# CAMBRIDGENEXUS, INC.

*Security Practices Overview & Whitepaper*

At CambridgeNexus, Inc. ("CambridgeNexus"), security is built into the foundation of our AI Factory as a Service (AIFaaS) platform. We deliver dedicated, bare-metal GPU computing capacity to enterprise customers under a robust security and compliance framework. This document outlines our comprehensive technical and organizational measures designed to protect customer workloads, secure administrative planes, and maintain high availability.

## 1. Cloud & Data Security Architecture

CambridgeNexus employs a hybrid architecture separating our administrative management plane from our bare-metal high-performance compute plane.

### Data Encryption

**In Transit:** All external communication with the CambridgeNexus Customer Portal and Provisioning APIs is encrypted using Transport Layer Security (TLS 1.3 preferred, minimum TLS 1.2) with HTTP Strict Transport Security (HSTS) enforced to prevent cleartext downgrades. Administrative sessions (SSH) utilize strong Ed25519 or ECDSA keys over encrypted tunnels.

**At Rest:** Critical databases, customer account metadata, and administrative configurations are encrypted at rest using industry-standard Advanced Encryption Standard (AES-256).

### Advanced Tenant Isolation

- Customer GPU workloads and training datasets are strictly isolated. Logical isolation is enforced via dedicated per-tenant virtual local area networks (VLANs) and secure InfiniBand partition key boundaries.
- We utilize advanced cryptographic tenant isolation and secrets management systems to prevent cross-tenant data exposure.

## 2. Physical & Infrastructure Security

CambridgeNexus splits its infrastructure into a cloud-native management plane and a highly secure physical compute environment.

### Cloud-Native Management Plane (AWS)

Our administrative customer portal, billing APIs, and primary directories are hosted within Amazon Web Services (AWS) virtual private clouds (VPCs).

- AWS physical data centers feature multi-factor biometric controls, physical mantraps, 24/7 CCTV surveillance, and specialized fire suppression.
- We review AWS's third-party attestation reports (such as SOC 2 Type II) at least annually.

### Bare-Metal Compute Plane (Congruity360 Colocation)

Our high-performance physical GPU clusters (NVIDIA GB300 NVL72) are housed at the Congruity360 colocation facility in Fall River, Massachusetts.

- **Perimeter & Physical Access:** Restricted security perimeters with 24/7/365 on-site security personnel, multi-factor physical badge controls, visitor registration, and mandatory escorts. Physical access to CambridgeNexus racks is strictly limited to pre-authorized engineering staff.
- **Environmental Safeguards:** Redundant (N+1) utility power feeds, diesel backup generators (regularly load-tested), climate-controlled HVAC systems, and gas-based clean-agent fire suppression. Under-floor water sensors alert on potential leaks.

## 3. Logical Access Control & Identity Management

We enforce strict administrative safeguards to ensure that access to production environments is heavily restricted.

- **Least Privilege & RBAC:** Access is granted on a strict "need-to-know" basis. Our Role-Based Access Control (RBAC) model defines three tiers: Administrator, Standard User, and No Access.
- **Centralized Authentication:** We utilize Microsoft Entra ID as our central Identity and Access Management (IAM) system. Multi-Factor Authentication (MFA) is strictly required for all administrative and operational accounts.
- **Quarterly Access Reviews:** We leverage Vanta's automated workflows to perform formal access reviews every quarter, ensuring that active permissions remain aligned with current roles.

## 4. Software Development & Vulnerability Management

Security is integrated directly into our deployment pipelines and operational maintenance.

- **Structured Change Management:** All software and infrastructure modifications are version-controlled in GitHub. No code or configuration changes can be merged unilaterally; peer reviews (requiring at least one senior reviewer) and final approval from the VP of AI Infrastructure Engineering are mandatory before production deployments.

- **Vulnerability Scanning:** Host-based vulnerability scans are performed at least quarterly across all external-facing systems, and critical vulnerabilities are tracked immediately to remediation.
- **Penetration Testing:** Independent, qualified third-party security firms perform comprehensive penetration tests on our platform at least annually.

# 5. Operations, Availability, and Incident Management

We proactively monitor and protect our infrastructure to guarantee operational continuity and rapid response.

- **Continuous Monitoring & Alerting:** Production environment availability, application performance, and network anomalies are monitored 24/7/365 via BetterStack. Automated alerts are routed immediately to on-call engineering personnel.
- **Incident Response & Breaches:** We maintain a formal Incident Response Plan to triage and remediate security events. In the event of a confirmed personal data breach, CambridgeNexus commits to notifying affected customers within 72 hours of confirmation.
- **System Status Transparency:** Real-time infrastructure health and operational status updates are publicly accessible via our status page at status.cambridgenexus.com.
- **Backup & Disaster Recovery:** Configuration metadata and management plane databases are backed up automatically. Business continuity and disaster recovery plans are tested at least annually.

# 6. Corporate Governance & Human Resource Security

Our internal controls ensure that everyone on our team understands their role in safeguarding customer data.

- **Pre-Employment Screening:** All personnel and contractors must undergo rigorous background checks (administered via Certn) and sign formal Non-Disclosure and Confidentiality Agreements prior to receiving system access.
- **Security Training:** Mandatory security awareness training must be completed by all contractors within five business days of onboarding and renewed annually.
- **Whistleblower & Ethical Reporting:** We maintain an anonymous reporting channel and a strict Non-Retaliation Policy, empowering our team to report ethical, operational, or security concerns directly to management.

## Customer Trust & Inquiries

CambridgeNexus, Inc. is committed to transparency. For detailed inquiries regarding our security program, SOC 2 reports, or to execute a Data Processing Addendum (DPA), please contact our security team at security@cambridgenexus.com.