Cloud Security Plan - Keyword Definitions

Core Cloud Security Terms

- Hybrid Cloud: A computing environment combining both private and public cloud components to optimize performance, cost, and compliance.

- IaaS (Infrastructure as a Service): Cloud service model providing virtualized computing resources over the internet (e.g., servers, storage).

- PaaS (Platform as a Service): Cloud service offering a development platform and tools to build, deploy, and manage applications without managing infrastructure.

Identity & Access Management (IAM)

- MFA (Multi-Factor Authentication): Requires users to verify their identity using multiple methods (e.g., password + mobile code).

- SSO (Single Sign-On): Allows users to log in once to access multiple systems securely.

- RBAC (Role-Based Access Control): Permissions are granted based on a users role, limiting access to only what's necessary.

- JIT Access (Just-In-Time): Grants temporary elevated privileges only when needed, reducing security risks.

Data Protection

- AES-256: Advanced Encryption Standard using 256-bit keys, commonly used for securing sensitive data.

- TLS 1.3: Latest version of Transport Layer Security for encrypted communications.

- HSM (Hardware Security Module): Physical device used to manage digital keys securely.

- Data at Rest: Data stored on disks or databases, requiring encryption and secure storage.

- Data in Transit: Data moving between systems, protected using secure communication protocols.

Cloud Security Plan - Keyword Definitions

Network Security

- VPC (Virtual Private Cloud): Isolated section of a public cloud for private use.

- Zero Trust Architecture: Never trust, always verify security model requiring continuous authentication.

- WAF (Web Application Firewall): Filters and monitors HTTP traffic to protect web applications.

- DDoS Protection: Defense against Distributed Denial-of-Service attacks that flood systems with traffic.

Incident Response

- SOC (Security Operations Center): Team that monitors and responds to security threats 24/7.

- SIEM (Security Information and Event Management): Tool for collecting and analyzing security logs in real-time.

- Containment: The step in incident response where threats are isolated to prevent spread.

- Root Cause Analysis: Investigative process to determine the underlying reason for a security incident.

Compliance & Monitoring

- HIPAA: U.S. law requiring protection of sensitive patient health information.

- Log Retention: Keeping system logs for a minimum period (e.g., 6 years for HIPAA).

- CloudWatch / Azure Monitor: Monitoring tools from AWS and Microsoft Azure used to track performance and detect issues.

- User Behavior Analytics: Identifying abnormal user activities that might indicate security threats.

Security Tools & Controls

- Antimalware: Software designed to detect and remove malicious programs.

Cloud Security Plan - Keyword Definitions

- Vulnerability Scanning: Regular checks for security weaknesses in software and systems.

- Container Security: Protecting containerized apps from threats and misconfigurations.

- Database Activity Monitoring: Logs and analyzes database actions to detect anomalies.

Implementation Strategy

- Phased Rollout: Security plan executed in 4 phases over 12 months setup, implementation, validation, deployment.

- Patch Management: Process of updating software to fix vulnerabilities.

- Disaster Recovery Plan: Strategy to restore systems after a catastrophic event.

- Business Continuity: Ensures operations can continue during/after disruptions.