Cloud Security and Compliance Checklist

1. Identity & Access Management

- □ Multi-factor authentication enabled for all accounts
- □ Least privilege access enforced
- □ Unused accounts regularly reviewed and removed
- □ Strong password policies in place

2. Data Protection

- □ Data encryption at rest and in transit
- □ Regular data backups implemented
- □ Sensitive data identified and classified
- □ Key management follows best practices

3. Network Security

- □ Security groups and firewalls configured
- □ Public access to cloud resources restricted
- □ Regular network vulnerability scans
- □ Segmentation of sensitive environments

4. Monitoring & Logging

- □ Centralized logging enabled
- □ Alerts for unauthorized or suspicious activities
- □ Audit trails retained per policy
- □ Regular log reviews conducted

5. Compliance & Governance

- □ Compliance requirements identified and documented
- □ Regular risk assessments performed
- □ Policies reviewed and updated regularly
- □ Roles and responsibilities clearly defined

6. Incident Response

- □ Incident response plan in place and tested
- □ Roles assigned for incident management
- □ Contacts for cloud provider support documented
- □ Post-incident reviews conducted