# Assignment-5

## Create a public bucket in AWS. Upload a file and give the necessary permission to check the file URL is working or not.

### Part 1: Create a Public Bucket

1. **Sign in to AWS**:
   - Log in to the **AWS Management Console**.
   - Navigate to the **Amazon S3 Console**.
2. **Navigate to Buckets**:
   - From the left-hand menu, select **Buckets**.
3. **Create a Bucket**:
   - Click **Create bucket**.
   - On the **Create bucket** page:
     - **Bucket Name**: Enter a unique name for your bucket (e.g., `snehapublicbucket`).
     - **Region**: Select your preferred AWS Region.
4. **Set Object Ownership**:
   - Under **Object Ownership**, enable **ACLs** to control ownership of uploaded objects.
   - Choose **Bucket owner enforced – ACLs enabled**.
5. **Adjust Public Access Settings**:
   - Uncheck the **Block Public Access settings for this bucket** checkbox.
   - Tick the acknowledgment box confirming your choice.
6. **Create the Bucket**:
   - Click **Create Bucket** to finalize the process.

---

### Part 2: Upload Files and Grant Public Access

1. **Open the Bucket**:
   - After creation, locate your bucket in the list and click its name.
2. **Upload Files**:
   - Within the bucket, click **Upload**.
   - On the upload page, click **Add files** and select the file(s) to upload.
   - Click **Upload** to complete the process.
3. **Set Permissions for Uploaded Files**:
   - Select the uploaded file and navigate to the **Permissions** tab.
   - Under **Access Control List (ACL)**, click **Edit**.
4. **Grant Public Access**:
   - Check the **Read permission** boxes for **Object** and **Object's ACL** under **Everyone (public access)**.
   - Tick the acknowledgment box confirming you understand the changes.
   - Click **Save changes**.
5. **Verify Public Access**:
   - Go to the **Properties** tab of the uploaded file.

  - Copy the **Object URL**.
  - Paste the URL into a web browser.

If permissions are correctly set, the file should be accessible publicly.

---

## Important Notes:

- Failing to edit the permissions under the ACL will result in access denial, even if the bucket is marked as public.
- Ensure the bucket name is unique across AWS.
- Publicly accessible files may expose sensitive data if permissions are not carefully managed.