☁️ Cloud Security Policy

Policy Title: Cloud Security Policy

Policy Type: IT Security / ISMS

Version: 1.0

Owner: IT Security / Cloud Infrastructure Team

Effective Date: [Insert Date]

Review Frequency: Annually or upon major cloud changes

1. Purpose

To ensure the confidentiality, integrity, and availability of systems and data hosted in cloud environments by defining security requirements, access controls, and operational procedures.

2. Scope

This policy applies to:
- All cloud-based infrastructure, applications, storage, and services
- All users with access to cloud resources
- Third-party providers and managed services

3. Cloud Provider Selection Criteria

- Provider must comply with industry standards (ISO 27001, SOC 2, GDPR, etc.)
- Regional data residency (e.g., Saudi for KSA clients)
- SLA for availability and support

4. Access Management

- Enforce Multi-Factor Authentication (MFA) for all users
- Role-Based Access Control (RBAC) with least privilege principle
- Periodic review and deactivation of unused credentials

5. Data Protection

- Data encryption at rest and in transit using AES-256/TLS 1.2+
- Tokenization or masking for sensitive fields
- Daily backups stored in a separate secure zone

6. Network Security

- Use Virtual Private Cloud (VPC) or private subnets
- Implement firewalls, security groups, and WAFs
- Disable public access unless explicitly required and approved

7. Monitoring & Logging

- Enable centralized logging (e.g., AWS CloudTrail, Azure Monitor)
- Monitor for unauthorized access, misconfigurations, and anomalies
- Integrate with SIEM for real-time threat detection

8. Vulnerability Management

- Periodic vulnerability scans of cloud workloads
- Patch management for OS, middleware, and applications
- Use of container security tools (if applicable)

9. Incident Response

- Cloud-specific incident response procedures
- Immediate revocation of compromised credentials
- Logs retained for forensic investigation

10. Business Continuity & Disaster Recovery

- DR plan tested annually
- Replication across availability zones/regions
- Defined RPO (Recovery Point Objective) and RTO (Recovery Time Objective)

11. Compliance & Audit

- Maintain evidence of compliance with customer and legal requirements
- Perform regular third-party audits
- Enforce contractual clauses with cloud vendors

12. Training & Awareness

- Annual cloud security training for IT staff and users
- Secure development training for cloud-native applications

13. Policy Violations

Violations of this policy may result in disciplinary action, revocation of access, or termination, depending on severity.