

# AUDIT-11 — Multi-Tenant-Isolation

**Trägerorganisation:** EcoHub München GmbH, Produktlinie CE-Doc / AIMOS **Aktueller Stand:** Initial-Lauf 2026-05-18; HIGH-Befund am Tag des Audits geschlossen; drei sekundäre Befunde mit Schließungs-Terminen **Letzter Lauf:** 2026-05-18 (Initial-Lauf, Same-Day-Post-Fix-Verifikation) **Nächster Lauf:** Halbjährliches Re-Audit, KW 47/2026

## Konvention

Das Audit-Bündel folgt der Sechs-Datei-Konvention nach POL-09 §3. Jeder Audit-Lauf hinterlässt seinen Befund in `04_findings.md` und seinen Bericht in `05_review_log.md` — append-only. Die Schließung eines Befundes wird mit Datum, Commit-Hash und Verifikationsform dokumentiert; geschlossene Befunde verbleiben im Audit-Trail.

## Befund-Status

| ID            | Schwere | Erstmals gemeldet | Status                         | Verifikation                                                                             |
|---------------|---------|-------------------|--------------------------------|------------------------------------------------------------------------------------------|
| AUDIT-11-F-01 | HIGH    | 2026-05-18        | geschlossen<br>2026-05-18      | Pytest<br><code>test_portal_tenant_isolation.py</code><br>9/9 bestanden; Re-Audit-Lauf 2 |
| AUDIT-11-F-02 | MED     | 2026-05-18        | offen,<br>Termin<br>2026-06-30 | Schließung im Sprint KW 26 vorgesehen                                                    |
| AUDIT-11-F-03 | MED     | 2026-05-18        | offen,<br>Termin<br>2026-06-30 | gekoppelt mit AUD-1 (Log-PII), Sprint KW 24-25                                           |
| AUDIT-11-F-04 | LOW     | 2026-05-18        | offen,<br>Termin KW<br>28/2026 | nächster Audit-Zyklus                                                                    |

## Datei-Inhalt

| Datei                     | Inhalt                               | ca. Lesezeit |
|---------------------------|--------------------------------------|--------------|
| <code>00_policy.md</code> | Selbstverpflichtung zum Audit-Aspekt | 1 min        |

| Datei            | Inhalt                                                       | ca. Lesezeit |
|------------------|--------------------------------------------------------------|--------------|
| 01_scope.md      | Bedrohungs-Modell und zehn Test-Vektoren V1-V10              | 3 min        |
| 02_controls.md   | Code-Inspektion mit Stellen-Verweisen, Mitigations-Skizze    | 8 min        |
| 03_evidence.md   | Code-Belege, Verzeichnis-Belege, Reproduktions-Szenario      | 4 min        |
| 04_findings.md   | Ein HIGH-, zwei MED- und ein LOW-Befund mit Schließungs-Pfad | 4 min        |
| 05_review_log.md | Audit-Bericht (append-only)                                  | 5 min        |

## Lebenszyklus dieses Audit-Bündels

| Datum         | Vorgang                                                                                                                                            |
|---------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| 2026-05-18    | Initial-Self-Audit (R-COMP); HIGH-Befund AUDIT-11-F-01 sowie drei sekundäre Befunde dokumentiert                                                   |
| 2026-05-18    | Same-Day-Fix (R-TECH): <code>_assert_tenant</code> -Helper, Erweiterung in <code>_lade_state</code> , Listen-Filter; 13 HTTP-Endpoints; Pytest 9/9 |
| 2026-05-18    | Post-Fix-Verifikations-Lauf 2 (R-COMP); V1/V4/V5 von ✗ auf ✓; AUDIT-11-F-01 geschlossen                                                            |
| KW 24–25/2026 | Geplante Schließung AUDIT-11-F-03 (Log-PII, gekoppelt mit AUD-1)                                                                                   |
| KW 26/2026    | Geplante Schließung AUDIT-11-F-02 (case_id-Regex-Validator)                                                                                        |
| KW 28/2026    | Geplante Schließung AUDIT-11-F-04 (Session-Token-Claim)                                                                                            |
| KW 47/2026    | Halbjährliches Re-Audit; vollständige V1-V10-Wiederholung                                                                                          |