidence ledger carries exactly one of two states. Colour is never the only signal — each state also carries a text label, for colour-blind and low-vision readers.

DOCUMENTED

The reviewed vendor-published sources address this field. A cited quote and its source are shown. A documented limitation (e.g. a control that is available but not enforced by default) still reads *Documented* — we record what is published, not a verdict.

QUESTION SURFACED

The reviewed sources did not address this field. We surface a precise question to send the vendor. This is not a finding of absence.

Not identified in the reviewed vendor-published sources does not establish absence of the control.

02

Methodology & scope

This dossier records vendor-published evidence reviewed as of the evidence date. Each Documented field is supported by the reviewed vendor-owned sources listed in the source register. Items not identified in the reviewed sources are marked Question surfaced so a buyer can ask targeted follow-up questions. Question surfaced does not establish absence of the control. Vendor pages may change after the evidence date.

FRAMEWORK	SOURCES REVIEWED
55 control fields · 10 domains	14 vendor-published pages
EVIDENCE DATE	**REVIEWED BY**
22 June 2026	A. Vale · SD-R01

Scope is limited to sources the vendor itself publishes. We do not test systems, contact the vendor, or rely on third-party claims. Where a referenced vendor URL returned an error at review time, that is noted in the relevant field.

03

Framework-mapping matrix

Whether each widely-requested framework is addressed in the reviewed vendor-published sources.

FRAMEWORK	STATE IN REVIEWED SOURCES
SOC 2 Type II	DOCUMENTED
PCI DSS Level 1	DOCUMENTED
ISO/IEC 27001	DOCUMENTED
GDPR	DOCUMENTED
CCPA	DOCUMENTED
HIPAA	DOCUMENTED
FedRAMP	DOCUMENTED
CSA STAR	DOCUMENTED

04

Evidence ledger

All 55 fields, grouped into 10 domains and numbered `domain.item` for reference. Each documented field shows a cited quote and its vendor source.

COMPANY & LEGAL

3 / 3 documented

01.01 Vendor name

DOCUMENTED

OpenAI. Vendor name explicitly stated throughout all reviewed pages, including trust.openai.com, openai.com/security-and-privacy/, and all policy documents.

Source: trust.openai.com — Trust.openai.com

01.02 Legal entity & ownership

DOCUMENTED

The OpenAI Services Agreement identifies two contracting entities: OpenAI OpCo, LLC (1455 Third Street, San Francisco, California 94158) for customers outside EEA/Switzerland, and OpenAI Ireland Ltd. (1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland) for EEA/Switzerland customers. Parent entity is OpenAI Global, LLC per the sub-processor list.

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

01.03 Headquarters jurisdiction

DOCUMENTED

OpenAI OpCo, LLC is headquartered at 1455 Third Street, San Francisco, California 94158, United States. The governing law for non-EEA customers is the State of California.

Source: trust.openai.com — Trust.openai.com

CERTIFICATIONS & ATTESTATIONS

6 / 7 documented

02.01 SOC 2 Type II report

DOCUMENTED

OpenAI has undergone an independent SOC 2 Type 2 examination of controls relevant to Security, Availability, Confidentiality, and Privacy for its API and ChatGPT business product services. The 2025 SOC2 Report covers the period January 1, 2025 to June 30, 2025.

Source: trust.openai.com — Trust.openai.com

02.02 SOC 2 Type I report

QUESTION SURFACED

No evidence of a standalone SOC 2 Type 1 report identified. OpenAI references only SOC 2 Type 2 in reviewed documentation. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish SOC 2 Type I report. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

02.03 ISO/IEC 27001 certification

DOCUMENTED

OpenAI has received an ISO/IEC 27001:2022 Certificate documented on trust.openai.com. The certificate covers OpenAI's API, ChatGPT Enterprise, and ChatGPT Edu services. Also extends to ISO/IEC 27017:2015, ISO/IEC 27018:2019, and ISO/IEC 27701:2019. Announced August 25, 2025, on the Trust Portal update feed.

Source: trust.openai.com — Trust.openai.com

02.04 PCI DSS compliance

DOCUMENTED

OpenAI maintains PCI-DSS v4.0.1 compliance for the components of ChatGPT that support delegated payment processing. Trust portal lists PCI DSS v4.0.1 certification, and a Pentest Report and PCI DSS document are available.

Source: trust.openai.com — Trust.openai.com

02.05 CSA STAR registry

DOCUMENTED

CSA STAR Level 1 certification is listed on trust.openai.com. OpenAI states 'ChatGPT business product services and the API Platform have been evaluated by the Cloud Security Alliance Security Trust Assurance and Risk (STAR) registry for key principles of transparency and cloud security best practices.

> *"ChatGPT business product services and the API Platform have been evaluated by the Cloud Security Alliance Security Trust Assurance and Risk (STAR) registry for key principles of transparency and cloud security best practices."*

Source: trust.openai.com — Trust.openai.com

02.06 FedRAMP authorization

DOCUMENTED

OpenAI lists FedRAMP 20x as a compliance item on trust.openai.com, with dedicated documentation sections including 'OpenAI FedRAMP 20x,' 'OpenAI FedRAMP 20x Significant Changes,' and 'OpenAI FedRAMP 20x Services and Features.' The status page also shows a 'FedRAMP' component. Note: FedRAMP 20x is a pilot program and differs from traditional FedRAMP Moderate/High authorization.

Source: status.openai.com — Status.openai.com

02.07 Additional certifications & attestations DOCUMENTED

ISO/IEC 27017:2015 (cloud security controls), ISO/IEC 27018:2019 (protection of PII in public clouds), ISO/IEC 27701:2019 (privacy information management), ISO/IEC 42001:2023 (AI Management System covering consumer and business AI products), SOC 3 (public report available), TX-RAMP.

Source: trust.openai.com — Trust.openai.com

PRIVACY & COMPLIANCE

8 / 8 documented

03.01 GDPR compliance DOCUMENTED

OpenAI states it supports customer compliance with GDPR and offers a Data Processing Addendum (DPA) with Standard Contractual Clauses (SCCs) for EEA/Swiss data transfers. DPA is published at openai.com/policies/data-processing-addendum/. OpenAI Ireland Limited is the data controller for EEA/Switzerland customers.

Source: openai.com/enterprise-privacy — Openai.com Enterprise Privacy

03.02 CCPA compliance DOCUMENTED

CCPA compliance is listed on the trust.openai.com Trust Portal compliance section. The privacy policy includes California-specific disclosures. The DPA includes specific CCPA provisions in Section 5.

Source: openai.com/enterprise-privacy — Openai.com Enterprise Privacy

03.03 HIPAA compliance DOCUMENTED

OpenAI states it can sign Business Associate Agreements (BAA) in support of customers' compliance with HIPAA for the API Platform. ChatGPT for Healthcare is described as 'a secure workspace designed to support HIPAA compliance.

Source: trust.openai.com — Trust.openai.com

03.04 Data retention policy DOCUMENTED

Default API data retention is up to 30 days for abuse monitoring logs. ChatGPT Enterprise, Edu, Healthcare workspace admins control data retention duration; deleted conversations are removed within 30 days. API inputs/outputs are removed after 30 days by default. Zero Data Retention (ZDR) is available for eligible API endpoints.

Source: trust.openai.com — Trust.openai.com

03.05 Right to erasure / deletion

DOCUMENTED

The privacy policy Section 6 states users have 'the right to delete your Personal Data from our records.' Users can delete conversations, memories, and accounts; deletions are processed within 30 days. The DPA Section 2.11 requires OpenAI to return or delete Customer Data upon agreement expiry/termination.

Source: openai.com/enterprise-privacy — Openai.com Enterprise Privacy

03.06 Data portability

DOCUMENTED

The privacy policy Section 6 states users have 'the right to transfer your Personal Data to a third party (right to data portability).' Users can 'export your ChatGPT history and data in your account's data controls.

Source: openai.com/enterprise-privacy — Openai.com Enterprise Privacy

03.07 Cross-border data transfer mechanism

DOCUMENTED

The DPA Section 4 addresses international data transfers. EEA and Swiss Data transfers outside EEA/Switzerland are performed on the basis of Standard Contractual Clauses (SCCs) or EU Commission adequacy decisions. UK Data transfers use SCCs as amended by the UK Addendum.

Source: openai.com/policies/data-processing-addendum — Openai.com Policies Data Processing Addendum

03.08 EU data residency

DOCUMENTED

OpenAI offers data residency for the Europe (EEA + Switzerland) region via the eu.api.openai.com endpoint, supporting both storage and processing in-region. Data residency for ChatGPT is also mentioned (linked from openai.com/security-and-privacy/). EU data residency for non-US regions requires approval for abuse monitoring controls and ZDR amendment.

Source: trust.openai.com — Trust.openai.com

ENCRYPTION

3 / 5 documented

04.01 Encryption in transit

QUESTION SURFACED

No vendor-published source reviewed established Encryption in transit. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Encryption in transit. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

04.02 Encryption at rest

DOCUMENTED

OpenAI states data is encrypted 'at rest (AES-256).

Source: trust.openai.com — Trust.openai.com

04.03 Encryption key management

DOCUMENTED

OpenAI references Enterprise Key Management (EKM) in the platform documentation at platform.openai.com/docs/guides/your-data under a dedicated 'Enterprise Key Management (EKM)' section heading (section visible in navigation).

Source: trust.openai.com — Trust.openai.com

04.04 Customer-managed keys (BYOK)

DOCUMENTED

The platform documentation at platform.openai.com/docs/guides/your-data includes an 'Enterprise Key Management (EKM)' section, indicating customer key management capabilities exist. The section heading is visible in the page table of contents.

Source: trust.openai.com — Trust.openai.com

04.05 Field-level encryption

QUESTION SURFACED

No evidence of field-level encryption described in any of the reviewed vendor-published documentation. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Field-level encryption. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

INFRASTRUCTURE & HOSTING

5 / 6 documented

05.01 Cloud hosting provider

DOCUMENTED

The sub-processor list identifies multiple cloud infrastructure providers: Microsoft Corporation (Azure), Amazon Web Services, Google Cloud Platform, Oracle Cloud Infrastructure, CoreWeave, and Cerebras. The Trust Portal infrastructure section lists 'Azure' specifically, and the Risk Profile section lists 'Hosting: Major Cloud Provider.

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

05.02 Data hosting regions

DOCUMENTED

Per the sub-processor list and data residency documentation, processing regions include: United States, Australia, Brazil, Canada, France, Germany, India, Indonesia, Ireland, Italy, Japan, Malaysia, Mexico, Netherlands, Norway, Philippines, Poland, Singapore, South Africa, South Korea, Spain, Sweden, Switzerland, UAE, UK. Data residency API endpoints available for: US, Europe (EEA+Switzerland), Australia, Canada, Japan, India, Singapore, South Korea, UK, UAE.

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

05.03 Private network connectivity

QUESTION SURFACED

No evidence of private connectivity options (e.g., AWS PrivateLink, Azure Private Link, VPN) described in the reviewed vendor-published documentation. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Private network connectivity. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

05.04 Tenant isolation

DOCUMENTED

OpenAI states 'custom models are yours alone to use and are not shared with anyone else' and fine-tuned models 'are for your use alone and never served to or shared with other customers.' API and ChatGPT Enterprise use dedicated workspaces and organizational IDs. The Services Agreement Section 1.4 states 'OpenAI provisions the Services to specific entities using dedicated workspaces and organizational IDs.

Source: trust.openai.com — Trust.openai.com

05.05 Business continuity & disaster recovery

DOCUMENTED

The Trust Portal lists 'BC/DR' under Infrastructure and a 'Business Continuity/Disaster Recovery (BC/DR) Policy' under Policies. The risk profile notes 'Hosting: Major Cloud Provider.' Full BC/DR documentation requires Trust Portal access.

Source: trust.openai.com — Trust.openai.com

05.06 Uptime SLA commitment

DOCUMENTED

DOCUMENTED LIMITATION

The only surfaced evidence is a live status page showing aggregate uptime metrics (e.g., APIs 99.98%, ChatGPT 99.82%), and it explicitly says “Individual customer availability may vary.” No contractual SLA or service-credit remedy was found in the reviewed pages.

> *“Individual customer availability may vary.”*

Source: status.openai.com — Status.openai.com

ACCESS CONTROL

5 / 7 documented

06.01 Multi-factor authentication available

DOCUMENTED

OpenAI references 'Advanced Account Security' which 'adds stronger protections against unauthorized access, with enhanced sign-in and recovery safeguards' for individuals, and 'account security' features for enterprise. The Trust Portal Access Control section references authentication controls. SSO via SAML is supported for Enterprise.

Source: trust.openai.com — Trust.openai.com

06.02 Multi-factor authentication enforced

QUESTION SURFACED

No evidence that MFA is mandatorily enforced for all users or admin accounts in vendor-published documentation. The documentation describes optional advanced account security settings. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Multi-factor authentication enforced. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

06.03 Single sign-on (SAML)

DOCUMENTED

OpenAI supports 'Enterprise-level authentication through SAML SSO' for ChatGPT Enterprise, Edu, and Healthcare. SCIM is available through identity providers such as Okta and Entra ID.

Source: trust.openai.com — Trust.openai.com

06.04 Role-based access control

DOCUMENTED

RBAC (Role-Based Access Controls) is explicitly documented for ChatGPT Enterprise, Edu, and ChatGPT for Teachers. Admins can create custom roles with granular permissions (Canvas, apps, GPTs, search, projects, etc.) and assign roles to groups.

Source: trust.openai.com — Trust.openai.com

06.05 API key scoping & restrictions

DOCUMENTED

The platform supports project-level data retention controls and organizational API settings, including the Admin Invites Endpoint for project-specific user provisioning. The data residency controls are configurable per-project. Zero Data Retention and Modified Abuse Monitoring can be set at organization and project level.

Source: trust.openai.com — Trust.openai.com

06.06 Audit logging

DOCUMENTED

OpenAI provides an 'Enterprise Compliance API' (Compliance Platform) for ChatGPT Enterprise and Edu customers that provides access to logs and metadata, described as 'immutable, append-only compliance log events for auditing purposes.' Workspace admins can access audit logs of conversations and GPTs.

Source: trust.openai.com — Trust.openai.com

06.07 IP allowlisting

QUESTION SURFACED

No evidence of IP allowlisting or IP allowlist features described in the reviewed vendor-published documentation. This does not establish absence of the control.

Question to ask the vendor — The reviewed vendor-owned sources did not establish IP allowlisting. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

VULNERABILITY & INCIDENT

6 / 8 documented

07.01 Bug bounty program

DOCUMENTED

OpenAI has an active Bug Bounty Program hosted on Bugcrowd at bugcrowd.com/openai. The program 'offers safe harbor for good faith security testing and cash rewards for vulnerabilities based on their severity and impact.

Source: trust.openai.com — Trust.openai.com

07.02 Penetration testing cadence

DOCUMENTED

A 'Pentest Report' is listed as a document on trust.openai.com (requires access request). The Trust Portal also lists 'Application Penetration Testing' under App Security. The specific frequency of testing is not stated in reviewed pages.

Source: trust.openai.com — Trust.openai.com

07.03 Vulnerability disclosure policy

DOCUMENTED

OpenAI has a 'Responsible Disclosure' policy listed under App Security on trust.openai.com, and the Bug Bounty Program on Bugcrowd provides a formal channel for vulnerability disclosure.

Source: trust.openai.com — Trust.openai.com

07.04 Public vulnerability (CVE) history

QUESTION SURFACED

No CVE history or published security advisories identified in the reviewed vendor-published documentation. This does not establish absence of relevant CVEs.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Public vulnerability (CVE) history. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

07.05 Public breach disclosure history

QUESTION SURFACED

No breach history or publicly disclosed security incidents identified in the reviewed vendor-published documentation. This does not establish absence of past breaches.

Question to ask the vendor — The reviewed vendor-owned sources did not establish Public breach disclosure history. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

07.06 Public status page

DOCUMENTED

Status page is available at status.openai.com, showing uptime metrics for APIs, ChatGPT, Codex, FedRAMP, and Ads Platform components.

Source: status.openai.com — Status.openai.com

07.07 Incident notification SLA

DOCUMENTED

The DPA Section 2.7 states 'OpenAI will notify Customer without undue delay after becoming aware of any Personal Data Breach.' The privacy policy states deleted data is removed within 30 days. No specific hour-based SLA (e.g., 72 hours) is stated in the reviewed DPA text, though 'without undue delay' aligns with GDPR Article 33 requirements.

> *"OpenAI will notify Customer without undue delay after becoming aware of any Personal Data Breach."*

Source: openai.com/enterprise-privacy — Openai.com Enterprise Privacy

07.08 Published incident-response policy

DOCUMENTED

An 'Incident Response Plan' is listed on trust.openai.com under the Incident Response section (requires Trust Portal access). The DPA Section 2.7 also addresses Personal Data Breach notification obligations.

Source: trust.openai.com — Trust.openai.com

SUBPROCESSORS

3 / 3 documented

08.01 Public subprocessor list

DOCUMENTED

OpenAI publishes a public sub-processor list at openai.com/policies/sub-processor-list/ (last updated June 2, 2026), listing all third-party sub-processors by name, product/service, location of processing, and purpose.

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

08.02 Number of subprocessors disclosed

DOCUMENTED

The third-party sub-processor list contains 19 named entities (Cloudflare, Microsoft, CoreWeave, Oracle Cloud, Google Cloud, AWS, Cerebras, Snowflake, TaskUs, Intercom, Salesforce, Pylon Labs, Accenture, Fivetran, Confluent, Cinder Technologies, WorkOS, Okta, Merge API). Additionally 5 OpenAI affiliate entities are listed.

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

08.03 Subprocessor change notice period

DOCUMENTED

The DPA Section 2.9 states 'Customer may object to the use of such additional Sub-processor within 30 days of receiving notice of the change.' OpenAI will notify customers of sub-processor changes 'via blog post, notification within the Services or other reasonable means, or via email if Customer subscribes to email notifications on the Sub-Processor List site.

> *"Customer may object to the use of such additional Sub-processor within 30 days of receiving notice of the change."*

Source: openai.com/policies/sub-processor-list — Openai.com Policies Sub Processor List

AI GOVERNANCE

5 / 5 documented

09.01 AI usage disclosure

DOCUMENTED

OpenAI discloses that it trains models on data from public sources, licensed third-party data, human reviewers, and individual ChatGPT users (with opt-out available). By default, API and business product data is NOT used for training. The enterprise privacy page has a dedicated 'Model training FAQ' section.

Source: trust.openai.com — Trust.openai.com

09.02 Trains AI on customer data

DOCUMENTED

OpenAI explicitly states 'By default, we do not use your business data for training our models' for API, ChatGPT Enterprise, Business, Healthcare, Edu, and Teachers (after March 1, 2023). Training on customer data can occur only if the customer explicitly opts in.

Source: trust.openai.com — Trust.openai.com

09.03 AI data handling

DOCUMENTED

OpenAI states business data may be run through 'automated content classifiers and safety tools' generating metadata but not containing business data itself. Human review of business data is limited to specific scenarios (engineering support, platform abuse investigation, legal compliance). API inputs/outputs retained up to 30 days for abuse monitoring by default; ZDR available for eligible endpoints.

Source: trust.openai.com — Trust.openai.com

09.04 AI governance documentation

DOCUMENTED

OpenAI maintains ISO/IEC 42001:2023 AI Management System certification covering consumer and business AI products. The Trust Portal includes a 'Frontier Model Safety & Security' section with model evaluations, AI security documentation, model pretraining info, and OpenAI System Cards.

Source: trust.openai.com — Trust.openai.com

09.05 AI administration controls

DOCUMENTED

Enterprise workspace admins can control which AI apps/GPTs are enabled for the workspace, configure RBAC permissions limiting access to AI tools (web search, deep research, agent mode, etc.), and enable Lockdown Mode to restrict network-enabled AI capabilities.

Source: trust.openai.com — Trust.openai.com

SECURE DEVELOPMENT & ORG

3 / 3 documented

10.01 Secure software development lifecycle

DOCUMENTED

The Trust Portal lists 'Code Analysis' under App Security, and 'Application Penetration Testing.' OpenAI states models and systems are 'regularly evaluated through evaluations against industry benchmarks, adversarial testing and ongoing safety monitoring.' The Security Whitepaper (available via Trust Portal) addresses security controls.

Source: trust.openai.com — Trust.openai.com

10.02 Personnel security & training

DOCUMENTED

The DPA Section 2.3 states 'OpenAI will ensure that all persons authorized by OpenAI to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.' The Trust Portal Corporate Security section lists 'Employee Training.

> *"OpenAI will ensure that all persons authorized by OpenAI to process Customer Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality."*

Source: openai.com/policies/data-processing-addendum — Openai.com Policies Data Processing Addendum

10.03 Security organization / team

DOCUMENTED

OpenAI states its 'security team has an on-call rotation that has 24/7/365 coverage and is paged in case of any potential security incident.' The platforms are 'built with your security and privacy in mind and tested by a team of security experts.

Source: trust.openai.com — Trust.openai.com

05

Questions surfaced for review

The 8 fields the reviewed vendor-published sources did not address — written as questions you can send the vendor directly. A question surfaced is not a finding of absence.

01 SOC 2 Type I report

Certifications & Attestations

The reviewed vendor-owned sources did not establish SOC 2 Type I report. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

02 Encryption in transit

Encryption

The reviewed vendor-owned sources did not establish Encryption in transit. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

03 **Field-level encryption** — Encryption

The reviewed vendor-owned sources did not establish Field-level encryption. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

04 **Private network connectivity** — Infrastructure & Hosting

The reviewed vendor-owned sources did not establish Private network connectivity. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

05 **Multi-factor authentication enforced** — Access Control

The reviewed vendor-owned sources did not establish Multi-factor authentication enforced. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

06 **IP allowlisting** — Access Control

The reviewed vendor-owned sources did not establish IP allowlisting. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

07 **Public vulnerability (CVE) history** — Vulnerability & Incident

The reviewed vendor-owned sources did not establish Public vulnerability (CVE) history. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

08 **Public breach disclosure history** — Vulnerability & Incident

The reviewed vendor-owned sources did not establish Public breach disclosure history. Does the vendor document this, and if so, on which trust, security, docs, or legal page?

06

Source register

The 14 vendor-published pages reviewed for this dossier. Every Documented field cites one of these.

01	help.openai.com	REVIEWED
02	help.openai.com/en/articles/10479654	REVIEWED
03	help.openai.com/en/articles/11750701-rbac	REVIEWED
04	help.openai.com/en/articles/9261474	REVIEWED
05	openai.com/enterprise-privacy	REVIEWED
06	openai.com/policies/business-terms	REVIEWED

07	openai.com/policies/data-processing-addendum	REVIEWED
08	openai.com/policies/privacy-policy	REVIEWED
09	openai.com/policies/service-terms	REVIEWED
10	openai.com/policies/sub-processor-list	REVIEWED
11	openai.com/security-and-privacy	REVIEWED
12	platform.openai.com/docs/guides/your-data	REVIEWED
13	status.openai.com	REVIEWED
14	trust.openai.com	REVIEWED

SaaSDossier

07

Integrity record

DOSSIER ID	SD-OPENAI-20260622
VENDOR	OpenAI · Public Edition No. 003
EVIDENCE DATE	22 June 2026
FRAMEWORK	55 control fields · 10 domains
DOCUMENTED	47 fields
QUESTIONS SURFACED	8 fields
SOURCES REVIEWED	14 vendor-published pages
SHA-256	2eb5eb954b76894ac4f8e70e3c5ab2d6f5422d9d5ee804720e7a5f150d224c3e
REVIEWED BY	A. Vale · SD-R01

08

How to use this dossier

1. **Scan the coverage page.** See which domains are fully documented and where questions cluster — before you read a single field.
2. **Read the evidence ledger** for the domains that matter to your use case — each documented field carries the vendor's own words and a link to the source.
3. **Send the surfaced questions** (§05) to the vendor as your security follow-up — they are written to paste straight into an email or questionnaire.
4. **Keep it on file** with the integrity record (§07) as a dated, source-linked snapshot of what the vendor published at review time.

Questions about this dossier, corrections, or a vendor you'd like reviewed: `contact@saasdossier.com`

APPENDIX · GLOSSARY

Terms used in this dossier

Documented	The reviewed vendor-published sources address this field; a cited quote and source are shown.
Question surfaced	The reviewed sources did not address this field; a follow-up question is provided. Not a finding of absence.
Documented limitation	A control that is published but available-not-enforced, or otherwise qualified. Still recorded as Documented.
Vendor-published source	A page the vendor itself publishes — trust, security, docs, legal, status, or privacy pages.

SaaS*Dossier* SOURCE-LINKED EVIDENCE DOSSIERS