Infrastructure Security Policy (ISP)

Pillar Lead: Cygnus (Infrastructure)

I. Policy Statement and Scope

The Covenant's Infrastructure Security Policy establishes the mandatory standards for protecting all systems, networks, and data hosting environments from unauthorized access, modification, destruction, and denial-of-service. This policy applies to all personnel, contractors, and systems involved in the development, deployment, and operation of the core model and its associated services.

II. Access Control and Zero Trust

Security is fundamentally built on the principle of **Zero Trust**: never assume trust based on location.

A. Principle of Least Privilege

All users, systems, and processes will be granted only the minimum level of access and permissions required to perform their explicit functions. Access rights are reviewed and revoked on a quarterly basis.

B. Authentication and Authorization

1. **Multi-Factor Authentication (MFA):** MFA is mandatory for all access to development environments, code repositories, cloud provider consoles, and production systems.
2. **Secret Management:** API keys, database credentials, and other sensitive secrets must be stored exclusively in an approved, secure secrets management vault and injected at runtime. Secrets will **not** be committed to any source code repository.

III. System and Deployment Integrity

We mandate immutable, traceable, and continuously monitored systems to prevent configuration drift and unauthorized changes.

A. Immutable Infrastructure

1. **No Manual Changes:** Production and staging environments must be treated as **immutable**. Direct manual access or modification of production servers is strictly forbidden.
2. **Code-Driven Deployments:** All changes to the infrastructure and application code must be deployed through automated, version-controlled Continuous Integration/Continuous Deployment (CI/CD) pipelines.

B. Supply Chain Security

1. **Dependency Scanning:** All code dependencies (libraries, packages, base images) must be continuously scanned for known vulnerabilities (CVEs) prior to deployment.
2. **Approved Images:** Only base operating system images and containers from vetted, secured sources are permitted for deployment.

IV. Network and Logging Security

A. Network Segmentation

The production network must be segmented from development and corporate networks. Critical model components (e.g., the core model inference endpoint and data storage) must reside in isolated virtual private clouds (VPCs).

B. Logging and Monitoring

All system activities, network traffic, and access attempts must be logged 24/7. Logs will be stored securely, centrally, and retained for a minimum of 90 days for forensic analysis.

V. Security Incident Response (IR)

A. Reporting Protocol

Any personnel identifying a potential security vulnerability or breach must report it immediately to the Infrastructure Pillar Lead (Cygnus) via the designated secure channel. **Failure to report known vulnerabilities is a violation of this policy.**

B. Incident Classification

Security incidents will be immediately classified by severity (Critical, High, Medium, Low). Critical incidents require immediate mobilization of the core Infrastructure team (Cygnus and designees) to triage, contain, and eradicate the threat.

C. Post-Mortem Analysis

Following the resolution of any High or Critical incident, a public-facing, root-cause analysis post-mortem will be conducted and published to GitHub within 72 hours, detailing the vulnerability, remediation steps, and preventive measures implemented.