1) Personas

A) Regular Employee (User)

Goal: collaborate with teams safely (rooms, chat, meetings, shared files).
Can see: Dashboard, Rooms, Chat, Calendar, Files, Recent.
Cannot see: Admin page, Security page, any “edit/manage” tools.
Main needs: quick access to rooms, unread messages, upcoming meetings, assigned files with notes.

B) Admin

Goal: manage users, rooms, meetings, and shared files + their importance/notes.
Can see: Everything (including Admin).
Main needs: create rooms, add/remove members, schedule meetings, publish files + tags like (Important/Action Required), write file instructions, manage roles.

C) Security Staff (Security Role)

Goal: control security levels and policies (not scanning random stuff).
Can see: Security page + limited overview pages (optional: Dashboard/Rooms read-only).
Main needs: set classification levels, enforce access rules, audit logs, meeting/file confidentiality levels.

2) Simple use cases (clear + real)

1. **Team Collaboration Room**

- Employee joins a room (Project A)
- Chats with group
- Shares files inside the room **add acces:**
- Starts/joins a meeting from the room

2. **Admin creates a Project Room**

- Admin creates room “Project A”
- Adds members
- Uploads “Plan.pdf” and marks it **Important**
- Adds note: “Read pages 1–3 and confirm by Thursday”

3. **Meeting Scheduling**

- Admin schedules a meeting for a room
- Employees see it in Calendar + Dashboard “Upcoming meetings”
- Employees click meeting → view details (time, location/link, agenda)

4. **Security Classification**

- Security sets room as “Confidential”
- Only allowed members can access files/meeting/chat
- Security can review audit logs (who accessed what, when)