

Want an AI challenger? Add only the capabilities your work can prove.

Optional for advanced volunteers. The beginner rollout has ended.

SAME PROJECT · RIGHT CAPABILITY · EVIDENCE WINS

The CLI is a cockpit - not a second system.

Desktop apps remain the company default.



Stay only if you want command-line control and can keep the approved project visible.

Same AGENTS.md. Same cursor. Same permissions. Same proof.

Install only what your role needs.

CODEX CLI

primary build + verify

CLAUDE CODE

independent challenge

GIT

checkpoint + diff

GH

optional GitHub
commands

PUBLIC RELEASE IS THE STANDARD SOURCE

Use v1.5.1 for the core, company kit and approved skills. Fetch/Pull syncs a checkout; lifecycle updates each installed worker.

Installed is not the same as ready.

APP / CONNECTOR

approved account +
data

SKILL

reusable judgment +
workflow

MCP TOOL

live action surface

CLI

command-line cockpit

**CONNECTED ≠ CONFIGURED ≠ AUTHORIZED ≠
PROVEN**

Add a layer only when the role has a real use case, the account is approved and a DONE WHEN proof exists.

Small, approved and provable.

PUBLIC KIT

v1.5.1 · hash checked

WORK PROJECT

separate live state

ASK MODE

@Computer /
@Chrome · task-
scoped

ONE PROOF

role use case passes

**START WITH PUBLIC v1.5.1 · MOVE TO THE NAMED
PRIVATE OR LOCAL WORK PROJECT**

The public repository holds clean system files only. Company work and secrets never go there.

Add only the lane that serves your work.

OPS + DOCUMENTS

Drive · Gmail · Docs ·
Sheets · Slides

SALES + MARKETING

Akshar · Rahul ·
explicit role opt-in

WEB + SHOPIFY

GitHub · Vercel ·
Shopify · browser QA

FMS + DATA

Sheets · Excel · Drive ·
exact scope

ROLE NEED → EXPLICIT OPT-IN → TEST → KEEP OR REMOVE

Web may add Playwright, Next.js or Cloudflare. Sentry is useful only after a live app is actually instrumented.

Configure per repository or live system.

CLAUDE CODE

independent plan-
mode challenge

GITLEAKS + LEFTHOOK

secrets + pre-commit
checks

MISE

project runtime pinning

SENTRY

only instrumented
production

**GH IS OPTIONAL · AUTHENTICATE, CONFIGURE AND
PIN ONLY WHEN NEEDED**

Tools installed on this Mac still need repo config, account auth or production setup before they can prove anything.

Check first. Install only if the command is missing.

CODEX CLI

Open Terminal. First run: `codex --version`

```
curl -fsSL https://chatgpt.com/codex/install.sh | sh
```

CLAUDE CODE

First run: `claude --version`

```
curl -fsSL https://claude.ai/install.sh | bash
```

Use the official native installers only after Setup Helper or IT confirms the command is missing.

```
git --version · gh --version
```



Done when `codex --version` and `claude --version` return a version.

Sign in only with approved company accounts. Never paste passwords or one-time codes into a prompt.

Check first. Install only if the command is missing.

CODEX CLI

First run: `codex --version`

```
powershell -ExecutionPolicy Bypass -c "irm  
https://chatgpt.com/codex/install.ps1 | iex"
```

CLAUDE CODE

First run: `claude --version`

```
irm https://claude.ai/install.ps1 | iex
```

Git for Windows is recommended for Claude Code. GitHub Desktop remains allowed.

```
git --version · gh --version
```



Done when `codex --version` and `claude --version` return a version.

Do not approve an Administrator prompt unless Ambuj or IT has named the exact reason.

Get the system, then open the work.

1

Check the tagged v1.5.1 release.

kairali-digital/ai-human-workspace · public · clean distribution

2

Update the installed worker separately.

Fetch/Pull changes a checkout only. After approval and a safe checkpoint, lifecycle updates core, kit and approved skills separately.



Done when v1.5.1, receipt and correct work path all pass.

Git sync is not lifecycle install/update.

Run the ruled task in Codex.

1

Start inside the approved project.

Type `codex`. Sign in with the approved company ChatGPT account.

2

Read the operating state first.

Confirm the one live task, scope, permissions and named validator.

3

Work one ruled batch. Review before ship.

Use `/review`. Inspect the diff, evidence and undo before calling it done.

Read `AGENTS.md` and `MASTER_CURSOR.md`. Tell me the one live task, or say NOT SET. Change nothing.

Codex executes only inside the approved task. New authority returns to the human.

Launch Claude as the challenger.

1

Stay in the same approved project.

Open a second shell in the same repository. Existing approved Claude Code access only.

2

Start highest review effort in plan mode.

Plan mode blocks source edits. Approve only read-only exploration checks.

3

Paste the challenge prompt + your use case.

No approved Claude access? Observe the facilitator. Do not purchase during the clinic.

```
claude --model opus --effort max --permission-mode plan
```

Plan mode must remain visible. Never use --dangerously-skip-permissions.

Build → challenge → evidence → ruling.

Primary model builds. Second model challenges.



THE SECOND MODEL CHALLENGES · IT DOES NOT AUTHORIZE

A second model can expose blind spots. It does not eliminate bias or override a validator.

Tell the reviewer exactly what to attack.



Intent + boundaries

User, desired result, exact files and prohibited actions.



Actual evidence

Inspect outputs and tests - not the author's summary.



Failure modes

Facts, numbers, edge cases, bias, drift, security, permissions and proof.

If evidence is missing, say UNKNOWN. Never invent.

Force a useful, auditable answer.

VERDICT

PASS or BLOCK

BLOCKERS

exact references

BIAS

blind spots

NEXT

one safe action

RETURN EXACTLY · NOT A CHATTERING ESSAY

Also require non-blocking observations and an evidence list. A preference is not a blocker.

Add only the checks this job needs.

PPT / PDF

flow · notes · handouts

WEBSITE

mobile · forms · a11y

DATA + FMS

formulas · scope ·
timeout

SHOPIFY + CAMPAIGN

claims · publish ·
spend

**REPLACE [YOUR USE CASE] · KEEP THE CORE
PROMPT**

Presentation: link and overflow. Website: live-change boundary. Data/FMS: no writes and batch cap. Shopify/campaign: no publish or spend.

Buyer insight → ethical message → ship gate.

UNDERSTAND

MoA · NDFF · buyer
evidence

CREATE

MCB · ARC · KIT ·
journey

REVIEW

claims · value ·
sequence

BLOCK

hype · Gate 0 · missing
proof

**MCB = MASS CONTROL BAIT · ‘BED’ WAS A
TRANSCRIPTION ERROR**

Use “What would Akshar say?” as a review lens—not an author voice, copied course or release approval.

Observe → map → pilot → review.

MAP

NBD · CRR · stages

SEPARATE

selling · operations ·
handoffs

MEASURE

evidence · formulas ·
unknowns

PRACTISE

SPIN · calls · roleplay

**NO INVENTED TARGETS, RATIOS, STAFFING,
CONVERSION OR UPLIFT**

Deep division of labour is a diagnostic principle. Reorganisation, policy, access and spend stay with the owner.

One release. Two explicit opt-ins.

1

Verify the signed component catalog.

`ai_human.py components --latest`

2

Install only the named role skill.

`Akshar or Rahul · approved runtime · --latest`

3

Open a new session; invoke the exact skill.

Confirm references, evidence block and one safe next action.

Components: `kairali-akshar-marketing-science · kairali-rahul-sales-system`

Upgrade or remove only at a checkpoint. The previous copy is archived; employee work is not managed.

Disagreement is a gate - not a vote.



Ask for exact evidence

File, slide, line, test result and user impact.



Run the owned validator

Inspect the actual artifact and repeat the relevant check.

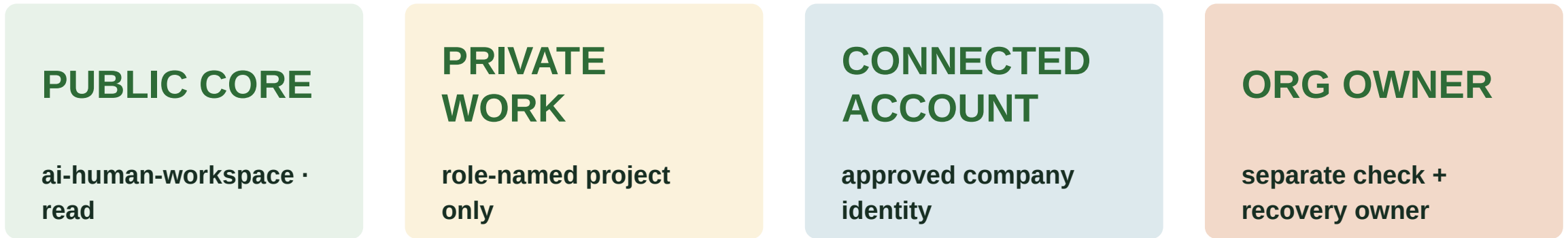


Apply the human rules

AGENTS, locked facts, owner decisions and Gate 0 outrank both models.

Push back on nonsense. Accept a blocker only when its evidence survives the check.

Public distribution. Private work. Minimum access.



PUBLIC REPO = SYSTEM FILES ONLY · NO COMPANY WORK OR SECRETS

Staff need no collaborator seat for the public kit. Private operations access remains least privilege; organization Owner is a separate recovery decision.

Leave only after the challenge loop works.

Project	v1.5.1 + receipt verified; correct work project; AGENTS.md and MASTER_CURSOR.md visible.
Codex	One ruled batch reviewed with diff, evidence and undo.
Claude	Approved seat or facilitator: verdict saved and one cited claim re-run.

DONE MEANS VISIBLE PROOF

REPO v1.5.1 + receipt + path	REVIEW prompt used	VERDICT evidence attached
---------------------------------	-----------------------	------------------------------