**Basik Marketing**

**Security Best Practices for Virtual Private Cloud (Amazon VPC) and Network Security SOP**

**Purpose:** Clearly state the purpose of this SOP, which is to establish security best practices for Amazon VPC and network infrastructure to ensure the confidentiality, integrity, and availability of resources.

**Objective:**

To define security best practices for Virtual Private Cloud (Amazon VPC) and other network security considerations, and establish internal processes for securing traffic within VPC. This SOP aims to ensure the confidentiality, integrity, and availability of data and services hosted in the AWS environment.

**Below recommendations were implemented for Security Groups to restrict VPC network traffic:**

**Ingress Traffic from Internet to Amazon VPC:**

Only necessary ports and protocols should be allowed in the security group rules to minimize the attack surface.

Regularly review and update inbound rules to restrict unauthorized access.

Implement source IP restrictions whenever possible, limiting access to trusted networks.

**Security Groups for Intra-VPC Traffic:**

Implement the principle of least privilege to allow only required communication between instances within the VPC.

Group instances based on their functionalities and assign appropriate security groups to each group.

Regularly review and update security group rules to prevent unintended access.

Network Access Control Lists (ACL) for Inbound and Outbound Traffic:

Use Network ACLs to add an additional layer of security to the subnets.

Default Network ACLs should deny all inbound and outbound traffic and then specific rules should be added as per requirements.

Regularly audit the ACL rules and update them as necessary.

**VPN Connection and AWS Direct Connect:**

Establish a VPN connection or AWS Direct Connect for secure communication between on-premises infrastructure and Amazon VPC.

Implement strong authentication methods such as multi-factor authentication (MFA) for VPN users.

Regularly monitor VPN and Direct Connect connections for any suspicious activity.

**AWS Shield for DDoS Protection:**

Enable AWS Shield to protect against Distributed Denial of Service (DDoS) attacks.

Review AWS Shield metrics and logs to detect and mitigate potential DDoS attacks.

**Secure Traffic to EC2 Instances and Services:**

Use AWS Systems Manager Session Manager for secure remote access to EC2 instances.

Implement Secure Sockets Layer (SSL) or Transport Layer Security (TLS) for encrypting data in transit.

Consider using Application Load Balancers with SSL termination for added security.

**Monitoring and Logging:**

Enable AWS CloudTrail to log API calls and detect unauthorized activities.

Use Amazon CloudWatch to monitor network traffic, performance metrics, and security-related events.

Implement a centralized logging solution (e.g., Elastic search, Log stash, Kibana stack) to aggregate and analyze logs.

**Regular Audits and Reviews:**

Conduct periodic security audits to assess the effectiveness of network security measures.

Review security group rules, network ACLs, and VPN/Direct Connect configurations regularly.

Perform security assessments to identify vulnerabilities and implement necessary fixes.

Evidence of Compliance: