Cloud Security Policy for Secure Application

May 03, 2025

1 Introduction

This policy establishes a robust framework to protect the cloud-based application's data, infrastructure, and user interactions. It addresses vulnerabilities identified by IriusRisk, such as injection attacks, unauthorized access due to missing MFA, and insecure session management. The policy aligns with the AWS Well-Architected Framework and industry standards like ISO 27001 and GDPR, ensuring a secure and compliant environment.

2 Access Control

Implement Role-Based Access Control (RBAC) using AWS Identity and Access Management (IAM) to assign permissions based on user roles, minimizing the risk of privilege escalation. Require Multi-Factor Authentication (MFA) for all users, including administrators, to mitigate unauthorized access attempts highlighted by IriusRisk. Utilize IAM Access Analyzer to continuously validate IAM policies, ensuring least privilege principles are enforced. Regularly review and rotate access keys to prevent long-term exposure, addressing the elevation of privilege vulnerability.

3 Encryption

Enforce AES-256 encryption for data at rest across all AWS services, such as RDS databases and EBS volumes, managed through AWS Key Management Service (KMS) with customer-managed keys for enhanced control. Use TLS 1.2 or higher for data in transit, implemented via AWS CloudFront and Elastic Load Balancers, to protect against interception and tampering. Restrict content access by configuring CloudFront with signed URLs and cookies, mitigating risks of unauthorized data access identified in the IriusRisk report.

4 Logging & Monitoring

Enable AWS CloudTrail to log all API calls and configuration changes across the AWS environment, providing a detailed audit trail for forensic analysis. Deploy AWS CloudWatch with custom metrics and alarms to monitor application performance, security incidents, and access patterns in real-time, addressing the monitoring gaps noted by IriusRisk. Integrate CloudWatch Logs with Security Hub to centralize alerts and enable

automated responses to anomalies, ensuring proactive detection of threats like tampering or information disclosure.

5 Incident Response

Develop a comprehensive incident response plan that includes immediate isolation of affected systems using AWS Security Groups and Network ACLs to contain breaches. Notify relevant stakeholders, including security teams and compliance officers, within one hour of detection, followed by a detailed forensic analysis using AWS Security Hub and CloudTrail logs. Address injection attack risks by implementing input validation and sanitization at the application layer, with WAF rules to filter malicious traffic, ensuring rapid recovery and minimal impact.

6 Compliance Measures

Adhere to ISO 27001 standards by implementing risk management processes and regular security assessments. Ensure GDPR compliance by enforcing data protection measures, such as data encryption and user consent mechanisms, particularly for EU-based users. Conduct regular audits using AWS Config to track configuration changes and ensure adherence to security best practices. Address session management vulnerabilities by enforcing secure session timeouts and token validation, with periodic reviews to maintain compliance with evolving regulations.