Model RBAC (MVP) – Roluri și permisiuni

1. Context

Aplicația dezvoltată în cadrul lucrării de dizertație este un sistem informatic pentru monitorizarea performanței proiectelor, bazat pe indicatori KPI (CPI, SPI etc.). Sistemul gestionează date operaționale (timp, cost), date de planificare (baseline) și rezultate agregate (KPI snapshot-uri), ceea ce impune un control clar al accesului la funcționalități și date.

Pentru MVP a fost adoptat un model de **Role-Based Access Control (RBAC)**, care permite: - separarea responsabilităților pe roluri, - limitarea accesului conform principiului *least privilege*, - demonstrarea controlului funcționalităților în cadrul aplicației și al lucrării academice.

---

2. Principii de proiectare RBAC (MVP)

1. **Least privilege** – fiecare rol primește doar permisiunile strict necesare.
2. **Separarea clară a responsabilităților** – introducerea datelor de execuție este separată de definirea și calculul KPI.
3. **Control managerial asupra KPI** – recalcularea KPI și gestionarea baseline-ului sunt acțiuni controlate.
4. **Read-only pentru rolurile de vizualizare** – utilizatorii fără responsabilități operaționale nu pot modifica date.

---

3. Roluri definite (MVP)

3.1 ADMIN

• Rol tehnic și administrativ.
• Gestionează utilizatorii și rolurile acestora (minim).
• Are acces complet la funcționalitățile aplicației în MVP.

3.2 PM (Project Manager)

• Creează și gestionează proiecte.
• Definește baseline-ul (planificare timp și cost).
• Definește KPI-urile și inițiază recalcularea acestora.
• Vizualizează și analizează rezultatele proiectelor.

3.3 MEMBER

• Introduce date de execuție (timesheets, cost entries).
• Contribuie la proiecte din punct de vedere operațional.
• Nu poate modifica planificarea sau recalcula KPI.

3.4 VIEWER

• Rol de tip read-only.

• Vizualizează dashboard-uri și KPI snapshot-uri.
• Nu poate introduce sau modifica date.

---

4. Capabilități funcționale (permisiuni)

Cod	Descriere
U-MGMT	Management utilizatori (listare, creare demo, schimbare rol)
P-MGMT	Creare și gestionare proiecte
W-EXEC	Gestionare work items
T-ENTRY	Introducere timesheets
C-ENTRY	Introducere cost entries
B-MGMT	Gestionare baseline (PV)
KPI-DEF	Definire KPI
KPI-CALC	Recalcul KPI și generare snapshot
KPI-VIEW	Vizualizare KPI și dashboard

---

5. Matrice rol → permisiuni (MVP)

Permisiune / Rol	ADMIN	PM	MEMBER	VIEWER
U-MGMT	✔️	✖️	✖️	✖️
P-MGMT	✔️	✔️	✖️	✖️
W-EXEC	✔️	✔️	✖️	✖️
T-ENTRY	✔️	✔️(opțional)	✔️	✖️
C-ENTRY	✔️	✔️(opțional)	✔️	✖️
B-MGMT	✔️	✔️	✖️	✖️
KPI-DEF	✔️	✔️	✖️	✖️
KPI-CALC	✔️	✔️	✖️	✖️
KPI-VIEW	✔️	✔️	✔️(doar proiecte asociate)	✔️(read-only)

---

6. Matrice rol → pagini (UI routes)

Pagină	ADMIN	PM	MEMBER	VIEWER
/login	public	public	public	public
/dashboard	✔	✔	✔ (filtrat)	✔ (read-only)
/projects	✔	✔	✖	✖
/projects/new	✔	✔	✖	✖
/projects/[id]	✔	✔	✔ (limitări)	✔ (read-only)
/projects/[id]/execution	✔	✔ (opțional)	✔	✖
/projects/[id]/baseline	✔	✔	✖	✖
/projects/[id]/kpi	✔	✔	✖	✖
/admin/users	✔	✖	✖	✖

7. Matrice rol → endpoint-uri API

Endpoint	Metodă	ADMIN	PM	MEMBER	VIEWER
/api/projects	GET	✔	✔	✖ / ✔ filtrat	✖ / ✔ agregat
/api/projects	POST	✔	✔	✖	✖
/api/projects/:id	GET	✔	✔	✔ (dacă membru)	✔ (read-only)
/api/projects/:id	PATCH	✔	✔	✖	✖
/api/projects/:id/timesheets	POST	✔	✔ (opțional)	✔	✖
/api/projects/:id/cost-entries	POST	✔	✔ (opțional)	✔	✖
/api/projects/:id/baseline	PUT/PATCH	✔	✔	✖	✖
/api/projects/:id/kpi/definitions	POST	✔	✔	✖	✖
/api/projects/:id/kpi/recalculate	POST	✔	✔	✖	✖
/api/projects/:id/kpi/snapshots	GET	✔	✔	✔ (dacă membru)	✔ (read-only)

Endpoint	Metodă	ADMIN	PM	MEMBER	VIEWER
/api/admin/users	GET/POST/ PATCH	✔️	✖️	✖️	✖️

---

8. Reguli fără ambiguități

- **Recalcularea KPI** este permisă exclusiv rolurilor **ADMIN** și **PM**.
- **Modificarea baseline-ului (PV)** este permisă exclusiv rolurilor **ADMIN** și **PM**.
- **Introducerea datelor de execuție (timp și cost)** este permisă rolului **MEMBER** (și opțional PM/ ADMIN).
- **VIEWER** are acces doar la date agregate și dashboard-uri, fără acces la date brute.

---

9. Concluzie

Modelul RBAC definit pentru MVP este simplu, coerent și suficient pentru a demonstra controlul funcționalităților în aplicație. Acesta asigură separarea responsabilităților, protejarea datelor sensibile și suportă în mod direct cerințele academice și practice ale lucrării de dizertație.