Statement of Work & Angebot

Go-Live Foundation — Security Audit & Production Infrastructure

Dokument-Nr.: `[SOW-NR]` · Stand: `[DATUM]`

AUFTRAGNEHMER

Martin Müller
Freiberuflicher Softwareentwickler
Schweriner Str. 6
19288 Ludwigslust, Deutschland
✉ office@martinmueller.dev
☎ +49 172 3724621

AUFTRAGGEBER

`[KUNDENNAME]`
`[STRASSE HAUSNR]`
`[PLZ ORT]`, `[LAND]`
USt-IdNr.: `[UST-ID / –]`
Ansprechpartner: `[ANSPRECHPARTNER]`
✉ `[EMAIL]`

Projekt:	`[PROJEKTNAME]` — Production Readiness
Zieltermin Go-Live:	`[ZIELDATUM]`
Leistungszeitraum:	`[START]` bis `[ENDE]` (ca. `[DAUER_WOCHEN]` Wochen)
Vertraulichkeit:	Vertraulich — nur zur Angebotserstellung / Projektplanung

1. AUSGANGSLAGE & ZIEL

`[KUNDENNAME]` betreibt eine webbasierte Anwendung (`[KURZBESCHREIBUNG PRODUKT]`). Die Entwicklungsumgebung nutzt `[MANAGED BaaS, z. B. Supabase Cloud]`; für den Produktivbetrieb ist eine selbst verwaltete Infrastruktur bei `[CLOUD-ANBIETER, z. B. Hetzner]` geplant.

Ziele dieses Auftrags:

- Sicherheitsbewertung der Anwendung und Backend-Konfiguration vor Go-Live
- Aufbau einer produktionsreifen Hosting-Umgebung inkl. Auth, Datenbank, Edge/API-Layer, Observability (Grafana LGTM) und AI-Agent-/MCP-Grundsetup
- Migration relevanter Daten und Konfiguration von Dev/Staging nach Production
- CI/CD, Backups, Basis-Härtung (TLS, Firewall) und technische Übergabe

2. LEISTUNGSUMFANG

Der Auftrag gliedert sich in zwei Workstreams. Details können im Kick-off an `[KUNDENSPEZIFIKA]` angepasst werden.

Workstream	Leistungen (In Scope)
WS1 — Security Audit	• Code-Review kritischer Pfade (Auth, API, Admin, Zahlungsflüsse) • Review Backend-as-a-Service: Auth/SSO, Row Level Security (RLS), Storage-Policies

Workstream	Leistungen (In Scope)
	• Prüfung Edge Functions / Serverless-Endpoints (Secrets, Input-Validierung, Fehlerbehandlung) • Review API-Keys, Umgebungsvariablen, Secret-Management • Review Integrationen: `[PAYMENT_PROVIDER]`, `[EMAIL_PROVIDER]` • Risikobewertung mit priorisierten Findings (Critical / High / Medium / Low) und Empfehlungen • Kurzbericht (schriftlich, DE oder EN nach Absprache)
WS2 — Production Environment	• Provisionierung Server/VM(s) bei `[CLOUD-ANBIETER]`, Docker-Setup • Self-Hosted Backend-Stack (`[z. B. Supabase Docker]`): Postgres, Auth, API-Gateway, Studio (admin-only) • Migration Schema + relevante Daten von `[QUELLE]` nach Production • Auth/OAuth-Konfiguration für Production-Domains • TLS (Let's Encrypt), Firewall-Grundkonfiguration, DNS-Einrichtung (`[DOMAIN-MUSTER]`) • CI/CD-Workflows für Static App + Backend-Deploy • Backup-Strategie (DB, Konfiguration) inkl. Restore-Smoke-Test • Smoke Tests zentraler User Journeys (Login, Kernfunktion, `[OPTIONAL: Payment]`) • **Observability (Teil von WS2):** dedizierte Observability-VM, Grafana LGTM (Metrics, Logs, Traces) • OpenTelemetry-Ingest (`otel.[domain]`), TLS, Bearer-Token-Auth • Alloy-/Agent-Deployment auf App- und Backend-VMs (Host-Metriken, Container-Logs, DB-Metriken) • Browser RUM / Frontend-Traces (Production only) und Edge-/API-Function Tracing (OTLP) • Grafana-Dashboards (Data Health, Infra, App, DB, Alerts) via IaC-Provisioning • SSO für Grafana (`[Google OAuth / SSO-PROVIDER]`), Basis-Alerting per E-Mail • **AI Agent & MCP (Teil von WS2):** Grundsetup AI-Coding-Agent (`[z. B. Cursor CLI / OpenClaw]`) • MCP-Server-Konfiguration (DB read-only, Docs, Issue-Tracker, `[WEITERE]`) • Agent-Skills / Projekt-Kontext (AGENTS.md, Tool-Notes, Guardrails), sichere Token-Verwaltung • Headless-/CI-taugliche Ausführung mit dokumentierten Approval-Regeln • Technische Übergabe: Architektur-Skizze, Zugänge, Runbook-Light inkl. Observability- & AI/MCP-Doku • Kurze Team-Einweisung (30–45 Min.) zu Observability & AI-Agent-Setup

3. DELIVERABLES

- Security-Audit-Report (Findings + Empfehlungen)
- Produktionsumgebung unter vereinbarten Hostnames (`app.[domain]`, `api.[domain]`)

- Infrastructure-as-Code / Deploy-Skripte im vereinbarten Repository
- Dokumentation: Architektur-Übersicht, Backup/Restore, Deploy-Ablauf, Observability-Runbook
- Grafana-Instanz unter `grafana.[domain]` mit provisionierten Dashboards
- OTLP-Ingest-Endpoint + Agent-Konfiguration auf Prod-VMs
- AI-Agent-/MCP-Setup-Doku + Beispiel-Konfiguration im Repo
- Abschluss-Call (60–90 Min.) mit Übergabe und Q&A

4. NICHT IM LEISTUNGSUMFANG

- Laufender 24/7-Betrieb / On-Call nach Projektende
- Penetrationstest / formales Compliance-Audit (ISO/SOC) — separat beauftragbar
- Feature-Entwicklung außerhalb Production-Readiness
- Migration historischer Daten > `[DATENVOLUMEN-GRENZE]` ohne Zusatzangebot
- Realtime, File-Storage-Self-Hosting — sofern nicht explizit beauftragt
- Langfristiger 24/7-Alerting-Betrieb / SRE-On-Call nach Projektende
- Custom LLM-Finetuning oder produktive KI-Features in der Enduser-App
- Rechtliche Verträge mit Drittanbietern (`[PAYMENT_PROVIDER]`, Cloud, Domain)

5. ANNAHMEN & VORAUSSETZUNGEN (AUFTRAGGEBER)

- Zugang zu Source Code, Cloud-Konten, DNS, Secrets (read/write nach Bedarf)
- Ansprechpartner mit Entscheidungsbefugnis, Reaktionszeit < `[SLA_STUNDEN]` Werktags
- Freigabe von Domains, OAuth-Apps, Webhook-URLs für Production
- Bestehende Dev/Staging-Umgebung ist funktionsfähig und dokumentiert
- Keine blockierenden Compliance-Freigaben ohne vorherige Abstimmung

6. ZEITPLAN (RICHTWERT)

Phase	Inhalt	Dauer
Kick-off	Scope-Freeze, Zugänge, Architektur-Check	Tag 1
WS1	Security Audit parallel zu WS2-Vorbereitung	Woche 1
WS2	Infra, Migration, CI/CD, Observability, AI/MCP, Übergabe	Woche 1–2
Abnahme	Smoke Tests, Übergabe, offene Findings	Ende Woche 2

7. VERGÜTUNG & ZAHLUNGSBEDINGUNGEN

POSITION	MODELL	NETTO (EUR)
Go-Live Foundation (WS1 + WS2, pauschal) Security Audit, Production inkl. Observability & AI/MCP	Festpreis	`[FESTPREIS_NETTO]`

USt.: 19% (sofern anwendbar) · **Gesamt brutto:** `[BRUTTO]` EUR
Zahlungsoption A: 50% bei Auftragserteilung, 50% nach Abnahme
Zahlungsoption B: 100% vor Projektbeginn
Zahlungsziel: 14 Tage netto · **Währung:** EUR

8. ABNAHME

Abnahme erfolgt nach erfolgreichem Abschluss der Smoke Tests (§2 WS2) und Übergabe der Deliverables (§3). Kritische Security-Findings (Critical/High) werden vor Abnahme behoben oder schriftlich als bewusst akzeptiertes Restrisiko dokumentiert.

9. HAFTUNG & VERTRAULICHKEIT (KURZFASSUNG)

- Haftung auf Vorsatz und grobe Fahrlässigkeit; bei leichter Fahrlässigkeit nur bei Verletzung wesentlicher Vertragspflichten, begrenzt auf typischen vorhersehbaren Schaden
- Beide Parteien behandeln Projektinformationen vertraulich
- IP an Deliverables: Nutzungsrechte an `[KUNDENNAME]` nach vollständiger Zahlung; Open-Source-Komponenten unter jeweiliger Lizenz
- Es gelten die AGB des Auftragnehmers, sofern nicht abweichend vereinbart: `[LINK AGB]`

10. ANNAHME DES ANGEBOTS

Ort, Datum — Auftraggeber `[KUNDENNAME]`	Ort, Datum — Auftragnehmer Martin Müller

Redaction-Hinweis: Template abgeleitet aus Projektstruktur „Security Audit + Production + Observability + AI/MCP“. Platzhalter `[…]` vor Versand ersetzen. Original-PDF nicht automatisch eingelesen — bei Abweichungen zum Kunden-PDF bitte manuell angleichen.