**Steps & Procedures for Implementing Data Encryption in AWS**

This document refers to the standard operating procedure for the data encryption along with the references to the AWS reference.

| **Step** | **Procedure** | **AWS Documentation Reference** |
| --- | --- | --- |
| 1 | Identify the data that needs to be encrypted at rest. | - [AWS Security Best Practices](https://aws.amazon.com/security/best-practices/) |
| 2 | Determine the appropriate AWS service(s) to store the data and enable encryption at rest. | - [AWS Key Management Service (KMS) Documentation](https://docs.aws.amazon.com/kms/index.html) |
| 3 | Create or use an existing AWS KMS customer master key (CMK) to encrypt the data. | - [Creating Keys](https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html) - [AWS KMS CMK Concepts](https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html) |
| 4 | Enable encryption at rest for the chosen AWS service(s) using the AWS Management Console, CLI, or API. | - [Amazon S3 Server-Side Encryption](https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html) |
| 5 | Configure the encryption settings for the specific AWS service(s) to use the designated AWS KMS CMK. | - [Amazon EBS Encryption](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSEncryption.html) - [Amazon RDS Encryption](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Overview.Encryption.html) |
| 6 | Verify that the data is being encrypted at rest by checking the service-specific encryption status indicators or metadata. | - [Amazon S3 Server-Side Encryption](https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html) |
| 7 | Implement access controls and permissions to restrict access to the encrypted data only to authorized entities. | - [IAM Policies](https://docs.aws.amazon.com/IAM/latest/UserGuide/access_policies.html) |
| 8 | Regularly rotate and manage the AWS KMS CMKs and encryption keys according to security and compliance requirements. | - [Rotating Keys](https://docs.aws.amazon.com/kms/latest/developerguide/rotate-keys.html) |
| 9 | Monitor encryption compliance and ensure ongoing encryption at rest for all relevant data. | - [AWS CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html) |
| 10 | Enable AWS CloudTrail logging and monitoring to track access to the encrypted data and detect any unauthorized access attempts. | - [AWS CloudTrail](https://docs.aws.amazon.com/awscloudtrail/latest/userguide/cloudtrail-user-guide.html) |
| 11 | Regularly review and audit encryption settings, access controls, and permissions to maintain the security of the encrypted data at rest. | - [AWS Security Best Practices](https://aws.amazon.com/security/best-practices/) |
| 12 | Backup and securely store the encryption keys or enable AWS Key Management Service (KMS) key replication for disaster recovery purposes. | - [Backing Up Keys](https://docs.aws.amazon.com/kms/latest/developerguide/backup-keys.html) |
| 13 | Train and educate personnel on the proper handling of encrypted data, including encryption key management and access controls. | - [AWS Security Training and Certification](https://aws.amazon.com/training/security/) |
| 14 | Periodically review and update encryption policies, procedures, and controls based on changes in security requirements or industry standards. | - [AWS Security Best Practices](https://aws.amazon.com/security/best-practices/) |
| 15 | Conduct vulnerability assessments and penetration testing to identify and address any security vulnerabilities related to encryption at rest. | - [AWS Vulnerability Assessment Documentation](https://aws.amazon.com/security/vulnerability-assessment/) |
| 16 | Implement encryption at rest for any new data storage resources provisioned in the future. | - [Amazon S3 Server-Side Encryption](https://docs.aws.amazon.com/AmazonS3/latest/userguide/serv-side-encryption.html) |
| 17 | Perform regular backups of encrypted data and test the restoration process to ensure data integrity and recoverability. | - [Amazon EBS Snapshots](https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSSnapshots.html) |
| 18 | Stay up to date with AWS encryption-related services and features to leverage the latest advancements in data encryption at rest. | - [AWS Encryption Services](https://aws.amazon.com/encryption/) |
| 19 | Implement multi-factor authentication (MFA) for critical encryption-related actions and key management operations. | - [AWS MFA Documentation](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_mfa.html) |
| 20 | Regularly assess and validate compliance with encryption policies and industry-specific regulations. | - [AWS Compliance Programs](https://aws.amazon.com/compliance/) |

Please refer to the provided AWS documentation links for detailed information and step-by-step instructions on implementing data encryption at rest using AWS native encryption features.