AIWORKDESK · BY GZINFINI

Security & Data Handling

How AIWorkDesk protects customer identities, documents and AI interactions. Version 1.0 · October 2026

1. Overview

AIWorkDesk is a multi-tenant software-as-a-service AI knowledge base operated by Guangzhou Infini Technology Co., Ltd. ("gzinfini"). It runs entirely on Microsoft Azure in the **East US 2** region. Customers sign in with Microsoft Entra ID, upload documents to knowledge libraries, and ask questions that are answered by Azure OpenAI using only the documents each user is allowed to see.

2. Architecture and Azure services

Component	Azure service	Purpose and key controls
Web application and API	Azure App Service	Serves the web app and REST API. HTTPS only, TLS 1.2 minimum, FTP restricted to FTPS, remote debugging disabled, system-assigned managed identity.
Identity	Microsoft Entra ID	OAuth 2.0 / OpenID Connect sign-in; access tokens are validated for signature, issuer, audience, lifetime and the access_as_user scope on every request.
Application data	Azure Cosmos DB (serverless)	Workspace settings, users, document metadata, text passages and vector embeddings, conversations, reports, usage and audit records. Partitioned by customer tenant ID.
Original files	Azure Blob Storage	Uploaded documents stored under a per-tenant path. Shared-key access disabled, anonymous public access disabled, HTTPS only, TLS 1.2 minimum.
Generative AI	Azure OpenAI	Chat model for answers and reports; text-embedding-3-small for semantic search. Global Standard deployments.
OCR	Azure AI Document Intelligence	Read model extracts text from images and scanned PDFs (up to 200 pages per document).
Secrets	Azure Key Vault	Stores API keys that customers supply for their own Azure OpenAI resource. Azure RBAC authorization, soft delete with 90-day retention.
Email	Azure Communication Services	Transactional emails such as activation and cancellation notices.
Subscriptions and billing	Microsoft Marketplace	SaaS Fulfillment API v2. Webhook calls are authenticated with Microsoft Entra tokens; outbound API calls use a federated credential with no stored secret.

The application authenticates to Cosmos DB, Blob Storage, Key Vault, Azure OpenAI, Document Intelligence and Communication Services with its **managed identity** and Azure role-based access control. No database, storage or AI service keys are stored in application configuration.

3. Identity and access control

- **Single sign-on:** users sign in with Microsoft Entra ID work or school accounts. gzinfini never receives or stores passwords, and customers' Conditional Access and MFA policies apply automatically.

- **Work accounts only in the workspace:** personal Microsoft accounts are accepted only on the Marketplace activation page and are rejected by the workspace API.
- **Tenant binding:** each workspace is bound to the customer's Entra tenant ID from the validated token. Users join only through an invitation created by a customer administrator (the first administrator is set during activation).
- **Roles:** Tenant admin, Knowledge manager, Analyst and Viewer, each with a fixed permission set enforced by the API, not just the user interface.
- **Library permissions:** each knowledge library is open to all members or restricted to selected members. Search and answers only use passages from libraries the user can access.
- **Operator access:** gzinfini's platform console requires a gzinfini tenant account *and* a dedicated app role. It manages subscriptions and tenant status and shows aggregate counts; it does not display customer documents, questions or answers.

4. Tenant isolation

Every record in Cosmos DB carries the customer's tenant ID as its partition key, and every query is scoped to the tenant ID taken from the caller's validated token, never from client input. Files in Blob Storage are stored under a tenant-specific prefix and are only accessed through the API after the same checks.

5. Data protection

- **In transit:** all traffic uses HTTPS with TLS 1.2 or later, both between browsers and AIWorkDesk and between AIWorkDesk and Azure services.
- **At rest:** Cosmos DB, Blob Storage and Key Vault encrypt data at rest with AES-256 using Microsoft-managed keys.
- **Malware scanning:** every uploaded file is scanned on upload by Microsoft Defender for Storage; security alerts are emailed to gzinfini's security contact.
- **Customer-supplied keys:** keys for a customer's own Azure OpenAI resource are written to Key Vault, are never returned to the browser, and are deleted when the setting is removed or the tenant is purged. Custom endpoints must be HTTPS Azure OpenAI or Azure AI endpoints, which prevents requests to arbitrary hosts.
- **Web protections:** HTTP security headers (X-Content-Type-Options, X-Frame-Options: DENY, Referrer-Policy), file type and size validation (20 MB per file), and per-user rate limiting of AI requests.

6. AI data handling

- **What is sent to the model:** the user's question, recent turns of the same conversation, and the most relevant passages from documents the user is allowed to access. Embeddings are created for document passages and questions.
- **No training on customer data:** AIWorkDesk does not train or fine-tune models on customer content. Under Microsoft's terms for Azure OpenAI, prompts and completions are not used to train OpenAI or Microsoft models.
- **Processing location:** Global Standard deployments may process prompts in any Azure region where the model is available. Stored data remains in East US 2.
- **Abuse monitoring and content filtering:** Azure OpenAI applies Microsoft's content filters. According to Microsoft's documentation, Azure OpenAI may retain prompts and outputs for up to 30 days for abuse monitoring.
- **Grounded, verifiable answers:** answers cite their source passages, and the product reminds users to verify important information.
- **Bring your own model:** customers can route AI requests to their own Azure OpenAI resource, in which case that content is processed under the customer's own agreement with Microsoft.

7. Data lifecycle and retention

Data	Retention
Documents, extracted text and embeddings	Until deleted by a user (removed from storage and index immediately) or until tenant purge.
Conversations and reports	Until deleted by the user, or until tenant purge.

Users, invitations, libraries, usage and audit records	For the life of the subscription, then removed at tenant purge.
After cancellation	Data is kept for at least 7 days so the subscription can be reinstated, then all tenant data, files and stored keys are purged, normally within 30 days.
Backups	Cosmos DB periodic backups every 4 hours, retained for 8 hours. Blob Storage keeps three synchronous copies within the region (LRS).
Subscription and billing records	Retained as required for accounting and legal purposes.

8. Logging and audit

Administrative actions are written to a per-tenant audit log that customer administrators can review in the product, including invitations, role changes, document and library changes, AI settings and subscription events. gzinfini's platform operations, such as activation, cancellation and tenant purge, are recorded in a separate platform audit log.

9. Privacy and compliance

- The customer organization is the data controller (data user under the Hong Kong Personal Data (Privacy) Ordinance) for its content; gzinfini processes it only to provide the service. See **https://aw.gzinfini.cn/privacy**.
- AIWorkDesk is built on Azure services that are covered by Microsoft's compliance programs, such as ISO/IEC 27001 and SOC 2; reports are available on the Microsoft Service Trust Portal. AIWorkDesk itself does not currently hold independent certifications.

10. Incident response

If gzinfini becomes aware of a security incident affecting customer data, we will investigate, contain it and notify affected customer administrators without undue delay, including what happened, what data was involved and what we are doing about it. Suspected vulnerabilities can be reported to the contact below.

11. Shared responsibility

> Customers are responsible for managing their users and roles, applying Conditional Access and MFA in Microsoft Entra ID, ensuring they have the right to upload their documents, and reviewing AI output before relying on it. gzinfini is responsible for the security of the AIWorkDesk application and its Azure configuration; Microsoft is responsible for the underlying Azure infrastructure.