OpenAI

OpenAI Services Agreement Security Measures

1. Corporate Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing internal employee and service access, including the following measures:
    - OpenAI uses single sign-on (SSO) to authenticate to third-party services used in the delivery of the Services. Role Based Access Controls (RBAC) are used when provisioning internal access to the Services;
    - Mandatory multi-factor authentication is used for authenticating to OpenAI's identity provider.
    - Unique login identifiers are assigned to each user;
    - Established review and approval processes for any access requests to services storing Customer Data;
    - Periodic access audits designed to ensure access levels are appropriate for the roles each user performs;
    - Established procedures for promptly revoking access rights upon employee separation;
    - Established procedures for reporting and revoking compromised credentials such as passwords and API keys); and
    - Established password reset procedures, including procedures designed to verify the identity of a user prior to a new, replacement, or temporary password.
2. Customer Identity, Authentication, and Authorization Controls. OpenAI maintains industry best practices for authenticating and authorizing customers to the Services, including the following measures:
    - Use of a third-party identity access management service to manage Customer identity, meaning OpenAI does not store user-provided passwords on users' behalf; and
    - Logically separating Customer Data by organization account using unique identifiers. Within an organization account, unique user accounts are supported.
    - Cloud Infrastructure and Network Security. OpenAI maintains industry best practices for securing and operating its cloud infrastructure, including the following measures:
    - Separate production and non-production environments;
    - Primary backend resources are deployed behind a VPN.
    - The Services are routinely audited for security vulnerabilities.
    - Application secrets and service accounts are managed by a secrets management service;
    - 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; and
    - Services logs are monitored for security and availability.
3. System and Workstation Control. OpenAI maintains industry best practices for securing OpenAI's corporate systems, including laptops and on-premises infrastructure, including:
    - Endpoint management of corporate workstations;
    - Endpoint management of mobile devices;
    - Automatic application of security configurations to workstations;
    - Mandatory patch management; and
    - Maintaining appropriate security logs.
4. Data Access Control. OpenAI maintains industry best practices for preventing authorized users from accessing data beyond their authorized access rights and for preventing the unauthorized input, reading, copying, removal, modification, or disclosure of data. Such measures include the following:
    - Employee access to the Services follows the principle of least privilege. Only employees whose job function involves supporting the delivery of Services are credentialed to the Services environment; and
    - Customer Data submitted to the Services is only used in accordance with the terms of the DPA, Agreement, and any other applicable contractual agreements in place with Customer.

5. Disclosure Control. OpenAI maintains industry best practices for preventing the unauthorized access, alteration, or removal of data during transfer, and for securing and logging all transfers. Such measures include:
    - Encryption of data at rest in production datastores using strong encryption algorithms;
    - Encryption of data in transit;
    - Audit trail for all data access requests for production datastores;
    - Full-disk encryption required on all corporate workstations;
    - Device management controls required on all corporate workstations;
    - Restrictions on use of portable or removable media; and
    - Customer Data can be deleted upon request.
6. Availability control. OpenAI maintains industry best practices for maintaining Services functionality through accidental or malicious intent, including:
    - Ensuring that systems may be restored in the event of an interruption;
    - Ensuring that systems are functioning, and faults are reported; and
    - Anti-malware and intrusion detection/prevention solutions implemented comprehensively across our environment.
7. Segregation control. OpenAI maintains industry best practices for separate processing of data collected for different purposes, including:
    - Logical segregation of Customer Data;
    - Restriction of access to data stored for different purposes according to staff roles and responsibilities;
    - Segregation of business information system functions; and
    - Segregation of testing and production information system environments.
8. Risk Management. OpenAI 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;
    - Penetration testing is conducted on the Services at least annually, and any remediation items identified are resolved as soon as possible on a timetable commensurate with the associated risk. Upon request, OpenAI will provide summary details of the tests performed and whether the identified issues have been resolved;;
    - Annual engagements of a qualified, independent external auditor to conduct periodic reviews of OpenAI's security practices against recognized audit standards, including SOC 2 Type II certification audits. Upon reasonable request, OpenAI will provide summary details; and
    - A vulnerability management program designed to ensure the prompt remediation of vulnerabilities affecting the Services.
9. Personnel. OpenAI maintains industry best practices for vetting, training, and managing personnel with respect to security matters, including:
    - Background checks, where legally permissible, of employees with access to Customer Data or supporting other aspects of the Services;
    - Annual security training for employees, and supplemental security training as appropriate.
10. Physical Access Control. OpenAI maintains industry best practices for preventing unauthorized physical access to OpenAI facilities, including:
    - Physical barrier controls including locked doors and gates;
    - 24-hour on-site security guard staffing;
    - 24-hour video surveillance and alarm systems, including video surveillance of common areas and facility entrance and exit points;
    - Access control systems requiring biometrics or photo-ID badge and PIN for entry to all OpenAI facilities by OpenAI personnel;

- Visitor identification, sign-in and escort protocols; and
- Logging of facility exits and entries.

11. Third Party Risk Management. OpenAI maintains industry best practices for managing third party security risks, including with respect to any subprocessor or subcontractor to whom OpenAI provides Customer Data, including the following measures:
    - Written contracts designed to ensure that any agent agrees to maintain reasonable and appropriate safeguards to protect Customer Data; and
    - Vendor Security Assessments: All third parties undergo a formal vendor assessment process maintained by OpenAI's Security team.
12. Security Incident Response. OpenAI 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 including the following:
    - OpenAI aggregates system logs for security and general observability from a range of systems to facilitate detection and response; and
    - If OpenAI becomes aware that a Personal Data Breach has occurred, OpenAI will notify Customer in accordance with the DPA.
13. Security Evaluations. OpenAI performs regular security and vulnerability testing to assess whether key controls are implemented properly and are effective as measured against industry security standards and its policies and procedures and to ensure continued compliance with obligations imposed by law, regulation, or contract with respect to the security of Customer Data as well as the maintenance and structure of OpenAI's information systems.