

Data Usage and Compliance

No Unauthorized Data Usage: GrowMind AI strictly adheres to its policy of not using customer data for purposes beyond agreed service provisions.

Geographic Data Residency: Data is stored in compliance with applicable regional laws, including GDPR and CCPA requirements.

Compliance Certifications: The AI network operates under ISO 27001, SOC 2, HIPAA, and other regulatory frameworks.

Database security for AI Server Networks

zero-trust model enforces strict identity verification for every access request.

- [Data Residency](/terms/data-residency) (/terms/data-residency)
- [VPC Service Controls \(VPC-SC\)](/vpc-service-controls/docs/supported-products) (/vpc-service-controls/docs/supported-products)
- [Access Transparency](/assured-workloads/access-transparency/docs/supported-services) (/assured-workloads/access-transparency/docs/supported-services)
- [Customer-managed encryption keys \(CMEK\)](/kms/docs/using-other-products) (/kms/docs/using-other-products)

Cybersecurity for AI Server Networks

Multi-tier firewalls block unauthorized access and provide a layered defense approach.
Critical systems are segmented to minimize lateral movement risks.
Intrusion Detection and Prevention Systems (IDPS)

AI-powered IDPS solutions monitor and block suspicious activity in real-time.
Threat Intelligence and Incident Response

A 24/7 incident response team is deployed to address and mitigate cybersecurity threats.
Threat intelligence systems track global cyber trends and preemptively strengthen defenses.
Routine Penetration Testing