**OCR + AI Summary Document System** with **Team-Based Access Control**

## **🔁 Project Flow**

### **1. User Authentication**

* Users log in via email/password.
* Roles:
  + **Access Control User**
  + **General User**

### **2. Team Management**

* ✅ **Access Control User can:**
  + Create new teams.
  + Create **general users** and assign them to teams.
  + Add/remove users from teams.
* ❌ **General Users:**
  + Cannot create teams or manage users.
  + Can only **see teams** where they have access (no management rights).

### **3. Folder Management**

* ✅ **Access Control User can:**
  + Create folders inside teams.
  + Assign specific **folder-level access** to users:
    - view
    - upload
    - delete
* ❌ **General Users:**
  + Cannot create or edit folders.
  + Can **only see folders** where they are explicitly granted access.

### **4. User Permissions (Folder Access)**

Access is controlled via a folder\_access table:

ts

CopyEdit

folder\_access {  
 folder\_id,  
 user\_id,  
 access: ['view', 'upload', 'delete']  
}

* **Access Control User**:
  + Can manage folder\_access
  + **Cannot see or open any files or summaries**
* **General User**:
  + Can only view or interact with folders/files they have access to.
  + No edit rights on teams or folders.

### **5. File Upload (Max 1GB)**

* ✅ Only users with upload permission can upload files.
* Files stored in **AWS S3** using **KMS encryption**.
* File size supported up to **1 GB**.
* On upload:
  + OCR is triggered
  + Text is extracted to .md file
  + .md file is stored in S3
  + AI Summary is generated and stored in the DB

### **6. File Viewing Rules**

* ✅ **General Users**:
  + Can view file and summary **only if they have view access**
  + Cannot view other folders/files
* ❌ **Access Control Users**:
  + **Cannot view any file contents or summaries**, even if they created the folder

### **7. File Deletion**

* ✅ Only users with delete access can delete files.
* System ensures only authorized users can delete based on access record.

### **8. Activity Logging**

Each action is recorded:

* team\_created, folder\_created, user\_added, file\_uploaded, file\_viewed, file\_deleted, etc.
* Stored in activity\_log table with:
  + User ID
  + Action
  + Target ID (team/folder/file)
  + Timestamp

### **9. Security Controls**

* 📱 Mobile apps will block screenshots (iOS & Android secure flags)
* 💻 Desktop screenshot prevention (Electron or OS-based) to be explored
* 🔐 Admins or access control users cannot access any file content

### **✅ Summary of Roles & Capabilities**

|  |  |  |
| --- | --- | --- |
| **Feature / Action** | **Access Control User** | **General User** |
| Login | ✅ | ✅ |
| Create Team | ✅ | ❌ |
| Create General Users | ✅ | ❌ |
| Create Folder in Team | ✅ | ❌ |
| Assign Folder Access | ✅ | ❌ |
| View Team/Folders | ✅ (structure only) | ✅ (if permitted) |
| Upload Files | ❌ | ✅ (if permitted) |
| View File Content | ❌ | ✅ (if permitted) |
| Delete Files | ❌ | ✅ (if permitted) |
| Edit or Delete Teams/Folders | ✅ (structure only) | ❌ |