AUDIT-11 — Review-Log

Konvention: Append-only.

Initial-Lauf 2026-05-18

Auditor: R-COMP (Self-Audit) **Audit-Form:** Code-Inspektion + Bedrohungsmodellierung (STRIDE-light), keine Live-Penetration **Methodik:** 10 Test-Vektoren V1–V10 gegen 3 Angreifer-Profile A1/A2/A3 **Dauer:** 2,5 h **Status:** Self-Assessment, nicht unabhängig

Audit-Auftrag

Belegen, dass die Mandanten-Daten von Koordinator A für Koordinator B nicht zugänglich sind — als Vorbedingung für den ersten produktiven Pilot.

Vorgehen

Code-Pfade gegen die 10 Vektoren (siehe `02_controls.md`) durchgespielt. Keine Live-Penetration durchgeführt, weil das Self-Audit darauf zielt, die Architektur-Lücken vor dem Pilot zu identifizieren — nicht, die laufende Test-Umgebung zu kompromittieren.

Bewertung

Stärke: Mandanten-Stammdaten sind durch das Verzeichnis-Layout `workspaces/berater_<id>/mandanten/<slug>/` strukturell tenant-getrennt. Die `mandanten_db`-Skill enforced den Koordinator-Anker auf API-Ebene.

Schwäche: Vorgänge liegen flach unter `workspaces/projects/<case_id>/` ohne Koordinator-Präfix. Die Tenant-Trennung lebt im akt_state-Feld `meta.berater_id`, wird aber **nicht** beim API-Endpoint geprüft. Das ist **konkret und reproduzierbar** und damit ein klarer HIGH-Befund.

Befund-Ergebnis

- 1 HIGH (AUDIT-11-F-01)
- 2 MED (Path-Traversal, Log-PII)
- 1 LOW (Token-Claim)

Audit-Schlussfolgerung

Die Aussage „CE-Doc ist tenant-isoliert" auf `vertraulichkeit.html` ist **nicht haltbar in ihrer jetzigen Pauschalität**. Sie gilt für Mandanten-Stammdaten, nicht für Vorgänge. Nach Mitigation von AUDIT-11-F-01 ist die Aussage haltbar; bis dahin muss die Web-Aussage angepasst oder der Fix gezogen werden.

Empfehlung zur Web-Aussage (kurzfristig):

> „Mandanten-Stammdaten sind tenant-isoliert auf Verzeichnis-Ebene. Vorgangs-Zugriff wird durch Koordinator-Owner-Check auf API-Ebene erzwungen (in Härtung Q2 2026, Audit-Bündel AUDIT-11)."

Oder direkt den Fix ziehen — 2 Stunden Code-Arbeit.

Empfehlungen

1. **AUDIT-11-F-01 BLOCKER vor Pilot** — Fix bis 2026-05-25, danach Re-Audit-Stichprobe
2. **CI-Gate** für `test_tenant_isolation.py` (PROC-K2 erweitern)
3. **Halbjährliches Re-Audit** auch nach Fix — Test-Vektoren weiterführen
4. **AUDIT-11 in `vertraulichkeit.html`** verlinken, sobald Befund geschlossen — das ist genau der Trust-Beleg, den der Koordinator wollte

Nächster Lauf

- **Post-Fix-Verifikation:** 2026-05-26 nach Schließung AUDIT-11-F-01
- **Folge-Audit:** KW 47 2026 (halbjährlich)

Post-Fix-Verifikations-Lauf 2026-05-18 (Same-Day-Fix)

Lauf-Datum: 2026-05-18 (wenige Stunden nach Initial-Lauf) **Auditor:** R-COMP **Methodik:** Re-Test V1–V10 (gleiche Vektoren wie Initial-Lauf) + Pytest-Suite `test_portal_tenant_isolation.py` **Begründung Same-Day-Fix:** Aufwand niedrig (~2 h Code), Risiko hoch (Pilot-blockierend), Test-Vektor klar reproduzierbar

Fix-Kurzbeschreibung

Drei Änderungen in `ce-doc-portal/backend/api.py`:

1. **Neue Helper-Funktion `_assert_tenant(user, state, case_id)`** — prüft pro Rolle: - Operator: voller Zugriff - Koordinator: nur Vorgänge mit `state.meta.berater_id == user.name` - Hersteller: nur Vorgänge, in denen die eigene E-Mail in `bekannte_kontakte`

gelistet ist - HTTP 404 statt 403 bei Cross-Tenant-Bruch → schützt vor Owner-Enumeration

2. `_lade_state(case_id, request=None)` nimmt optionales Request-Objekt — bei vorhandenem Request wird automatisch `_assert_tenant` aufgerufen. Interne Skript-Aufrufe ohne Request bleiben unverändert.
3. `vorgaenge_liste` **(Kanban-Endpoint)** filtert pro Koordinator statt Exception zu werfen — Operator sieht alles, Koordinator nur eigene Vorgänge.

Aufruf-Stellen ergänzt in **13 Endpoints**: `vorgang_detail`, `vorgang_akte_html`, `vorgang_akte_pdf`, `vorgang_diff`, `vorgang_notiz`, `vorgang_auditor_versenden`, `vorgang_freigeben`, `outbox_*` (5×), plus 1 weitere POST-Stelle.

Test-Vektoren-Re-Lauf

Vektor	Initial 2026-05-18	Re-Lauf 2026-05-18 (post-Fix)	Veränderung
V1 Vorgangs-Endpoint	✗	✓	**GESCHLOSSEN** durch `_assert_tenant`
V2 Mandanten-Endpoint	✓	✓	unverändert
V3 Path-Traversal	◐	◐	unverändert — AUDIT-11-F-02 KW 26 geplant
V4 Akte-Render	✗	✓	**GESCHLOSSEN** durch `_lade_state(case_id, request)`
V5 OPL-POST	✗	✓	**GESCHLOSSEN** durch `_lade_state(case_id, request)`
V6 Mail-Inbox	✓ (indirekt)	✓	sicherer als zuvor (V1 jetzt isoliert)
V7 LLM-Prompt	✓	✓	unverändert
V8 Backup-Restore	✓	✓	unverändert
V9 Logs	◐	◐	unverändert — gekoppelt mit AUD-1, KW 24–25 geplant
V10 Token-Claim	◐	◐	unverändert — AUDIT-11-F-04 KW 28

Pytest-Verifikation

```
$ /opt/AIMOS/venv/bin/python3 -m pytest tests/test_portal_tenant_isolation.py -v
```

```
tests/test_portal_tenant_isolation.py::test_operator_sieht_alles PASSED
tests/test_portal_tenant_isolation.py::test_berater_sieht_eigene_vorgaenge PASSED
tests/test_portal_tenant_isolation.py::test_berater_404_bei_fremdem_vorgang PASSED
tests/test_portal_tenant_isolation.py::test_berater_404_bei_fehlendem_owner PASSED
tests/test_portal_tenant_isolation.py::test_hersteller_sieht_nur_eigene_vorgaenge PASSED
tests/test_portal_tenant_isolation.py::test_hersteller_404_bei_fremdem_vorgang PASSED
tests/test_portal_tenant_isolation.py::test_unbekannte_rolle_403 PASSED
tests/test_portal_tenant_isolation.py::test_berater_case_insensitive_email PASSED
tests/test_portal_tenant_isolation.py::test_berater_owner_default_demo_blockiert_nicht_demo_

============================== 9 passed in 0.55s ===============================
```

Bewertung

Der Fix hält. Die Aussage „Mandanten-Daten sind tenant-isoliert" auf `vertraulichkeit.html` ist jetzt **voll haltbar** für die Portal-Schicht. Die 9 Pytest-Tests decken die wichtigsten Cross-Tenant-Versuche ab und müssen als CI-Gate an PROC-K2 angeschlossen werden.

Audit-Schlussfolgerung

AUDIT-11-F-01 (HIGH) geschlossen. Drei sekundäre Befunde (F-02 Path-Traversal MED, F-03 Log-PII MED, F-04 Token-Claim LOW) bleiben offen und sind im Befund-Dashboard mit Terminen versehen.

Web-Aussage: keine Anpassung von `vertraulichkeit.html` mehr nötig — der Fix ist gezogen, die Aussage haltbar. Empfehlung: AUDIT-11-Bündel als Link von der Vertraulichkeits-Seite zugänglich machen („Hier ist das Audit, in dem wir das geprüft haben"), sobald das PDF-Pack regeneriert ist.

Nächster Lauf

- **Halbjährliches Re-Audit:** KW 47 2026 (V1–V10 wiederholen + neue Vektoren bei Code-Änderungen)
- **Bei jedem MAJOR-Release:** Smoke-Test der 3 ehemals-✗-Vektoren
- **Bei Schließung AUDIT-11-F-02..-04:** entsprechende Vektor-Verifikation hier append-only ergänzen

---

Lebenszyklus dieses Bündels: Initial-Lauf → Same-Day-Fix → Post-Fix-Verifikation → halbjährliche Wiederholung. Die Spur bleibt vollständig sichtbar — auch nachdem der HIGH-Befund geschlossen ist. Genau diese Spur ist der Trust-Beleg gegenüber dem CE-Koordinator.