

POL-09 — Audit-Programm-Policy

Policy-ID: POL-09 **Norm-Basis:** ISO 9001:2015 §9.2 + ISO 19011 + ISO 42001 §9.2

Stand: 2026-05-17 **Verantwortlich:** R-COMP **Review-Zyklus:** jährlich

1. Grundsatz

Die EcoHub München GmbH verpflichtet sich zu einem strukturierten internen Audit-Programm, das die Wirksamkeit ihres Qualitäts-, KI- und Informationssicherheits-Managements regelmäßig überprüft. Audits werden unabhängig, fakten-basiert und nach dokumentierter Methodik durchgeführt.

2. Geltungsbereich

Das Audit-Programm deckt **dreizehn Audit-Aspekte** ab (siehe `audits/`):

- AUDIT-01 DSGVO TOM
- AUDIT-02 OWASP ASVS Level 2
- AUDIT-03a ISO/IEC 42001
- AUDIT-03b NIST AI RMF
- AUDIT-04 ISO/IEC 25010 Software-Qualität
- AUDIT-05 Verfügbarkeit & Incident-Response
- AUDIT-06 Cross-Provider-Privacy
- AUDIT-07 Penetration-Test-Self-Assessment
- AUDIT-08 DPIA (ab 2026-05-18 Anbieter-DPIA + Koordinator-Vorlage)
- AUDIT-09 ISO 9001 (ab 2026-05-17)
- AUDIT-10 ISO 14001 (ab 2026-05-17, leichtgewichtig)
- AUDIT-11 Multi-Tenant-Isolation (ab 2026-05-18)
- AUDIT-12 Forensische Reproduzierbarkeit (ab 2026-05-18)

3. Audit-Methodik

Jeder Audit-Lauf folgt der Sechs-Datei-Konvention im jeweiligen Bündel-Ordner:

- **00_policy.md** — Selbstverpflichtung zum Aspekt
- **01_scope.md** — Geltungsbereich
- **02_controls.md** — Norm-Anforderungen + implementierte Kontrollen
- **03_evidence.md** — Belege für Kontrollen
- **04_findings.md** — Offene Befunde mit Mitigations-Roadmap

- **05_review_log.md** — Audit-Historie (append-only)

4. Audit-Zyklen

Aspekt	Frequenz	Modus
AUDIT-01, -02, -03a, -03b, -09	jährlich	intern, R-AUD
AUDIT-04	halbjährlich	intern, R-AUD
AUDIT-05	vierteljährlich mit DR-Drill	intern, R-AUD
AUDIT-06	quartalsweise + bei Provider-Wechsel	intern, R-COMP
AUDIT-07	halbjährlich intern + jährlich extern	R-EXT-AUD ab Q3 2026
AUDIT-08	pro Pilot-Mandant + jährlich	intern, R-COMP
AUDIT-10	jährlich	intern, leichtgewichtig
AUDIT-11 Multi-Tenant-Isolation	halbjährlich + bei jedem MAJOR-Release	intern, R-COMP + R-TECH
AUDIT-12 Forensische Reproduzierbarkeit	jährlich + bei Lookup-Major-Update	intern, R-TECH

5. Externe Audits

Wir unterscheiden zwei Ausprägungen externer Audit-Substanz:

- **„unabhängig-extern“** im Sinne von ISO 19011 §5 — Auditor steht in keiner persönlichen oder wirtschaftlichen Beziehung zur EcoHub München GmbH oder zu deren Inhabern.
- **„strukturiert-extern, nicht-unabhängig“** — Auditor ist in der Sache fachlich qualifiziert und außerhalb der Trägerorganisation tätig, steht aber in einer persönlichen Beziehung zu Rollen-Inhabern (z. B. Familien-Audit). Wertvoll für Coaching und Methodik-Schulung, aber **nicht** als unabhängige Bestätigung verwertbar.

Ziel: **Mindestens ein unabhängig-externer Audit-Lauf pro Jahr** plus optional weitere strukturiert-externe Läufe.

Jahr	Unabhängig-extern	Strukturiert-extern, nicht-unabhängig
2026	AUDIT-07 Pentest (Q3)	AUDIT-09 ISO 9001 Coaching-Audit durch R. Fuchsenberger sen. (KW 21–23)
2027	AUDIT-07 Pentest + AUDIT-03a ISO 42001	nach Verfügbarkeit

Jahr	Unabhängig-extern	Strukturiert-extern, nicht-unabhängig
2028	AUDIT-07 Pentest + AUDIT-02 OWASP	nach Verfügbarkeit

KPI-Konsequenz: Die in PROC-K4 geführte KPI „Externe Audit-Quote ≥ 2 / Jahr" wird ab 2026 in zwei separate KPIs gesplittet: - „unabhängig-externe Audits / Jahr" — Soll ≥ 1 - „strukturiert-externe Audits / Jahr" — Soll ≥ 1

Für 2026 wird zusätzlich geprüft, ob AUDIT-01 DSGVO-Stichprobe (~3.000 €) als zweiter unabhängig-externer Lauf vorgezogen wird, um den 2026er Stand auf ≥ 2 unabhängig-extern zu heben. Entscheidung im Quartals-Review 2026-08-17.

6. Auditor-Unabhängigkeit

In einer Zwei-Personen-GmbH ist vollständige interne Auditor-Unabhängigkeit nicht herstellbar. Wir adressieren das durch:

1. **Externe Audits** für mindestens 2 Aspekte jährlich
2. **CI-Tests** als unbestechlicher dritter Akteur für Code-bezogene Audits
3. **Explizite Kennzeichnung** interner Audits als „Self-Assessment", nicht als unabhängige Bewertung
4. **Familien-Audit-Beziehungen** (z. B. Vater als Auditor) werden in der Audit-Doku transparent gemacht und nicht als „unabhängig" deklariert

7. Befund-Management

Befunde werden klassifiziert:

Schwere	Definition	Termin
HIGH	Verletzt Norm-Anforderung oder gefährdet Mandanten-Daten	binnen 90 Tagen
MED	Norm-Konformität eingeschränkt, kein akutes Risiko	binnen 180 Tagen
LOW	Verbesserungs-Potenzial, normkonform	nächster Audit-Zyklus

Alle Befunde werden im Befund-Dashboard (`audits/_BEFUND_DASHBOARD.md`) zentral verfolgt. Geschlossene Befunde bleiben im Audit-Trail erhalten (append-only).

8. Audit-Antwort-Pack

Auf Anfrage liefern wir Mandanten / deren Auditoren ein Bundle:

- Interne Audit-Bündel pro Aspekt

- Externer Pentest-Bericht (geschwärzt)
- Befund-Dashboard
- Sub-Verarbeiter-DPAs
- Vertragsvorlagen
- Reifegrad-Belege

9. Verbindlichkeit

Diese Policy ist Teil des Qualitäts-Management-Systems der EcoHub München GmbH. Verletzungen sind im Sinne von ISO 9001 §10.2 als Nichtkonformität zu erfassen und durch entsprechende Korrekturmaßnahmen zu adressieren.