GoAGI

GoAGI Security & Compliance Overview

Introduction

GoAGI's secure language services environment spans a wide range of products and capabilities, supporting thousands of clients worldwide—including Fortune 500 companies and leading universities. With such a diverse and prominent customer base, our security program must constantly adapt to meet the specialized needs of different industries, ensuring every organization can confidently entrust its data protection and privacy to us.

Safeguarding client data is our top priority. GoAGI pledges to protect your business and information with industry-leading security measures that align with stringent regulations—such as GDPR and HIPAA. Special attention is given to highly regulated sectors like Finance and Healthcare, where our multi-tiered security protocols ensure consistent service availability and rapid recovery when necessary.

This overview details how GoAGI manages security in its day-to-day operations, covering system administration, business continuity, security and operations, data centers, and privacy.

Cloud Service Providers

GoAGI partners with **Amazon Web Services (AWS)** as its primary hosting provider for our language services platform. This partnership ensures high performance, reliability, and resilience across all our product offerings. AWS maintains multiple industry-recognized security certifications—most notably ISO 27001, CSA STAR, and SSAE16 SOC 1, SOC 2, and SOC 3—underscoring its commitment to rigorous data protection standards. Our reliance on AWS helps us safeguard client data while delivering secure, scalable solutions to organizations around the globe.

How Secure Is AWS?

- **Physical Security:**

  All AWS data centers are secured with robust access controls, including biometric authentication and 24/7 surveillance.

- **Constant Monitoring:**

  AWS provides proactive threat detection, real-time logging, and automated alerting to ensure rapid response to any potential incident.

- **Encryption:**

  Data is encrypted both at rest and in transit, leveraging advanced encryption technologies such as AES-256 for stored information and SSL/TLS protocols for transfers.

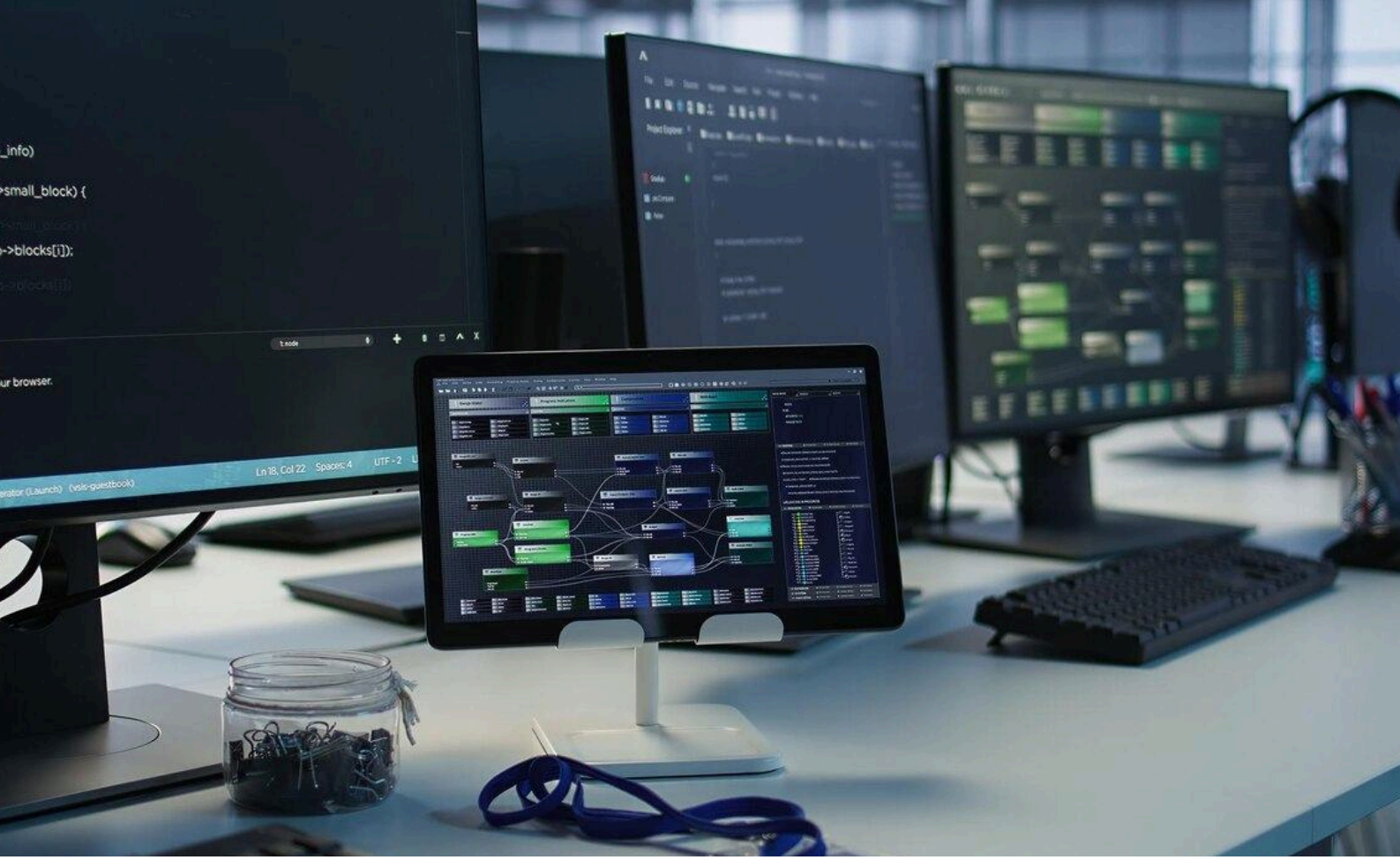
- **Global Redundancy:**

  Multiple availability zones and global points of presence help maintain uptime and data continuity, even under adverse conditions.

Identity and Access Management (IAM)

GoAGI employs a robust Identity and Access Management framework to secure all aspects of our cloud infrastructure:

- **Multi-Factor Authentication (MFA):**
  MFA is enforced for all administrative access to our cloud platforms. This ensures only authorized personnel can log in to management consoles and tools, adding an extra layer of security.
- **Access Controls & Least Privilege:**
  Each user is granted only the permissions necessary for their role. We review these permissions regularly to maintain strict adherence to the principle of least privilege.
- **Comprehensive Monitoring & Logging:**
  All actions within our management consoles and tools are centrally logged. Our security team continuously monitors these logs, using industry-leading tools to identify threats, intrusions, or abnormal behaviors. Any anomalies trigger automated alerts, prompting rapid investigation and remediation.
- **Security Intelligence & Response:**
  Our highly trained security experts leverage advanced analytics and tooling to provide proactive threat intelligence, rapid threat detection, and response capabilities. This approach enables us to stay ahead of evolving cyber threats and maintain a secure environment for client data.
- **Centralized Security Framework:**
  GoAGI's security posture includes clear policies for access control, authorization, and accountability. By aggregating and analyzing security logs in real-time, we swiftly detect and address potential risks.



Availability and Proactive Monitoring

GoAGI employs a comprehensive set of tools and processes to ensure the **continuous availability** and **responsiveness** of our services:

- **Redundant Connectivity & DDoS Protection**

  By utilizing redundant internet connections, advanced threat mitigation, and specialized Distributed Denial of Service (DDoS) protection, we maintain high uptime and safeguard against sophisticated cyberattacks.

- **24/7/365 Cloud Operations Center**

  Our dedicated Cloud Operations team monitors system health around the clock, using real-time alerts to immediately detect and address potential issues.

- **Rapid Security Upgrades**

  Our R&D teams regularly review third-party dependencies for known issues and push security updates with urgency—ensuring that critical patches are applied before vulnerabilities can be exploited.

- **Regular Vulnerability Scanning & Patching**

  We continuously scan our applications and infrastructure—covering operating systems, software dependencies, and the broader technology stack—to identify and patch vulnerabilities. This automated approach ensures our environment remains up to date with the latest security patches and system updates.

Data Security and Logical Protection

GoAGI implements a range of logical security measures to safeguard sensitive data:

1. Dedicated Cloud Operations

Our language services are hosted and managed by a specialized Cloud Operations team that is completely separate from GoAGI's corporate systems. This isolation limits the scope of potential threats.

2. Logical Segmentation & Encryption

Each customer's data is logically isolated to prevent unauthorized cross-access. All live and backup data is encrypted at rest—ensuring additional protection against data breaches.

3. Principle of Least Privilege

Only authorized staff members who require access to fulfill their responsibilities can view or manage client data or backups. These individuals undergo role-based security training and background checks in accordance with local regulations.

4. Regular Backups

Daily backups are performed and retained for up to four weeks, enabling point-in-time recovery. This approach mitigates data loss in the event of unforeseen incidents.

5. Network Segmentation & Firewalls

Servers requiring public internet access reside in a demilitarized zone (DMZ). All inbound and outbound internet traffic passes through multiple layers of firewalls and gateways, minimizing the attack surface while maximizing threat detection capabilities.

Business Continuity and Disaster Recovery

GoAGI deploys its language services and maintains backups across multiple data centers and geographic regions to safeguard against catastrophic failures such as natural disasters or other major disruptions affecting a single location. Our site selection process ensures that data residency requirements are met while providing maximum redundancy and resilience.

To deliver uninterrupted service, GoAGI's Cloud Operations staff are strategically located worldwide. This global distribution not only mitigates the impact of regional incidents on service management but also enables around-the-clock support—ensuring continuous, high-level business continuity for all our clients.

HIPAA Compliance

GoAGI recognizes that healthcare organizations require the highest level of data protection to safeguard protected health information (PHI). To address these needs, GoAGI offers HIPAA-compliant solutions that adhere to stringent privacy and security regulations. Our commitment to HIPAA compliance includes:

Technical Safeguards

- Audit Logging & Monitoring: Comprehensive logs capture every interaction with PHI, facilitating quick identification and mitigation of potential issues.
- Multi-Factor Authentication (MFA): Enforced for all privileged user accounts to prevent unauthorized access.

Robust Administrative Controls

- Role-Based Training: Staff undergo specialized HIPAA and security training to ensure proper handling of sensitive data.
- Background Checks: All personnel with access to PHI are screened according to local regulations.

Secure Infrastructure

- Encrypted Data Handling: PHI is safeguarded both in transit (TLS) and at rest (AES-256).
- Controlled Access: Access to PHI is strictly limited to authorized personnel with clearly defined roles.

Physical Security

- Data Center Protections: Our infrastructure is hosted in secure, HIPAA-ready data centers that employ multiple layers of access control and environmental monitoring.
- Redundancy & Disaster Recovery: Regular backups and geographically distributed infrastructure minimize downtime and data loss.

Continuous Compliance & Risk Assessment

- Regular Audits: We conduct periodic reviews to maintain alignment with HIPAA requirements and promptly update security measures as needed.
- Incident Response Plans: Established protocols ensure immediate action and notification if a breach or incident occurs.

PII Protection

GoAGI places a high priority on the protection of Personally Identifiable Information (PII). Our team has undergone specialized training in Identifying and Safeguarding Personally Identifiable Information (PII), a program originally developed for the U.S. Department of Defense personnel and contractors. By extending this training to our staff, we demonstrate our unwavering commitment to data security. Key focus areas include:

- **Incident Response:**
  Implementing clear procedures for detecting, reporting, and mitigating any potential PII breaches.
- **Continuous Education:**
  Providing regular refresher training to keep our team current on best practices and evolving regulations.
- **Access Control:**
  Enforcing the principle of least privilege so that only authorized personnel handle sensitive data.
- **Data Classification:**
  Recognizing different types of PII to apply the most appropriate safeguards.

Non-Disclosure Agreements (NDA)

GoAGI understands the sensitivity of our clients' intellectual property and confidential information. To maintain strict confidentiality and peace of mind:

- **Employee NDAs**
  All GoAGI employees and contractors are required to sign comprehensive NDAs prior to accessing any client data, ensuring legal and professional accountability.
- **Client-Specific NDAs**
  We are open to customizing NDAs to meet specific client requirements. This includes tailored clauses for regulated industries and heightened confidentiality stipulations.
- **Strict Compliance**
  Our internal policies reinforce NDA obligations through robust access controls, continuous security training, and ongoing monitoring—ensuring your confidential information remains protected at all times.

Our “No AI Training” Policy

At GoAGI, the privacy and confidentiality of your content is paramount. This principle is reflected in our firm commitment to never use client materials—whether audio, video, or text—for training any AI models or third-party machine learning systems. Below is a deeper look at how we maintain this policy:

Clear Scope of Work

- Authorized Use Only: We use your content exclusively for the services you request, such as transcription, proofreading, or translation.
- Contractual Assurance: All agreements explicitly prohibit the unauthorized use of client data for any other purpose, including AI training or data mining.

No Third-Party Sharing

- No Data Resale: We do not share or license client data to external parties, including AI developers or data brokers.
- Subcontractor Oversight: When specialized subcontractors or consultants are involved, they operate under binding agreements that mirror our “No AI Training” restrictions.

Internal Governance & Oversight

- Policy Enforcement: Our “No AI Training” policy is embedded in our internal compliance framework. Employees and contractors receive clear directives on permissible and prohibited data uses.
- Accountability Mechanisms: Regular audits and reviews confirm strict adherence to data-handling guidelines. Violations of policy can result in significant disciplinary action.

Transparent Retention & Deletion

- Retention Policies: We only retain materials as long as necessary for quality assurance, compliance, or per contractual obligations.
- Secure Deletion: Upon completion of services or at your request, data is securely purged from our systems, further eliminating the possibility of future misuse.

Strict Data Isolation

- Segmented Systems: Client content is logically separated within our infrastructure, ensuring that no single repository or process can siphon data for unrelated purposes.
- Limited Access: Access to client materials is restricted to authorized personnel based on the principle of least privilege. This minimizes any risk of data being diverted for outside projects.

Compliance & Best Practices

- Industry Standards: Our data-protection measures are frequently updated in line with best practices and legal requirements (e.g., GDPR, HIPAA).
- Client-Led Transparency: Should regulations or business needs change, we promptly adapt our processes to maintain security and respect client preferences.

GoAGI Security Tools and Capabilities

GoAGI employs **industry-leading security software** for Security Information and Event Management (SIEM). This includes comprehensive **log consolidation and analysis** as well as **file integrity monitoring**, ensuring we maintain deep visibility across our infrastructure.

- **Perimeter Firewalls & Intrusion Prevention**

  We maintain robust perimeter defenses with firewalls, intrusion detection, and intrusion prevention services. Combined with endpoint protection (anti-malware) and Extended Detection and Response (XDR) tools, our system continuously monitors network traffic, data, and logs—quickly detecting and stopping malware, breaches, or intrusions. Modules update automatically with new vendor signatures upon release.

- **24/7 Monitoring & Event Management**

  Our Cloud Operations Center functions around the clock (24×7×365) to rapidly identify and mitigate security events. This includes real-time monitoring, alerting, and logging to facilitate immediate incident response.

- **Threat Detection & Predictive Analytics**

  We use industry-recommended solutions for visibility into advanced threats, combining predictive analytics, security configuration management, and automated incident response. These tools enable us to preempt and address potential vulnerabilities across our cloud infrastructure.

- **System Hardening**

  All GoAGI systems are deployed following a system hardening profile that aligns with the Center for Internet Security (CIS) guidelines. This ensures our default configurations are secure and resilient against known exploits.

- **Regular Vulnerability Scanning**

  We have configured an industry-leading vulnerability scanning tool that performs regular automated scans of our infrastructure and hosted services, checking for compliance with the OWASP Top 10 and other relevant security standards. Reports guide our remediation efforts and help maintain a secure environment.

- **Penetration Testing**

  GoAGI conducts penetration tests on all new major versions of our products and services —or every 12 months—whichever comes first. This rigorous testing process helps us stay ahead of emerging threats and maintain a strong security posture.

- **ITIL-Compliant Incident Management**

  We rely on an IT Infrastructure Library (ITIL)-compliant ticketing tool to manage incidents (including security incidents), handle requests, uphold service level agreements, resolve problems, and oversee change management. This structured approach ensures efficient tracking and resolution of security events.

- **Change Advisory Board (CAB)**

  Our security team actively participates in the Change Advisory Board, reviewing all proposed changes from a security standpoint before they're implemented—this prevents unauthorized or risky modifications from being deployed.

In summary, **GoAGI** delivers **comprehensive security operations** ideally suited for highly regulated industries, including Finance, Healthcare, and beyond. We continually enhance our security measures to keep pace with evolving threats, regulations, and client requirements—ensuring our customers' data remains protected at the highest level.

Want to learn more?

goagi.ai/

Ready to connect with one of our specialists?

Contact us

About GoAGI

GoAGI is the world's first **Agentic AI Data Foundry**—a full-stack platform purpose-built to power the next generation of intelligent, self-improving systems. We enable AI to evolve **beyond training**—by transforming raw, real-world data into continuously learning, context-aware, multimodal intelligence. From battlefield robotics to autonomous agents and advanced decision-making systems, GoAGI provides the data infrastructure needed to scale agentic AI in the real world.

What We Do

- **Real-World Data Collection:**

  Multimodal, multilingual, and mission-critical—from geospatial to voice, sensor, video, and robotic data.

- **Semantic Data Infrastructure:**

  AI-native storage, content-aware retrieval, and dynamic memory systems built for evolving intelligence.

- **Adaptive Labeling Engine:**

  Self-learning annotation with human-in-the-loop, RLHF, and active learning workflows.

- **Deployment-Ready Pipelines:**

  From RAG to fine-tuning, GoAGI connects data to model to real-world action—fast.

Why It Matters

Tomorrow's AI isn't static—it's **agentic**. It perceives, adapts, and improves over time. GoAGI is the infrastructure that makes that future possible.

© 2025 GoAGI. All rights reserved. Information contained herein is deemed confidential and the proprietary information of GoAGI.