**Policy: AWS Cloud Data Encryption**

This document is **a typical policy outline** for the customers for the starting point dealing with AWS Data Encryption for the data at rest and data in transit. Please refer to the

**Objective**: Ensure that data at rest and data in transit within the AWS cloud environment are properly encrypted to protect sensitive information from unauthorized access or interception.

**Scope**: This policy applies to all AWS resources and services that handle sensitive data within the organization's AWS cloud environment.

**Policy Statement**:

* **Data at Rest Encryption:**
* 1.1. All sensitive data stored in AWS services, such as Amazon S3, Amazon RDS, and Amazon EBS, must be encrypted at rest.
* 1.2. Use AWS-managed encryption keys or customer-managed encryption keys (CMKs) to encrypt data at rest.
* 1.3. Configure the appropriate encryption settings for each AWS service based on the sensitivity of the data being stored.
* 1.4. Regularly review and audit encryption settings to ensure compliance with this policy.
* **Data in Transit Encryption:**
* 2.1. All data transmitted between AWS resources and services must be encrypted in transit.
* 2.2. Use Transport Layer Security (TLS) 1.2 or later protocols for encrypting data in transit.
* 2.3. Enable encryption for all AWS service communication protocols, including HTTPS, SSL/TLS, and SSH.
* 2.4. Avoid the use of insecure protocols and deprecated encryption algorithms. 2.5. Regularly review and update encryption protocols and ciphers to align with industry best practices and security standards.
* **Key Management:**
* 3.1. Implement strong access controls and permissions for encryption keys to prevent unauthorized access.
* 3.2. Use AWS Key Management Service (KMS) to manage encryption keys securely.
* 3.3. Rotate encryption keys periodically or in accordance with organizational policies.
* 3.4. Regularly review and audit key management practices to ensure compliance with security requirements.
* **Compliance and Monitoring:**
* 4.1. Regularly monitor and review AWS service logs, CloudTrail logs, and CloudWatch metrics to detect any unauthorized access or security incidents related to data encryption.
* 4.2. Enable AWS CloudTrail to capture API calls related to encryption configuration changes and key management activities.
* 4.3. Implement automated monitoring and alerting for any changes or disruptions to encryption settings or key management.
* 4.4. Conduct periodic audits and vulnerability assessments to ensure compliance with encryption policies and identify any potential security vulnerabilities.
* **Employee Awareness and Training:**
* 5.1. Provide regular training and awareness programs to employees on data encryption best practices, including encryption at rest and in transit.
* 5.2. Ensure employees understand their responsibilities for handling sensitive data and complying with encryption policies.
* 5.3. Regularly update employees on changes to encryption technologies, protocols, and encryption key management practices.

**Enforcement**:

* Non-compliance with this policy may result in disciplinary action, including but not limited to, employment termination, revocation of access privileges, and legal action as deemed appropriate.
* Compliance with this policy will be regularly monitored and reviewed. Any exceptions or violations should be reported to the designated security team for investigation and resolution.

References:

* [AWS Encryption Services](https://aws.amazon.com/encryption/)
* [AWS Key Management Service Developer Guide](https://docs.aws.amazon.com/kms/latest/developerguide/overview.html)
* [AWS CloudTrail Documentation](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html)
* [AWS CloudWatch Documentation](https://docs.aws.amazon.com/cloudwatch/index.html)