TASK 4 REPORT: IMPLEMENT IAM POLICIES, SECURE STORAGE & DATA ENCRYPTION (AWS)

Student: Harini P
College: Amrita Vishwa Vidyapeetham, Nagercoil Campus
Program: B.Tech CSE (2nd Year)
Internship: Codtech – Cloud Computing

1. IAM POLICIES IMPLEMENTATION
An IAM user named **harini-task4-user** was created using AWS Identity and Access Management (IAM). The following policies were attached:
• AmazonS3FullAccess
• CloudWatchReadOnly (optional)

This ensures secure, permission-based access to AWS services.

2. SECURE CLOUD STORAGE (AWS S3)
A secure S3 bucket named **harini-cloudtech-bucket** was configured with:
• Block Public Access (All options: ON)
• Restricted access using a custom bucket policy

Only the IAM user has access to list, upload, and download objects.

3. DATA ENCRYPTION (S3 DEFAULT ENCRYPTION)
Default server-side encryption was enabled:
• Encryption Type: SSE-S3 (Amazon S3 Managed Keys)
• Bucket Key: Enabled

This ensures all uploaded files are encrypted at rest.

4. RESULT
The cloud environment is now secured using:
• Identity & Access Management
• Secure Private Storage
• Automatic Data Encryption

This meets all requirements of Task 4 successfully.

END OF REPORT