# Acme Manufacturing Cloud Migration: Security Best Practices

This document outlines the security measures implemented throughout the Acme Manufacturing cloud migration project. Our approach prioritizes defense in depth, employing multiple layers of security to protect data and systems.

**I. Network Security:**

- **Virtual Private Cloud (VPC):** Our infrastructure is built within a VPC, providing a logically isolated network for enhanced security. This isolates our resources from the public internet and other AWS accounts. The VPC is segmented into public and private subnets, further enhancing security.
- **Internet Gateway (IGW):** Used only for public-facing resources, minimizing the attack surface.
- **NAT Gateway:** Enables private instances to access the internet without directly exposing them to the public internet, further enhancing security.
- **Security Groups:** Every EC2 instance, RDS instance, and other resources are protected by carefully configured security groups. Inbound and outbound rules are strictly limited to only absolutely necessary traffic based on the principle of least privilege. Each group is named clearly to indicate its purpose and is tagged appropriately for easy identification. Security groups are implemented as the first line of defense against unauthorized access.
- **AWS Shield:** We utilize AWS Shield to protect against distributed denial-of-service (DDoS) attacks, a critical measure in mitigating potential outages.
- **VPN:** Secure remote access to our VPC is enabled via a VPN connection, providing an additional layer of security for authorized users.

**II. Data Security:**

- **Data Encryption at Rest and in Transit:** Data encryption is crucial to protecting sensitive information. We employ AWS KMS to manage encryption keys for databases (RDS, DynamoDB), storage (S3, EBS), and other sensitive data. We also ensure that data in transit is encrypted using HTTPS and other appropriate protocols.
- **S3 Bucket Security:** Our S3 buckets have stringent access control lists (ACLs) and bucket policies that limit access only to authorized users and services. Versioning is enabled on S3 to protect against accidental data deletion or modification. Server-side encryption (SSE) is enabled for all data stored in S3.
- **Database Security:** We utilize the RDS and DynamoDB services, which offer built-in security features such as encryption at rest and in transit. Database access is controlled via security groups, IAM roles, and appropriate database user credentials.

- **IAM Roles:** Instead of relying on access keys, IAM roles are used to grant permissions to our EC2 instances and Lambda functions. This promotes least privilege and reduces the risk associated with compromised credentials.

**III. Identity and Access Management (IAM):**

- **Principle of Least Privilege:** All IAM users and roles are granted only the minimum necessary permissions required for their tasks, following the principle of least privilege.
- **Multi-Factor Authentication (MFA):** MFA is enforced for all users accessing the AWS Management Console. This adds a critical layer of security against unauthorized access.
- **Regular IAM Reviews:** Our IAM configurations are regularly reviewed and audited to ensure that permissions remain appropriate and minimize risk.

**IV. Monitoring and Logging:**

- **CloudTrail:** We utilize CloudTrail to maintain a complete audit trail of all API calls and activity within our AWS environment. This allows us to detect and respond to any suspicious or unauthorized activity.
- **GuardDuty:** GuardDuty continuously monitors our AWS environment for malicious activity and provides alerts on potential threats. This proactive security monitoring is critical for early detection of issues.
- **CloudWatch:** We utilize CloudWatch for real-time monitoring of our systems' performance, health, and security. Alarms are configured to notify us of potential problems or security breaches.

**V. Compliance:**

- **Regular Security Audits:** We will conduct regular security assessments and penetration testing to proactively identify and address vulnerabilities. This proactive approach will ensure our systems remain secure and compliant with all applicable regulations.
- **Security Documentation:** This document and all other relevant security documentation will be kept up-to-date, accurately reflecting the security measures implemented. We maintain a formal security policy and actively work to comply with industry best practices.

This document provides a high-level overview. More detailed procedures and configurations are documented separately. The importance of adhering to security best practices and implementing strong controls throughout this project cannot be overstated. Regular reviews and updates to our security posture are crucial.