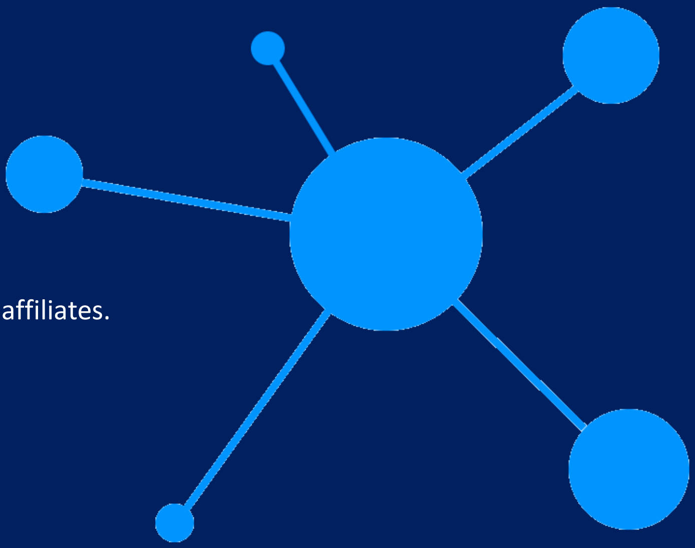
KnowledgeNet.ai

Security White Paper

September 2023

CONFIDENTIAL



ABSTRACT

Security and privacy are the highest priority at KnowledgeNet.ai. Our cloud platform is designed to be safe, secure, scalable, and reliable from the ground up. We earn customer trust by enforcing world-class security practices and standards. Our promise is to keep customer data private and secure through a multi-layered approach called “Defense in Depth.” (Reference #5) However, security doesn’t start with the technology; it starts with the business. This document details our security procedures and processes.

For direct inquiries, please contact info@knowledgenet.ai.

Table of Contents

DUE DILIGENCE

KnowledgeNet.ai maintains operational excellence. We believe our security practices should be clear and unambiguous. We have interwoven policies for employee background checks, code of conduct, business continuity, incident response, data privacy, data encryption, secure development, and audit/oversight. We have outlined some of these practices below.

Background Checks: KnowledgeNet.ai knows that security starts with the people entrusted with information. We perform rigorous background checks using an independent third-party provider to lay a secure foundation. We expect all our employees to respect the critical relationship between KnowledgeNet.ai and our customers.

Code of Conduct: KnowledgeNet.ai expects our employees and partners to treat client data BETTER than treat their own. We choose to be very conservative and risk-averse to mitigate the potential possibility of data breaches. Our staff is required to always be on guard against possible threats and to escalate any concerns they have.

Incident Response: Our commitment to all customers is to closely monitor and quickly respond to critical incidents. Our Engineering team uses the automated notification and alert systems to constantly monitor our platform for threats and Quality of Service (QOS) issues. Once identified, our team proactively begins mitigation procedures. KnowledgeNet.ai's real-time system status is available publicly at https://status.knowledgenet.ai.

Data Privacy: The KnowledgeNet.ai Privacy policy is publicly available at https://knowledgenet.ai/privacy.html. KnowledgeNet.ai adheres to the principle of “Least Privilege.” (Reference #6) Therefore, only those employees who require access to customer data as a necessary part of their job function are permitted to access it. These groups include our customer support and infrastructure security teams.

Data Encryption: We treat your data with the utmost care, whether a multi-tenant or enterprise customer. All sensitive data within the client datasets are encrypted with AES 256-bit or higher encryption while at rest and using TLS 1.2 or higher while in transit between the user and KnowledgeNet.ai infrastructure.

Secure Development: KnowledgeNet.ai performs regular security scans of our code, third-party libraries, and infrastructure. Before code is deployed to production, it must pass a rigorous security evaluation. After deployment, our systems are validated to ensure safety and stability.

Audit: All access to production environments is logged, and the logs are audited regularly. The production environments are accessible only to KnowledgeNet.ai operational staff and engineers, whose primary responsibility is to construct and maintain the KnowledgeNet.ai platform and services.

Penetration Testing: Penetration tests are performed on a regular basis to validate the system(s). This testing conforms to industry best practices for scope and coverage to ensure systems and data are protected.

COMPLIANCE

KnowledgeNet.ai fully complies with key government and industry regulations and policies in the US. KnowledgeNet.ai has achieved and maintained SOC 2 Type II compliance since June 2022 as validated by independent auditors.

HIPAA Compliance: By law, the HIPAA Privacy Rule applies only to covered entities: health plans, healthcare clearinghouses, and certain healthcare providers. KnowledgeNet.ai is not classified as a covered entity according to HIPAA, nor does KnowledgeNet.ai store medical information. It may be possible to architect your processes to comply with the HIPAA Privacy and Security Rules while using KnowledgeNet.ai for part(s) of your workflow. Our customers are strongly encouraged to familiarize themselves with the HIPAA requirements and security assessment procedures if applicable.

PCI DSS Compliance: KnowledgeNet.ai does not store cardholder information. However, processes built around KnowledgeNet.ai may be eligible to become PCI DSS compliant. Our customers are strongly encouraged to familiarize themselves with the PCI DSS requirements, Payment Application Data Security Standard (PADSS) Implementation Guide, and security assessment procedures if applicable.

SOC 2 TYPE II: Service Organization Control (SOC) framework consists of SOC 1, SOC 2, and SOC 3. SOC 1 is concerned with internal controls over financial reporting. SOC 2 and SOC 3 address security, availability, confidentiality, and privacy for service organizations. (Reference #8)

The SOC 2 Type II is the most comprehensive security certification in the industry. KnowledgeNet.ai undergoes independent audit of existing security protocols, processes, and systems to achieve SOC 2 Type II certification. The SOC 2 Type II certification provides confidence that our data management systems and processes are designed to keep sensitive information secure and reliable.

Our most recent SOC 2 Type 2 report is available upon email request to info@knowledgenet.ai.

DATA SECURITY AND ACCESS CONTROL

KnowledgeNet.ai implements best practices to ensure a robust and all-encompassing security posture. We strive to provide uninterrupted service and are standing guard against attack. All user authentication requires Multi-Factor Authentication codes, and user data is encrypted using AES 265-bit or higher encryption standards. Internal platform infrastructure is isolated from the public-facing infrastructure. Storage layers are encrypted and secured behind firewalls.

Multi-Factor Authentication: KnowledgeNet.ai ensures user information and identity protection through our use of MFA for user authentication. MFA is the industry-standard secure authentication mechanism that provides an additional layer of security by requiring the user to enter a short-lived pin in addition to their user credentials. (Reference #7)

SSL: The KnowledgeNet.ai platform is exclusively accessed via authenticated SSL, which uses TLS 1.2 or higher to encrypt all session traffic. The TLS protocol provides data encryption and authentication between users and KnowledgeNet.ai infrastructure. Our systems enforce TLS communication channels and support only certificates signed by well-known CAs to prevent third parties from gaining illegitimate access to information. We update encryption methods as they evolve.

Customer Data Backups: Data is stored in a combination of Graph and NoSQL databases. This data is replicated to a secondary region to guard against data loss. All data is encrypted in transit and at rest using robust industry encryption techniques. Files are stored redundantly across multiple regions using Amazon's S3 service and are secured by Amazon. S3 is secured with strict authentication and authorization rules.

Least Privilege: KnowledgeNet.ai has procedures and controls to limit access to customer data. Customer data may be accessed to support a customer-reported incident. This data is not accessed for debugging unless an error cannot be resolved without doing so; all private data is excluded from system logs. (Reference #6)

Network Firewalls: KnowledgeNet.ai adheres to industry-standard practices for securing infrastructure. We use firewalls to restrict access from external networks and between systems internally, and access is limited to only the specific ports and protocols required.

Denial-of-Service (DOS) Prevention: KnowledgeNet.ai implements best practices for preventing DoS attacks, including using Route 53 to maintain highly available DNS endpoints and following DoS prevention and mitigation practices. KnowledgeNet.ai DoS security controls protect against malicious users who overload the KnowledgeNet.ai platform with traffic.

Distributed Denial-of-Service (DDOS) Prevention: KnowledgeNet.ai data centers are hosted at AWS. AWS uses proprietary DDoS mitigation techniques to guard against the risk of attacks. In addition, AWS's networks are multi-homed across several providers to ensure network availability.

Clustered Infrastructure: CICD tools deploy new code to KnowledgeNet.ai clusters to ensure smooth transitions between software updates with no downtime.

INFRASTRUCTURE AND PHYSICAL SECURITY

KnowledgeNet.ai is hosted at Amazon Web Services (AWS) state-of-the-art data centers, which are highly scalable, secure, and reliable. AWS complies with leading security policies and frameworks, including but not limited to SSAE 16, SOC framework, and ISO 27001. KnowledgeNet.ai development machines run on unprivileged networks.

AWS physical security and reliability measures

Physical Security*:* KnowledgeNet.ai servers are always secured by trained security guards at each AWS hosting site, and access is authorized strictly on a least-privileged basis (Reference #6). The data centers use state-of-the-art electronic surveillance to monitor any suspicious activity. (Reference #1)

Availability*:* Every AWS data center uses best practices for fault tolerance at each level of the system infrastructure, including independent power grids, redundant power, HVAC, and fire suppression systems.

KnowledgeNet.ai security and reliability measures

Security Logs*:* AWS CloudTrail provides logs of all user activity to the KnowledgeNet.ai resources. KnowledgeNet.ai employees can monitor and track which actions were performed on each of the KnowledgeNet.ai resources and by whom.

Multi-Factor Authentication*:* Multi-Factor Authentication (MFA), such as using PIN in addition to their username and password, is required to access KnowledgeNet.ai infrastructure. (Reference #7)

Multiple Redundancy Zones*:* KnowledgeNet.ai infrastructure is hosted in various geographic regions, and Availability Zones within AWS environment to allow resources to remain operational under most circumstances, including natural disasters or system failures.

RELIABILITY & SLAS

SLAs: At KnowledgeNet.ai, our goal is to ensure you can successfully leverage our platform to support your business. All KnowledgeNet.ai customers have access to our Basic support plan. For additional assistance, please contact us to discuss your Enterprise needs.

Status reports: KnowledgeNet.ai maintains a real-time system status at https://status.knowledgenet.ai

Communications: If a data breach occurs, KnowledgeNet.ai notifies all impacted customers within 72 business hours of the data breach via email.

ADDITIONAL REFERENCES:

1) https://aws.amazon.com/compliance/data-center/controls;
2) https://aws.amazon.com/compliance/data-center/data-centers;
3) https://docs.aws.amazon.com/whitepapers/latest/aws-overview/security-and-compliance.html;
4) https://wa.aws.amazon.com/wat.pillar.security.en.html;
5) https://us-cert.cisa.gov/bsi/articles/knowledge/principles/defense-in-depth;
6) https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege;
7) https://www.cisa.gov/publication/multi-factor-authentication-mfa;
8) https://us.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome;
9) https://gdpr-info.eu/;