Infrastructure and Network Security Policy

Version: 1.0
Last Updated: October 2025
Approved By: Chief Technology Officer (CTO)

1. Purpose

This policy establishes Orbitel.ai's framework for maintaining a secure and resilient infrastructure.
Its objectives are to:

- Protect Orbitel's systems from unauthorized access, misuse, or disruption.
- Ensure high availability, reliability, and performance for all AI and SaaS services.
- Maintain compliance with security and privacy obligations globally.

2. Scope

Covers all Orbitel-managed:

- Cloud infrastructure and platforms (production, staging, and development).
- Networking components, such as firewalls, routers, VPNs, and intrusion detection systems.
- Endpoints, servers, and employee devices connected to Orbitel's corporate network.

3. Governance and Responsibilities

- **CTO** is accountable for infrastructure resilience and compliance.
- **Infrastructure and DevOps Teams** design, implement, and monitor network controls.

- **Security Operations Center (SOC)** provides continuous monitoring and threat detection.

4. Policy Statements and Controls

a. Network Architecture and Segmentation

- Networks are segmented to separate production, staging, and corporate environments.
- Critical systems are isolated through firewalls and virtual private cloud (VPC) boundaries.
- Remote access requires VPN connectivity with MFA.

b. Perimeter Security and Defense-in-Depth

- Firewalls and intrusion prevention systems (IPS) protect against external threats.
- Web Application Firewalls (WAF) defend Orbitel's AI APIs from injection and DDoS attacks.
- DNS security and anti-spoofing controls are enforced across all zones.

c. Endpoint and Server Security

- All systems are configured using secure baseline templates.
- Endpoint Detection and Response (EDR) tools are deployed for malware prevention.
- Operating systems and libraries are updated via an automated patch management schedule.

d. Encryption and Transmission Security

- All data in transit uses TLS 1.2 or higher; legacy protocols are disabled.
- VPNs use IPSec or SSL-based encryption for administrative access.
- Internal system-to-system communication is authenticated and encrypted.

e. Monitoring and Alerting

- Centralized SIEM (Security Information and Event Management) tools aggregate and analyze logs.
- Real-time alerts are triggered for anomalies, unusual traffic, or potential intrusions.
- System performance and uptime are monitored 24/7.

f. Change and Configuration Management

- Infrastructure changes are documented, peer-reviewed, and approved prior to deployment.
- All configurations are version-controlled and validated against security baselines.
- Configuration drift is detected and remediated automatically.

g. Resilience and Redundancy

- Orbitel maintains multi-region deployment with automated failover for critical services.
- Load balancing and distributed storage protect against single points of failure.
- Regular disaster recovery tests verify system restoration capabilities.

5. Compliance and Continuous Improvement

Orbitel benchmarks its network security practices against **ISO/IEC 27001**, **SOC 2 Type II**, and **NIST CSF** frameworks.
Annual third-party penetration tests, cloud provider security reviews, and internal audits ensure continuous improvement.