AWS ML Associate — Section 4.2: Secure ML Solutions

This section covers security best practices for machine learning solutions on AWS, including data encryption, IAM policies, and network isolation.

# Security Best Practices

• Encryption — SSE-S3 or SSE-KMS for data at rest, TLS for data in transit

• IAM — enforce least privilege access policies for SageMaker roles and users

• Networking — use VPC endpoints, PrivateLink, disable public internet access for training and inference jobs

# Additional Considerations

• Enable logging and auditing for compliance

• Rotate KMS keys and monitor encryption policies

• Isolate environments for development, testing, and production

# Exam Tips

• Default = use IAM roles + bucket policies for access control

• Always enable encryption by default

• Isolate workloads inside VPCs for maximum security