# AWS Security Checklist Report

## AWS Security Checklist - Amazon SQS

| Item | Description |
|---|---|
| Encrypt data in transit | Encrypting your SQS data in transit helps protect your data from unauthorized interception or disclosure during transmission. |
| Use secure AWS Identity and Access Management (IAM) policies | Using secure IAM policies helps ensure that access to your SQS resources is limited to authorized users and applications. |
| Implement monitoring and logging | Implementing monitoring and logging helps you identify potential security issues or anomalies in your SQS environment. |
| Regularly review and audit security controls | Regularly reviewing and auditing security controls helps ensure that your SQS resources are secure and compliant with your security policies. |
| Implement least privilege access | Implementing least privilege access helps ensure that users and applications have only the minimum privileges necessary to perform their intended actions. |
| Secure your SQS VPC | Securing your SQS Virtual Private Cloud (VPC) helps protect your SQS resources from unauthorized access and network-based attacks. |
| Implement retention policies for your SQS messages | Implementing retention policies helps ensure that your SQS messages are stored securely and in compliance with your security policies. |
| Implement message-level encryption | Implementing message-level encryption helps protect your SQS messages from unauthorized access or disclosure. |
| Implement message filtering and validation | Implementing message filtering and validation helps protect your SQS resources from malicious or invalid messages. |

This report has been generated by awscheck.fyi