# OmniCore Security & Compliance Overview

## Platform Posture

â¢ Built atop SOC 2 Type II audited infrastructure with continuous controls monitoring.

â¢ Isolated tenant workspaces with customer-managed encryption keys available.

â¢ Data residency selectable across EU, UK, US, and APAC sovereign regions.

â¢ Zero standing access: privileged actions require short-lived, auditable elevation.

## Authentication & Access

â¢ Mandatory SSO via SAML 2.0 or OpenID Connect.

â¢ SCIM provisioning keeps groups and roles in sync with identity provider.

â¢ Granular role-based access controls and row-level policies per dataset.

â¢ Step-up MFA challenges for high-risk actions or sensitive data exports.

# OmniCore Security & Compliance Overview

## Data Handling & Encryption

â¢ Data encrypted in transit with TLS 1.3 and at rest with AES-256.

â¢ Field-level encryption for PII, PHI, or PCI-controlled attributes.

â¢ Option for customer-controlled keys managed via AWS KMS or Azure Key Vault.

â¢ Automatic key rotation and tamper-evident logging for all cryptographic events.

## Network Controls

â¢ Private network peering or VPN tunnels for ingestion pipelines.

â¢ IP allow-listing for management interfaces and APIs.

â¢ Web application firewall with behavioural anomaly detection.

â¢ DDoS mitigation backed by cloud provider shield services.

# OmniCore Security & Compliance Overview

## Compliance Alignments

â¢ SOC 2 Type II report available under NDA.

â¢ ISO 27001 aligned controls with annual third-party gap assessment.

â¢ GDPR and UK GDPR compliant processing with signed DPA and SCCs.

â¢ HIPAA-ready deployment option with BAAs where required.

## Audit & Monitoring

â¢ Immutable activity trails with retention tailored per customer jurisdiction.

â¢ SIEM forwarding via syslog or webhook to Splunk, Azure Sentinel, or Datadog.

â¢ Real-time anomaly detection for unusual data access or export patterns.

â¢ Monthly control health reports supplied to security stakeholders.

# OmniCore Security & Compliance Overview

## AI Governance

â¢ Models operate on governed, customer-scoped vector stores.

â¢ No training on customer data; ephemeral context windows only.

â¢ Prompt and response logs redacted for sensitive fields.

â¢ Allow/deny guardrails to prevent unsafe or speculative answers.

## Shared Responsibility Model

â¢ OmniABI secures the platform, infrastructure, and core services.

â¢ Customers control identity, content quality, and downstream actions.

â¢ Joint runbooks cover incident response, breach notification, and audits.

# OmniCore Security & Compliance Overview

## Business Continuity

â¢ Active-active architecture with automated failover across regions.

â¢ Daily encrypted backups with point-in-time recovery controls.

â¢ Quarterly disaster recovery drills with documented results.

â¢ RPO of 15 minutes and RTO under 1 hour for critical services.

## Third-Party Risk

â¢ Vendor risk assessments and penetration tests conducted annually.

â¢ Continuous monitoring of sub-processors with contractual security obligations.

â¢ Public vulnerability disclosure programme and bug bounty coverage.

â¢ SBOM maintained for core services with automated dependency alerts.

# OmniCore Security & Compliance Overview

## Customer Next Steps

â¢ Request most recent SOC 2 and penetration test summaries.

â¢ Schedule technical deep dive for architecture and data flow diagrams.

â¢ Map OmniCore obligations into your internal control framework.

â¢ Align on joint incident response exercise within first 90 days.

â¢ Establish quarterly security governance touchpoints with OmniABI.