Backlog tasków - K0-CST

1. Zasada zarządzania taskami

Każdy task musi mieć: ID, priorytet, ownera, wynik, kryterium odbioru i ryzyko. Nie publikować modułu jako LIVE bez ownera, źródła, statusu i minimalnej walidacji.

2. Backlog główny

ID	Priorytet	Task	Owner	Output	Uwaga
T-000	P0	Utworzyć branch/repo dla CST	Dev	Repo lub katalog /Common-Source-of-Truth, README, env example, zasady publikacji.	Nie mieszać z /ai-truth.
T-001	P0	Zamrozić stare linki /ai-truth	Dev	Mapa linków i komunikat: wcześniejsze prace pozostają pod swoimi adresami.	Brak utraty SEO i historii.
T-002	P0	Landing /Common-Source-of-Truth/start	Content+Dev	Hero, misja, zasady, 8 wejść, link do dokumentów.	Publikowalne.
T-003	P0	Model danych Claim	Dev+Governance	claim_id, statement, source_id, evidence_id, status, owner, version, timestamp, visibility, appeal_path.	Walidacja JSON.
T-004	P0	Statusy prawdy	Governance	FACT, OFFICIAL, TECHNICAL, GAP, DISPUTED, SIMULATION, DRAFT, ARCHIVED.	Definicje nie mylą faktów z narracją.
T-005	P0	Formularz zgłoszenia incydentu	Dev+Security	Cyber/AI/data/BigTech/vulnerability/PPP/sandbox.	Minimum danych, triage P0/P1/P2.
T-006	P0	Evidence Graph MVP	Dev+Security	Relacje claim-source-evidence-actor-damage-owner-action.	Eksport JSON/CSV/PDF.
T-007	P0	Regulatory Trigger Engine v0.1	Legal+Dev	Macierz triggerów AI Act/NIS2/KSC/RODO/DSA/CRA/eIDAS/odpowiedzialność.	Informacyjne, bez automatycznego orzekania.
T-008	P0	PPP P0 brief	Strategy	Oferta bezpłatnej analizy P0, pilot GO CONTROLLED, produkty P0.	Gotowe do maila.
T-009	P0	Dev/Security Responsible Disclosure	Security+Content	Zasady testowania, zakazy, sandbox, kontakt, skutki braku znajomości obowiązków.	Neutralne i legalne.
T-010	P0	Documents index	Content	PDF/MD, opis, status, data, wersja, hash.	Pobieralny pakiet.
T-011	P1	Legal Live Board	Legal+Dev	Tabela aktów, obowiązków, statusów i terminów.	Ręczna aktualizacja na start.
T-012	P1	Gap & Abuse Register	Governance	Luki, nadużycia, pozorna zgodność, nierówna praktyka organów/dostawców.	Dowód + appeal.
T-013	P1	Human Responsibility Matrix	Ops+Legal	RACI dla ról; owner działania; owner decyzji; owner ryzyka.	Nie przypisuje winy bez dowodu.
T-014	P1	Effectiveness Proof template	Security	Baseline, control, test, evidence, result, residual risk, retest.	Szablon raportu.
T-015	P1	Playbooki 6 podstawowych incydentów	Security	Phishing, ransomware, DDoS, wyciek danych, supply chain, prompt injection.	Każdy ma pierwsze 15 minut.
T-016	P1	BigTech dependency map	Strategy+Dev	Dostawca, usługa, krytyczność, dane, jurysdykcja, ryzyko, alternatywa.	Mapa ryzyk i plan redukcji.
T-017	P1	Open-source / EU tech stack register	DevSecOps	SIEM/SOC, CTI, case mgmt, IAM, docs, repo, monitoring, vector DB.	Kryteria licencji i SBOM.

ID	Priorytet	Task	Owner	Output	Uwaga
T-018	P2	Agent Action Inventory	Agent Ops+Dev	ID, rola, uprawnienia, narzędzia, input/output, log, decyzja człowieka, autonomia, owner, kill switch.	Obowiązkowe przed agentami aktywnymi.
T-019	P2	Dashboard API	Dev	GET status, claims, evidence, incidents, modules; POST report, evidence, dispute, export.	Auth i audit log.
T-020	P2	Sandbox separation	Security+Dev	Osobny namespace danych SIMULATION, brak mieszania z REAL.	Kontrola fałszywych alarmów.

3. RACI skrócone

Rola	Odpowiedzialność
Operator	Decyzja publikacji, zatwierdzenie statusu GO CONTROLLED/GO LIVE, blokada działań ryzykownych.
Dev	Root, routing, API, schema, formularze, dashboardy, eksport, bezpieczeństwo techniczne.
Security	Threat model, responsible disclosure, playbooki, dowody, separacja REAL/SIMULATION.
Legal/Governance	Trigger engine, legal live board, zasady claim-proof, brak przypisywania winy bez dowodu.
Content	Landing, dokumenty, linki, komunikaty, wersjonowanie treści.
Partner/PPP	Brief P0, rozmowy z instytucjami, zakres pilotażu, decyzje finansowania.
Agent Ops	Agent Action Inventory, limity autonomii, scoring, quarantine, kill switch.

4. Krytyczna ścieżka

1. T-000 repo/root.
2. T-001 freeze /ai-truth.
3. T-002 landing.
4. T-003/T-004 model claim i statusy.
5. T-005 formularze.
6. T-006 evidence graph.
7. T-007 trigger engine.
8. T-008/T-009 PPP i dev/security.
9. T-010 documents.
10. Dopiero potem P1/P2.

5. Blokady przed GO LIVE

Blokada	Kiedy blokuje
Brak ownera	Każda akcja operacyjna.
Brak źródła	Każdy claim publiczny jako FACT/OFFICIAL/TECHNICAL.
Brak zgody na test	Każdy test security lub skan aktywny.
Brak separacji SIMULATION/REAL	Każdy dashboard incydentowy.
Brak kill switch dla agentów	Każde działanie aktywne agentów.
Brak legal review	Publikacja o obowiązkach prawnych i odpowiedzialności.
Brak logów	Dowody, statusy, agent actions.