AUDIT-11 — Multi-Tenant-Isolation

Aspekt: Tenant-Isolation zwischen Koordinator-Mandaten **Norm-Basis:** ISO 27001 A.13.1 (Netzwerk-Sicherheit), A.9.4 (Zugriffs-Kontrolle); OWASP ASVS V8 (Authorization); CSA STAR „Multi-Tenancy" **Stand:** 2026-05-18 (Initial-Lauf) **Verantwortlich:** R-TECH + R-COMP **Reife-Stand:** ◐ Im Aufbau — kritischer Befund identifiziert, Fix sprintgeplant

Selbstverpflichtung

Daten eines Koordinators dürfen unter keinen Umständen für einen anderen Koordinator einsehbar oder veränderbar sein. Diese Isolation ist:

1. **Architektonisch** — über Verzeichnis-Trennung pro Koordinator-Tenant
2. **Vertraglich** — über AVV mit jedem Koordinator
3. **Operativ-überprüfbar** — durch dieses Audit, das wir aktiv gegen uns selbst durchführen

Wir verpflichten uns, das Audit **bei jedem MAJOR-Release** (PROC-K2) und mindestens **halbjährlich** zu wiederholen.

Geltungsbereich

- HTTP-Endpoints des Koordinator-Portals (`ce-doc-portal/backend/api.py`)
- Auth-Service (`ce-doc-portal/backend/auth_service.py`)
- Mandanten-DB (`core/skills/cdp/mandanten_db.py`)
- Workspace-Verzeichnis-Layout (`workspaces/`)
- Sub-Verarbeiter-Pfade (Tenant-Trennung im Prompt-Kontext)
- Mail-Bridge-Inbox-Buckets

Bezugsdokumente

- `01_scope.md`
- `02_controls.md`
- `03_evidence.md`
- `04_findings.md`
- `05_review_log.md`