

Who has the keys

A people map for the tools behind your live build. Write names and safe account labels. Never write passwords, keys, or recovery codes.



One hook for each person. One clear owner for each tool.

Keep the names. Leave out the secrets.

Your password app holds the secret. This packet tells you who can get in, who can help, and who can take access away.

A name on this paper doesn't grant access. A crossed-out name doesn't remove it. Changes have to happen in the real tool.

Use this when

- Someone joins, leaves, or changes jobs.
- A tool asks for its owner.
- A bill, lockout, or lost phone needs a decision.

01

Owner

Can give and remove access.

02

Worker

Has only the access their job needs.

03

Backup

A named person who can help if the owner is out.

People may have more than one role. Write what each person can actually do.

FIND IT HERE	PAGE
How to write a useful row	2
Calls, customer list, mail, and calendar	3
Site, payments, AI, and core accounts	4
Your team and ED access	5
Keep it current; handle a person leaving	6–7
A lost phone, lockout, or missing roster	8

Private, even without passwords

Keep this with your handoff papers or in a private team folder. Don't post it on the office wall where visitors can read it.

Make every row mean something.

Blank means “not checked.” Write “not used” for a tool you don't have. Don't turn a guess into a name.

What belongs in a row

- 01

The right account

Use a safe account label, such as “company website.” If your team has two accounts in one tool, give each one a row.
- 02

A real person

Write the person who owns access. “IT,” “the office,” and “someone at ED” aren't names.
- 03

A backup and a date

The backup needs their own access where the tool allows it. Write the date you checked the real member list.

Names you can safely write

- Tool name and work account label.
- Owner and backup names.
- Role, such as read only or can publish.
- Password app and item label only.
- Date checked and who checked it.

Never put these here

Passwords. API keys. One-time sign-in codes. Recovery codes. Private sign-in links. A photo of any of those. The Keys, Bills, and Quotas workbook doesn't hold them either.

EXAMPLE ONLY

Tool: Booking app, company account
Owner: Maya Chen
Backup: Lee Ortiz
Access: Maya can add staff; Lee can view bookings
Secret location: Team password app, “Booking account” item
Checked: [date the member list was actually checked]

Our password app name

Person who owns that app

Private place where this roster is kept

Shared login? Flag it, don't hide it.

Use separate sign-ins when the tool supports them. If it doesn't, ask the owner for the approved shared-access plan. Don't change a shared password mid-job by guesswork.



A backup is a person, not a password written on paper.

Calls, customers, mail, and time.

Check the member list in each tool, or ask its owner to check it. List more people on a copy of this page if needed.

TOOL OR ACCOUNT	OWNER NAME	BACKUP NAME	ACCESS / CHECKED
Voice / phone tool			
Customer list / CRM			
Work email			
Calendar / booking			
Call recordings			

Ask about these rights

- Can this person see all customer records?
- Can they hear or download recordings?
- Can they send from the work inbox?
- Can they add staff or change bookings?

Keep the job and the rights matched

A person who answers calls may not need to hear every saved recording. A person who books visits may not need to add new staff.

Don't remove access during live work without a plan. Have the owner make the change, then note what changed below.

ACCESS CHANGE NEEDED	OWNER OF THE CHANGE	FINISHED DATE

A work email can open other doors

If an email account can reset another tool's password, note which tool it can reset. Never copy the reset link. Keep the extra sign-in check on.

Access to one tool may let someone reset another. Keep the owner clear.



The site, money, and core accounts.

Split accounts that do different jobs. A site editor, a payment owner, and a domain owner don't need the same rights.

TOOL OR ACCOUNT	OWNER NAME	BACKUP NAME	ACCESS / CHECKED
Website / web app editor			
Payments / payouts			
AI / agent tools			
Hosting (where the site runs)			
Domain (your web address)			
Password app			

Write the powerful rights down

Can they publish a page? Refund a payment? Change where money goes? Add a new user? Move the web address? Put those rights beside the name.

Use the smallest role that fits the job. The person who reads the bill doesn't always need the right to change the system.

A high-risk right we need to change, and who will change it

Check separately

- Bills and renew dates go in Keys, Bills, and Quotas.
- Names and access go on this board.
- Secrets stay in the approved password app or secure connection.
- Don't paste any real key into either file.

Not sure who owns an account?

Mark it “needs check” and name the person who will find out. Don't open a second paid account to work around the missing owner.

The right to edit a page isn't the right to move your web address.

Your team and ED can have different keys.

Write what your handoff says. Don't assume that every tool has the same owner or the same transfer plan.

Your business accounts

Your domain, payment account, private records, and agreed client-owned services need a named owner at your business.

ED may have a separate staff invite to do the work. An invite is better than handing over your own password.

A service in ED’s work account

Some build or hosting tools may sit in ED’s team account under your agreement. Note that clearly.

Write the agreed way to get a copy or move the build later. Don't assume a staff invite transfers the whole account.

01

Your owner

Approves who has access.

>

02

Named ED contact

Uses only the access agreed for the job.

>

03

Your backup

Knows the handoff and how to get help.

Removing ED access can stop support or live jobs. Agree the change before removing a working connection.

TOOL / ACCOUNT	WHICH TEAM OWNS IT?	ED ACCESS AND PURPOSE	END / REVIEW DATE

Our business owner for access

Our named ED contact

Where the handoff or move plan lives

A useful question for the next handoff

“If our contact is away, who can help us get into this tool, and where is the agreed plan?” Save the answer here. Don't ask for a password in the reply.

Name the person on each side. Keep the agreement easy to find.



Keep the board current.

Check it when people or roles change. Use a short regular review as a backstop, not as a reason to wait when someone leaves.

- 01

Look at the real member list
Compare this page with the tool. Include outside helpers and old invites, not just staff.
- 02

Ask what changed
New person? Different job? Lost phone? Shared login? Write each gap in the action column.
- 03

Close the gap in the tool
The account owner makes the change. Mark it done only after the real access list matches.

A quick review asks

- Are these people still with us?
- Does each role still fit their job?
- Can the owner and backup get help?
- Are there open invites we no longer need?
- Is our private roster copy the current one?

DATE / CHECKER	GAP FOUND	WHO WILL FIX IT / DUE	CHECKED DONE

Our next review date

Person who keeps this board

Don't mark every row “fine” from memory

If the owner couldn't check a tool, leave that row open with a name and a follow-up date. A blank box is more honest than a made-up check.



Someone leaves. Close their doors.

Have the account owner do this at the agreed leaving time. Keep business records. Removing access isn't the same as deleting someone's work.

Person leaving

Access ends: date, time, time zone

- 01

Move the work first

Name the new owner of shared files, inboxes, bookings, and running jobs. Keep the records your business needs.
- 02

Remove access in each real tool

Remove staff invites and team roles. Have the owner end active sign-in sessions where the tool allows it.
- 03

Handle any shared secrets safely

If they knew a shared password or key, ask the owner and ED to replace it safely. A changed key can stop a live job. Never write the old or new key here.
- 04

Check the paths outside the login

Take them off the after-hours list, recovery contacts, shared devices, and private team folders. Check outside helper access too.

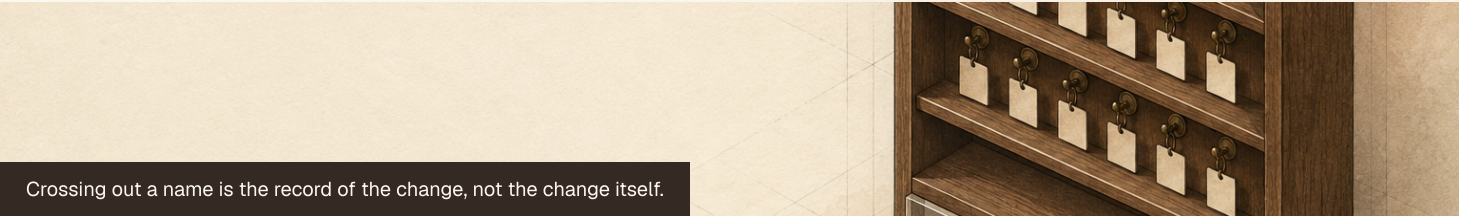
DOOR TO CLOSE	WHO CLOSED IT	TIME / PROOF IN TOOL
Mail, CRM, calendar		
Voice, recordings, after-hours route		
Site, payments, AI tools		
Password app, shared links, devices		

Don't delete by reflex

A former worker's file may hold a live business record. Follow the owner's record-keeping plan. Cross out the name here only after the access change is real.

Done when

Their access is gone, their work has an owner, running jobs still have a safe connection, and calls no longer go to their phone.



If the keys are out of reach.

A lost phone or a locked account is a job for the named owner. Use the approved recovery path, not a shared password in a text.

WHAT HAPPENED	SAFE NEXT STEP	DON'T DO THIS
Owner is away	Ask the named backup. Use their own sign-in.	Pass the owner's sign-in code around.
Phone is lost	Tell the owner. Use the account's approved recovery route.	Turn off the extra sign-in check for everyone.
A secret may have leaked	Tell the owner and ED in the usual private thread. Name the tool only.	Paste the secret again to prove it leaked.
A vendor is the only person listed	Check the handoff and agreed account or move plan.	Assume the account can be transferred with one click.
This roster is lost	Treat names and account labels as private. Tell the owner and replace the copy.	Post a photo online asking who owns it.

First person to contact

Backup person and safe contact route

Where our recovery plan lives (location only, no codes)

What to say

“We can't get into [tool / account label]. The owner is [name]. The problem started [time]. We haven't shared a code or changed the account. Please use our recovery plan.”

Keep the note in the same private thread. The support route and hours stay as agreed in your handoff.

Keep these three records apart

This roster holds names. Keys, Bills, and Quotas holds safe labels and costs. Your password app holds secrets. None belongs on a public wall or a screenshot sent to a group.

