Network Segmentation Policy

Our organization segments its cloud and on-premises production networks based on the sensitivity of assets and their exposure requirements to the open internet.

Key Measures:

- Segregation of sensitive environments (production, staging, development) with strict ACLs.
- Firewalls and security groups enforce least privilege between sub-networks.
- Critical assets (databases, authentication systems, payment infrastructure) are placed in private subnets without direct internet access.
- Web-facing components are isolated in demilitarized zones (DMZs).
- Continuous monitoring and access reviews ensure segmentation is effective and updated as architecture evolves.

This segmentation approach minimizes the attack surface, reduces lateral movement risk, and ensures regulatory and security compliance.