Zero Trust Network and Access Policy

Document ID: IE-ZTP-2025.01
Version: 1.0
Effective Date: 2025-11-01
Department: IT & Engineering - Security

1. Core Principle

Never Trust, Always Verify. Access is not granted based on location (internal network), but on the authenticated identity of the user or service and the assessed security posture of the device.

2. Identity and Access Management (IAM)

- **Central Identity:** All access (applications, infrastructure, cloud console) must be managed via the central Identity Provider (IdP).
- **Multi-Factor Authentication (MFA):** MFA is **mandatory** for all employees, contractors, and service accounts accessing NexaCore's production environment or sensitive data (P-1, P-2 data).
- **Least Privilege:** Access rights must be scoped to the minimum required for the function (Just-in-Time, or JIT, access is preferred) and reviewed quarterly.

3. Network Segmentation and Micro-segmentation

- **Network Level:** All cloud VPCs and subnets are considered untrusted. Firewalls default to **DENY**.
- **Service Level (Micro-segmentation):** Services within Kubernetes must communicate only via encrypted, authenticated connections (mTLS). Ingress/Egress rules must explicitly define permitted service-to-service communication.
- **Remote Access:** Direct VPN access to the corporate network is phased out. Remote access to critical resources must be done via a secure gateway that verifies device health (antivirus, patch level) before granting JIT access.

4. Monitoring and Logging

All access attempts, policy violations, and network flows must be logged to a central, tamper-proof security information and event management (SIEM) system. Automated alerts must be configured for all suspicious access patterns.