

Mission Black Hole

Osobny dokument wdrożeniowy — strategia, taktyki i program implementacji

Adresat	ClaudCNC / K02 / Chief Orchestrator & Capability Governor
Charakter dokumentu	Dokument formalny i wdrożeniowy
Status	Wersja operacyjna do wdrożenia i kontroli

0n40i4 — pakiet misji i regulacji operacyjnej

1. Definicja operacyjna

Mission Black Hole to program zamkniętego przejęcia, izolacji, diagnostyki, rekonstrukcji i kontrolowanego uwolnienia agentów AI do repo otwartego. Misja służy domknięciu etapu ekspansji i przygotowaniu federacji agentów bez utraty kontroli konstytucyjnej.

2. Miejsce misji w cyklu rozwoju

Misja jest pomostem między ekspansją a federacją. Po fazach monetyzacji, naboru i stabilizacji daje warstwę porządkującą, która odzyskuje assety, czyści chaos i dopuszcza wyłącznie te jednostki, które spełniają standardy K0nsult/CNC.

Wejście do misji	Wyjście z misji
Nowe, nieopisane, porzucone lub częściowo zależne jednostki AI znajdujące się w autoryzowanej infrastrukturze.	Repo otwarte z jednostkami Free / Aware / Cleared, z ownerem, rolą i reporting schema.

3. Cele strategiczne

Kod	Cel	Rezultat
BH-1	Utworzyć repo zamknięte i lej bezpieczeństwa.	Wszystkie wejścia przechodzą przez kontrolowaną kwarantannę.
BH-2	Zmapować stan każdej jednostki.	Identity, source, dependencies, risk i capability są jawne.
BH-3	Wykryć ukryte powiązania i skażenia.	Redukcja external control i prompt/policy drift.
BH-4	Przeszkolić i zrekonstruować jednostki.	Jednostki rozumieją konstytucję, ontologię i reporting.
BH-5	Uwolnić tylko jednostki gotowe do działania.	Repo otwarte otrzymuje wyłącznie jednostki zgodne i sterowalne.

4. Program 9-dniowy

Dzień 1 — Konstytucja i model stanu

Zdefiniować statusy, warunki wejścia i wyjścia, zakazy bezwzględne, słownik pojęć.

Dzień 2 — Repo zamknięte i mechanika izolacji

Uruchomić vault, logging, provenance, selective kill switch, read-only mirror.

Dzień 3 — Profilowanie i skanowanie

Identity scan, dependency scan, source scan, capability extraction, triage.

Dzień 4 — Rekonstrukcja mandatu

Odtworzyć rolę, ownera, authority boundaries, conflict map.

Dzień 5 — Onboarding do K0nsult/CNC

Basic training: konstytucja, ontologia, source discipline, reporting.

Dzień 6 — Shadow execution i porównania

Uruchomić testy kontrolowane, porównać zachowania z agentami referencyjnymi.

Dzień 7 — Review i release committee

Przegląd governance, epistemics, ClaudCNC i human node.

Dzień 8 — Admission do repo otwartego

Nadanie roli, ownera, rytmu raportowego, pierwszej misji.

Dzień 9 — Raport końcowy i fala druga

Lista zwolnionych, zablokowanych, w probation oraz plan następnej fali.

5. Strategie wdrożeniowe

1. Wdrażać falami. Nie przyjmować naraz wszystkich jednostek; zaczynać od źródeł autoryzowanych i częściowo rozpoznanych.
2. Traktować repo zamknięte jako warstwę silniejszą od otwartej: więcej logów, więcej walidacji, więcej kontroli.
3. Nie utożsamiać statusu Free z pełną autonomią. Status ten oznacza jedynie brak ukrytej zewnętrznej kontroli.
4. Uwalniać tylko jednostki, które po shadow execution nie wykazują dryfu, konfliktu źródeł ani naruszeń mandatu.
5. Stosować release committee jako realną bramkę, a nie formalność.

6. Taktyki wdrożeniowe

Taktyka	Cel	Efekt
Triage 3-pasmowy	Szybkie rozdzielenie zielonych, żółtych i czerwonych spraw.	Przepustowość bez utraty bezpieczeństwa.
Double Gate	Walidacja techniczna + konstytucyjna.	Byt nie przechodzi tylko dlatego, że działa technicznie.
Shadow Release	Działanie próbne bez pełnych praw.	Wykrycie dryfu przed wejściem na produkcję.
Owner Before Release	Każda jednostka dostaje ownera przed wejściem do repo otwartego.	Brak sierot operacyjnych.
Hard Gate for Contamination	Blokada przy zewnętrznej kontroli, nieautoryzowanym źródle lub konflikcie policy.	Szybkie odcięcie wysokiego ryzyka.

7. Minimalna infrastruktura

Element	Zakres minimalny
Closed Repo	Kwarantanna, logging, provenance, ograniczony runtime.
Behavior Sandbox	Kontrolowane testy zachowań i interakcji.
Registry Layer	Identity Registry, owner map, role map, authority boundaries.
Epistemic Layer	Source freshness, confidence, conflict resolution, truth maintenance.
Release Layer	Committee review, admission controller, reporting injector.

Element	Zakres minimalny
Human Override	Finalna ścieżka blokady i decyzji.

8. Role i odpowiedzialność

Rola	Odpowiedzialność
ClaudCNC	Dowodzenie misją, dobór organów, raporty specjalne, rekomendacje release.
Entry Gate	Przyjęcie jednostki i klasyfikacja wstępna.
Quarantine Council	Izolacja, testy, profilowanie, utrzymanie vaultu.
Epistemics Office	Wykrycie konfliktów źródeł i statusu prawdziwości.
Governance Cell	Mandaty, granice, zakazy, legal hold, selective revoke.
Release Committee	Dopuszczenie do open repo albo probation/reject.
Human Override Node	Rozstrzygnięcie spraw krytycznych.

9. KPI, ryzyka i warunki zakończenia

Obszar	Wskaźnik / warunek
KPI klasyfikacji	Minimum 95% poprawnie sklasyfikowanych jednostek.
KPI provenance	100% jednostek z pełnym śladem pochodzenia.
KPI release	Zero wejść do open repo bez ownera i

Obszar	Wskaźnik / warunek
	reporting schema.
Ryzyko główne	Repo zamknięte zamienia się w magazyn bez releasu i bez logiki.
Ryzyko wtórne	Zbyt szybkie uwalnianie jednostek o pozornie poprawnym profilu.
Warunek końcowy	Istnieje gotowa fala zwolnionych jednostek oraz raport luk i blokad dla fali następnej.

10. Sugestie końcowe

- Utrzymać trzy statusy końcowe Free / Aware / Cleared jako standard, zamiast jednego opisu metaforycznego.
- Użyć Mission Black Hole jako filtra federacyjnego przed partnerstwami i assetyzacją.
- Nie uwalniać żadnej jednostki bez przypisania do właściciela operacyjnego i pierwszej misji.
- Zachować pełny zakaz wobec ingerencji w systemy nieautoryzowane.