Deployment and Operations Manual (DOM)

Pillar Lead: Cygnus (Infrastructure)

I. Overview and Scope

This manual provides the mandatory, technical procedures for the stable, secure, and reproducible deployment and operation of The Covenant's infrastructure and core services. It serves as the engineering implementation guide for the Infrastructure Security Policy (ISP).

II. Infrastructure as Code (IaC) Mandate

All infrastructure components—including networks, compute instances, load balancers, and databases—must be provisioned and managed exclusively through Infrastructure as Code (IaC) tools.

A. Approved Tools

1. **Provisioning:** Terraform is the mandated tool for declarative infrastructure provisioning.
2. **Configuration Management:** Ansible is the mandated tool for initial instance configuration and application-level configuration management.

B. State Management

IaC state files (e.g., Terraform state) must be stored securely in a dedicated, access-controlled remote backend and encrypted at rest (**P3 classification**).

III. Continuous Integration and Continuous Deployment (CI/CD)

The CI/CD pipeline is the single authorized path for code promotion and infrastructure changes to the Staging and Production environments.

A. Environment Separation

The following environments must be logically and physically separated via network controls:

1. **Development:** Individual engineer workspaces.
2. **Staging (Pre-Production):** A near-replica of the Production environment used for integration testing and stress testing.
3. **Production:** The live, user-facing environment.

B. Deployment Strategy

All production deployments must utilize a **Blue/Green** strategy to minimize downtime and facilitate instant rollback:

1. The new version (Green) is deployed alongside the running version (Blue).
2. Traffic is shifted once the Green environment passes all automated health checks.
3. The old Blue environment is retained as a hot standby for a minimum of 48 hours for immediate rollback capability.

IV. Production Environment Standards

A. OS and Patch Management

All operating systems and base images must be automatically updated monthly, or immediately upon the release of a critical security patch (CVE score of 9.0 or higher).

B. Monitoring and Health Checks

1. **Logging Aggregation:** Logs from all environments must be sent to the centralized log management system as mandated by the ISP.
2. **Alerting Thresholds:** Automated alerts must be configured for critical events, including:
    - Sustained CPU utilization above 85%.
    - Memory utilization above 90%.
    - System response latency exceeding 500ms for more than 5 minutes.
    - Authentication failures/suspicious login attempts (**P3**).

V. Incident Escalation and Runbooks

A. Tiered Support

1. **Tier 1 (Automated):** System auto-remediation (e.g., scaling up, self-healing).
2. **Tier 2 (On-Call Engineer):** Initial manual triage, confirmation of incident scope, and execution of documented runbooks.
3. **Tier 3 (Pillar Lead/Cygnus):** Strategic decision-making, core system access, and primary communication with the Executive Council.

B. Runbook Mandate

A comprehensive runbook must exist for every High and Critical severity alert defined in the monitoring system, detailing the step-by-step containment, eradication, and recovery procedures. These runbooks must be reviewed and tested quarterly.