

COMPULSORY COMPANY ROLLOUT

One public kit. The right separate worker.

A no-command setup and managed-update guide for Mac and Windows

IRON MAN
MODEL

You are learning to wear Codex like an Iron Man suit. You provide the mission and judgment. Codex performs approved work through a controlled autonomous loop.

THE CHANGE

The latest protected public release is the clean setup and update source. It contains system files, the company reference kit, homework starters and two optional role skills—but no live company work or secrets.

Layer	What it is	Your access
PUBLIC KIT	Clean versioned setup, update and reference files.	No invitation or collaborator seat needed.
WORK PROJECT	Your live role work and state.	Named private project only when assigned, otherwise an approved local worker.
ROLE SKILL	Akshar or Rahul governed workflow.	Only when your role owner explicitly opts you in.

NEVER

Do not save company work, passwords, customer data or secrets in the public distribution repository.

Official release: <https://github.com/kairali-digital/ai-human-workspace/releases/tag/v1.5.1>

FIRST RESCUE

Start the Setup Helper before guessing.

Open a normal ChatGPT chat and paste the complete message

I am stuck setting up my Kairali AI workspace. I do not know Terminal, Python, Git, GitHub, folders, projects or Codex.

Be my Setup Helper.

1. Work out whether I am on Mac or Windows and check what is already installed before changing anything.
2. Do every approved safe setup step you can yourself.
3. If a click, login, account choice or permission must be done by me, show me only that one action in plain Mac or Windows words. Wait for me, then verify it worked.
4. Never ask me to use Terminal, PowerShell, Command Prompt, Python, a CLI or type a command.
5. Never ask for, read or repeat my password or one-time code.
6. Use only my approved company account and company folder.
7. Keep permissions on Ask for approval. Never choose Full access.
8. For the shared Kairali workspace, use GitHub Desktop buttons. For a standalone local project, do not install GitHub unless it is actually needed.
9. Continue until ChatGPT is installed, Codex is open, the correct project is connected, AGENTS.md is visible, approved apps are connected when required, and the startup test passes.
10. If you cannot continue safely, write one OPEN_REGISTER.md row with the failed step, exact error, what you checked, and the one human access or decision needed. Then tell me whether Ambuj or Abilash must help.

Do not teach me how the machinery works unless I ask. Start now by checking what I already have.

DONE WHEN

The helper gives one visible action, waits for you, verifies it, then continues. You never type a command.

SETUP PATH

Check first. Install only what is missing.

The same visible steps work on Mac and Windows

1

Open ChatGPT or chatgpt.com.

Use the approved company account. Type your password or one-time code only into the service login screen.

DONE WHEN: Your approved company account is visible.

2

Let the helper get the latest approved kit.

No invitation is needed. The helper uses the official tagged release and verifies the downloaded kit before opening it.

DONE WHEN: The kit reports the current approved semantic version and contains packages → kairali.

3

Choose the right work project.

Use a named private operations project only if it was assigned to you. Otherwise copy the approved standalone Email, Drive or role worker into your company folder.

DONE WHEN: The selected work folder contains AGENTS.md and MASTER_CURSOR.md.

4

Open that work project in Codex.

Choose the visible Open folder or Add project button. Keep Ask for approval. Never choose your whole computer or Full access.

DONE WHEN: AGENTS.md is visible in Codex.

5

Run the startup test.

Paste the exact sentence below and read the answer before starting work.

DONE WHEN: Codex names one live task or says NOT SET.

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

CHOOSE ONE WORK HOME

Public distribution and live work stay separate.

Your role owner or the Setup Helper confirms which row applies

If this is your work	Use this project	GitHub Desktop?
Named company operations	The exact private repository assigned to your role.	Yes—buttons only. Private invitation may be required.
Email homework	A separate copy of 01-Email-Triage-AI-Human.	No.
Drive homework	A separate copy of 02-Drive-Inventory-AI-Human.	No.
Standalone role or Sheet/local work	A separate approved local worker.	No, unless a future shared-work decision explicitly requires it.

PUBLIC REPO	Read or download the clean system kit. Do not work inside it and do not put employee state into it.
PRIVATE REPO	Access is least privilege and role-named. Being the organization Owner is a separate recovery/administration decision, not an employee default.
LOCAL WORKER	It is still a complete AI-human project. It simply does not need GitHub to operate.

MANAGED UPDATE CHECK

A new release starts with a check, not an overwrite.

Open the existing worker after the company notice

1

Start a new Codex chat in the existing worker.

Do not download a replacement worker and do not copy state into the public repository.

DONE WHEN: AGENTS.md and the existing MASTER_CURSOR.md are visible.

2

Paste the exact read-only check.

The helper may also perform this check automatically at session start when the release is reachable. It must not change files.

DONE WHEN: Installed/latest versions, changes, affected layers and preserved files are reported.

CHECK FOR KAIRALI UPDATE

Read .ai-human/VERSION, .ai-human/system/SESSION-START.md and the installed component receipts for this project. Check only the latest approved semantic-version release from kairali-digital/ai-human-workspace. Do not change any file yet.

Tell me the installed and latest versions; whether the core, reference kit or an already approved role skill is older; the plain-language changes; whether a live task means the update must wait; and exactly which managed files may change and which employee-owned files stay preserved.

If everything is current, show the check proof and stop. If an update is available, wait for me to say UPDATE NOW. Never ask me to use Terminal, PowerShell, Command Prompt, Python, a CLI or type a command.

**GITHUB
DESKTOP**

Fetch origin and Pull origin synchronize only the selected repository. They do not install or update a worker, reference kit or role skill.

APPROVE + PROVE

You approve the apply at a safe checkpoint.

Setup Helper performs the machinery and shows the receipt

3

Defer if a live task exists.

The helper records the available update and leaves every managed file unchanged until the task reaches a real checkpoint.

DONE WHEN: The deferred update row and checkpoint condition are visible.

4

Say UPDATE NOW only at the checkpoint.

The helper backs up and verifies the tagged release before changing a managed copy.

DONE WHEN: No live batch is uncheckpointed and your approval is explicit.

UPDATE NOW

Use the Setup Helper. Confirm there is no uncheckpointed live task. Back up the current managed copy, verify the tagged release and hashes, update only the affected managed core, reference-kit or already-approved-skill layer, validate it, and show me the old version, new version, receipt, preserved-state result and undo. If any check fails, restore the prior managed copy and stop.

5

Update each managed layer separately.

Core, Kairali reference kit and an already approved role skill each keep their own receipt and recovery copy. A copied homework worker is not rewritten by a kit update.

DONE WHEN: Only the named layer changed and validation passed.

6

Keep the proof.

Open .ai-human/VERSION, the receipt and your evidence-log reference. Monitor reads these proofs for the announced batch without rewriting your state.

DONE WHEN: Version, receipt, preserved-state result and recovery location agree.

**ROLLBACK +
REMOVAL**

A failed update restores the prior managed copy. Later rollback uses the named backup. Removal moves the managed copy to a recoverable archive and deletes no employee work.

UNIVERSAL HOMEWORK

Two required. One optional. Prove each status.

Available in the kit is not live for the employee

Worker	Boundary	Proof
EMAIL — REQUIRED	Choose a daily local time. Prove a read-only 25-message pilot; then rule brief-only or reversible safe filing.	Pilot report + active automation; permanent Gmail filters unchanged.
DRIVE — REQUIRED	Use FULL DRIVE INDEX for company completion. Every batch is at most 25; no file contents open.	All supported scopes + CSV + final cursor + validator. TEST 25 is setup only.
LINKEDIN — OPTIONAL	Use task-scoped Computer control in the local worker, then stop before LinkedIn. Manually paste batches ≤25 and manually send.	Local-control proof + handoff + numbered queue + confirmed outcomes.
SEPARATE PROJECTS	Email, Drive and LinkedIn each have their own folder, task state and evidence. Never mix their files.	
EMAIL DAILY	The employee chooses the local run time and confirms the time zone. The automation follows the tested prompt. New permanent filter rules stay in human review.	
LINKEDIN SATURDAY	The employee chooses the local time, confirms the time zone and approves task-scoped Computer control only for the local worker. Computer and Chrome stop before LinkedIn; the employee manually supplies Focused and Other conversations, reviews every draft and manually sends.	
BATCH CAP	Twenty-five remains the hard maximum for each Email, Drive or LinkedIn batch. Longer approved periods continue only after a durable checkpoint.	
GO-LIVE READBACK	Email: LIVE FOR ME or exact blocker. Drive: LIVE FOR ME after FULL DRIVE INDEX, or exact blocker. LinkedIn: OPTIONAL LIVE, NOT ENABLED BY CHOICE, or exact blocker.	

RIGHT-LEVEL ACCESS

Computer handles the local worker. You take over on LinkedIn.

The real permission appears in ChatGPT; the portal cannot grant computer access

1

Close LinkedIn first.

Close every LinkedIn tab and the LinkedIn app. In the local project, choose Computer from the @ tools menu and use the exact request in LINKEDIN-CONTROL-HANDOFF.md.

DONE WHEN: LinkedIn is closed and the real ChatGPT permission prompt is visible.

2

Approve only the current local task.

Approve only the visible local project and task. Keep Ask for approval. Never choose Full access, Always allow, your whole computer or another employee's screen.

DONE WHEN: Codex can name AGENTS.md and LINKEDIN-CONTROL-HANDOFF.md from the local folder.

3

Use Chrome only outside LinkedIn.

Use @Chrome only for a named non-LinkedIn public setup page. Stop browser control when that page is finished.

DONE WHEN: The approved page is closed or left and Chrome control is stopped.

4

Hand control to the employee.

Codex stops every Computer and Chrome tool and shows YOUR TURN ON LINKEDIN. The employee copies no more than 25 conversations, closes LinkedIn, returns to the local project and says BATCH READY.

DONE WHEN: The batch is local, LinkedIn is closed and no AI LinkedIn action occurred.

HARD BOUNDARY

While LinkedIn is visible, Codex never inspects a screenshot or page, moves the mouse, clicks, types, reads, copies, pastes, opens a link or sends. The employee alone performs those actions.

Official Computer Use guide: <https://learn.chatgpt.com/use-cases/use-your-computer-with-codex>

FINAL PROOF

Leave only when the correct project answers.

Show the evidence; do not describe it from memory

- [] The latest approved public-kit version is visible and validation passed.
- [] If an update was announced, its receipt, preserved-state result and recovery location are visible.
- [] The correct separate work project is open; AGENTS.md is visible.
- [] The startup test names the expected live task or says NOT SET.
- [] Permissions remain Ask for approval.
- [] Any required app uses the approved company account.
- [] The Email pilot report, chosen schedule and active automation exist; permanent Gmail filters are unchanged.
- [] FULL DRIVE INDEX finished every supported scope; its CSV, summary, final cursor and validator agree. TEST 25 alone is not completion.
- [] If chosen, task-scoped local Computer control and YOUR TURN ON LINKEDIN handoff are proven; the numbered queue and confirmed outcomes exist; no AI LinkedIn action occurred.
- [] No optional trainer skill was activated without a named role decision.

IF ANY BOX FAILS

Return to the complete Setup Helper prompt. The helper records one precise blocker and names whether Ambuj or Abilash must decide.