**📌 Cloud Storage Setup Guide**

**🎯 Deliverable:**

✅ A cloud storage **bucket** is created.  
✅ Example files are uploaded.  
✅ Access permissions are configured.

**🛠 Option 1: Setup on AWS S3**

**Step 1: Sign in to AWS S3**

1. Go to the **AWS Management Console**: <https://aws.amazon.com/console/>
2. Click on **"Sign In"** (or create an AWS account if you don’t have one).
3. In the AWS Console, search for **"S3"** and open it.

**Step 2: Create an S3 Bucket**

1. Click **"Create Bucket"**.
2. Enter a **unique bucket name** (e.g.,muskaansbucket).
3. Choose a **region** (select the one closest to your users).
4. **Block Public Access** (default settings; uncheck if you need public access).
5. Click **"Create bucket"**. A screenshot of a computer

   AI-generated content may be incorrect.

**Step 3: Upload Example Files**

1. Open your **S3 bucket**.
2. Click **"Upload"** → **"Add files"**.
3. Select any sample file (e.g., example.txt or image.png).
4. Click **"Upload"**.

**Step 4: Configure Access Permissions**

* **Make File Public (Optional)**:
  1. Click on the uploaded file.
  2. Go to the **Permissions tab**.
  3. Click **"Edit"** → Uncheck **"Block Public Access"** (if needed).
  4. Click **"Save Changes"**.
  5. Copy the **File URL** for sharing.
* A screenshot of a computer

  AI-generated content may be incorrect.
* A screenshot of a computer

  AI-generated content may be incorrect.

**✅ AWS Deliverables Check**

✔ **S3 Bucket Created**  
✔ **Example File Uploaded**  
✔ **Permissions Configured**

**📌 Object Creation & Policy Modification in Cloud Buckets**

**🛠 1. AWS S3: Object Creation & Policy Changes**

**🔹 Step 1: Upload an Object (File) Inside an S3 Bucket**

1. Sign in to **AWS Console** → Open **S3 Service**.
2. Click on the **bucket name** where you want to add objects.
3. Click **"Upload"** → **"Add Files"**.
4. Select a file (e.g., example.txt, image.png).
5. Click **"Upload"** to store the object inside the bucket.

**🔹 Step 2: Modify Bucket Policy (Public Access or Role-Based Access)**

**➡️ Option 1: Making the Bucket Public (If Allowed)**

1. Open your S3 **bucket settings**.
2. Go to **Permissions** → Click **"Bucket Policy"**.
3. Paste the following JSON **bucket policy** to allow public read access:
4. Replace "your-bucket-name" with your actual bucket name.
5. Click **"Save Changes"**.

🚨 **Security Note:** Making a bucket public allows anyone to access the files. Use IAM roles instead if security is a concern. A screenshot of a computer

AI-generated content may be incorrect.

**➡️ Option 2: Granting Specific User Access via IAM Policies**

1. Go to **AWS IAM (Identity & Access Management)**.
2. Click **Policies → Create Policy**.
3. Select **"JSON"** tab and add:

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Click **"Review Policy" → Name your policy** → Click **Create Policy**.

1. Attach this policy to IAM users, groups, or roles.

**✅ AWS Deliverables Check**

✔ **Object (file) uploaded inside the bucket**  
✔ **Bucket policy updated (public access or IAM role assigned)**

A screenshot of a computer

AI-generated content may be incorrect.