Security Architecture for Cloud Environments

1. Overview

This document outlines a high-level security architecture framework for organizations adopting cloud environments. It provides principles, layers, and controls to mitigate risks and ensure the security of cloud-based assets.

2. Security Principles

- Shared Responsibility Model
- Zero Trust Architecture
- Defense in Depth
- Least Privilege Access
- Continuous Monitoring & Improvement
- Automation & Consistency

3. Architectural Layers

Layer	Description
Physical / Infrastructure	Provider-managed. Includes physical security, data centers, network infrastructure.
Network	Cloud VPCs, subnets, firewalls, VPNs, secure connectivity, segmentation.
Compute & Storage	Servers (VMs, containers), storage buckets, encryption, backup, DR.
Identity & Access	Users, roles, policies, multi-factor authentication (MFA), IAM controls.
Application	Secure coding, API security, secret management, vulnerability management.
Data	Classification, encryption at rest and in transit, key management, DLP.
Monitoring & Response	Logging, alerts, SIEM, incident response plans, metrics dashboards.

4. Key Controls & Practices

- Identity & Access Management (IAM): Role-based access, policy review, least privilege
- Network Security: Segmentation, security groups, NACLs, traffic monitoring
- Encryption: Data-at-rest and in-transit, key lifecycle management
- Vulnerability Management: Regular scans, patching, secure images
- Monitoring & Logging: Centralized logs, anomaly detection, alerting
- Incident Response: Playbooks, root cause analysis, recovery testing
- Compliance: Mapping controls to standards (ISO 27001, SOC 2, etc.)

5. Example Cloud Security Reference Diagram

[Diagram placeholder: Insert a network diagram showing users, IAM, firewalls, VPC/subnets, services, storage, monitoring]

6. Continuous Improvement

1. Maintain up-to-date asset and data inventory
2. Regularly review and test incident response plans
3. Conduct security assessments (automated and manual)
4. Provide ongoing security training and awareness
5. Monitor threat intelligence and update controls accordingly

7. References

- Cloud Security Alliance (