

Security in plain English

Keep control of the tools you already use. Give each person the access their job needs, and know who can help when something changes.

A name for each door.

This guide is for the owner and office lead. It never asks you to write a password.



01 / PEOPLE

Who gets in

Named logins make it clear who has access. A blank list means you still need to check.

02 / POWER

What they can do

Reading a call, changing a rule, and owning the account are different jobs.

03 / HELP

Who can stop harm

Use the support route and pause control agreed at handoff. Don't guess at a switch.

Use the page that fits today.

- Someone joins or changes jobs: pages 2–4.
- You need to share access: page 5.
- Someone leaves: page 6.
- A phone is lost or a secret leaks: page 7.
- Your regular owner check: page 8.

Keep these things off this page.

- Passwords, one-time codes, and private sign-in links.
- Keys that let one app use another.
- Customer recordings and private customer details.
- The recovery codes for your own account.

This isn't a test of the build. Your system is already live. These pages help you handle staff, access, and later changes. They aren't proof of legal compliance or a promise that nothing can go wrong.

Person who keeps the access list

Agreed support route, no private links

Keep one safe way back in.

Before access changes, make sure an authorized owner can still sign in.



Match access to the job.

Start with what the person needs to do. Then choose the smallest set of rights that lets them do it.

READ

See a record

A person may need a caller's name and next step without hearing the full call.

CHANGE

Do the work

A staff member may update an appointment without changing the agent's rules.

OWN

Control the tool

An owner may manage billing, other logins, or the way the system runs.

PERSON / JOB	NEEDS TO DO	DOESN'T NEED
Front desk	Read assigned leads; record a callback	Change who owns the tool
Office lead	Assign work and agreed schedule changes	Share the owner's login
Builder or support	Only the access needed for the agreed work	Keep broad access after the work ends

There isn't one right headcount.

Two people may be enough in one shop. A larger team may need more. The test is whether each named person has a real job to do with that access. Don't cut someone off just to meet a number.

Ask before you grant more.

If the tool can't separate reading from changing, ask the owner or builder for the safest setup. Don't share an owner login as a shortcut. Some tools may charge for extra seats. Get the cost approved.

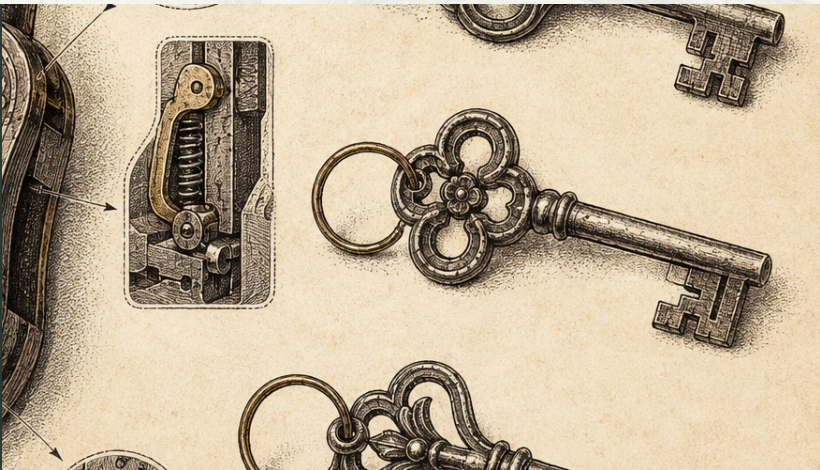
Person and job being added or changed

Access needed / when it should end

Calls contain private details. Give recordings and transcripts only to people who need them for their work. Being on staff doesn't mean everyone needs to hear every caller.

Change the role when the job changes.

A promotion, new shift, or short support visit is a reason to review access, not to hand out every key.



Write what you checked.

Look at the actual user list in each tool, or ask its authorized owner to check it. A blank row never proves that nobody can get in.

Checked You saw the real list and wrote who has access.	Needs checking You don't yet know. Name the person who will check.	Not used Your business doesn't use this tool. Say so clearly.
---	--	---

TOOL / ACCOUNT NAME	OWNER + BACKUP	CHECKED BY / DATE / NEXT STEP
Work email		
Customer list / CRM		
Website or app		
Voice / calendar		
Payments / billing		
AI tools / password app		

This is the short map.
Use Who Has the Keys for the full roster of people. Here, name the exact tool and the owner who can confirm the list. If two accounts have similar names, add a safe label such as “main office.”

Keep the check honest.
Write “needs checking” if you couldn’t see the list. Give it an owner and a due date. Don’t tick “checked” because an old printed page looks right. Don’t remove anyone just to make the sheet tidy.

Only names and safe labels. No password, private account link, card number, or key belongs in these boxes. Keep the paper where only the right staff can read it.

The tool’s list is the proof.
A name crossed off on paper still has access until the change is made in the actual account.



Make sign-in harder to steal.

Use your own login, a password app, and the extra sign-in check the tool offers. Ask for help if those choices aren't clear.

01

Your own login

Don't use another person's name.

>

02

A strong secret

Let a password app make and keep it.

>

03

One more check

Use a passkey or extra sign-in step where offered.

A passkey lets a trusted device prove it's you. An extra sign-in check asks for more than a password.

Don't approve a surprise.

If your phone asks you to approve a sign-in you didn't start, choose no. Don't read a code to someone who called you. Open the tool in your usual way and use the known support route, not the message that scared you.

Keep a safe recovery path.

The owner needs a way back in if a phone is lost. Keep recovery codes in the approved password app or another approved secure place. Never put them in this packet. Ask the owner who can help before you change that setup.

CHECK	YES / NO / UNKNOWN	OWNER / NEXT STEP
Each person has their own login		
The tool's extra sign-in check is on where offered		
An owner has a safe way to recover access		
Shared devices lock when left alone		

One password per tool. Reusing the same password lets one leak reach more than one account. A password app can make separate passwords so you don't have to remember them all.

When in doubt, stop the sign-in.

A real support person doesn't need you to send the code from your phone in a chat.



Invite a person. Don't paste a key.

A key is a secret that can let one app use another. Treat it like a password, even if it looks like a long line of random letters.

Normal staff access

Add the person inside the real tool, using their own login and the role their job needs. Send the tool's normal invitation. Check the address before you send it.

A shared secret is truly needed

Ask the authorized owner or builder to use the approved password-app sharing method for one named person. Use a time limit if the tool supports it. Don't paste the value.

Safe things to put in a help note.

- The tool's name and a safe account label.
- Who needs access and what job they need to do.
- The name of the password-app entry, not its contents.
- Who approved the access and when it should end.

Never put these in a help note.

- The actual password or app key.
- A sign-in code or recovery code.
- A private password-reset link.
- A screenshot that exposes any of those secrets.

01

Ask

Name the person and their job.



02

Approve

The owner checks access and any cost.



03

Invite

Use the real tool or approved safe share.



04

Check

Confirm the right person got the right role.

ACCESS REQUEST

WRITE NAMES OR SAFE LABELS ONLY

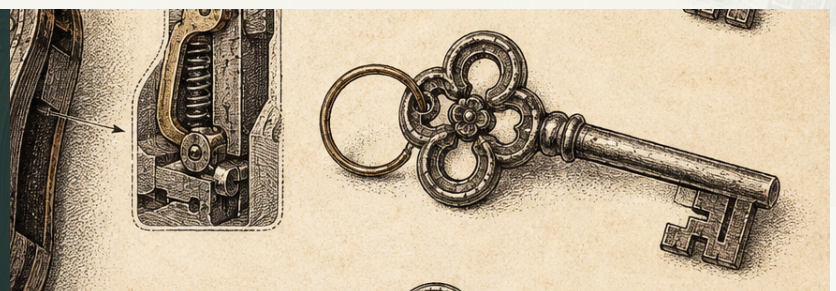
Person / job / tool

Owner who approved / date

Role / end date if temporary

A private link can be a key too.

If a link lets someone sign in or reset a password, don't copy it into this packet.



When someone leaves, close their access.

The owner or authorized admin handles the cutoff at the agreed time. Take access away without losing the business's records or locking out the owner.

Before the cutoff Confirm who can still sign in as owner. Move needed job ownership, mailbox duties, and on-call work to a named person. Keep records the business must keep. Don't delete the account or its data as a shortcut.	At the cutoff Use the tool's proper remove-access or suspend-user control. End their active sessions and remove devices or personal recovery routes where the tool allows it. Ask the builder if you can't do this safely.
---	--

CLOSE EACH PATH	DONE / OWNER / NEXT STEP
Email, customer list, calendar, website and billing	
Recordings, transcripts, shared files and guest links	
Password-app access and saved/shared secrets	
After-hours number, phone device and work ownership	

Saved secrets may still work. Removing someone from a password app doesn't erase a copy they already kept. Ask the owner or builder which shared passwords or keys they could know. Replace or revoke those through the real tool.	Don't break a running connection. A shared app key may power a live form, payment, or agent. Have the builder plan the replacement and confirm the new one works. If harm is happening now, use the agreed incident route right away.
--	---

Person leaving / cutoff date and time

Admin who closed access / proof checked

Done means access is gone in the tool.

Update the paper roster after the real change. Note any open item, its owner, and when it will be finished.



A lost phone or leaked secret needs action.

Don't wait for the monthly check. Use a known phone number or support route. Don't click a strange sign-in link or send the secret to prove it leaked.

STOP

Don't add harm

Don't approve a surprise sign-in, forward the secret, or keep testing a risky action.

REACH

Tell the right person

Contact the account owner and agreed support person. Say what happened and which tool.

CLOSE

Block the old path

The authorized person secures the account or device and confirms the old access no longer works.

WHAT HAPPENED	WHAT THE AUTHORIZED PERSON HANDLES
Lost work phone or laptop	Remove access from that device; end its sessions. Keep a safe owner login.
Password or reset link exposed	Change the password or cancel the link in the real tool; review active sign-ins.
App key exposed	Revoke the exposed key and arrange a safe replacement for any live connection.
Wrong person saw customer data	Limit access, preserve the facts safely, and get the owner's incident help.

If money or data is moving now.

Use only the pause or block control agreed for that system, if you know it. Contact support immediately. Don't wait to fill out this page, and don't switch off unrelated tools.

Keep proof, not more copies.

Write the tool, time, and what you saw. Don't paste the secret into the report. Keep any private evidence only through the restricted route support approves. The owner handles any required notices with qualified help.

Tool / time / what happened, no secrets

Owner reached / action / time checked

Deleting a message doesn't cancel a key.

The old secret must stop working in the real tool. Removing it from chat alone isn't the fix.



Keep the list current.

Pick a regular review date, then review sooner when someone joins, leaves, changes jobs, loses a device, or gets temporary support access.

01

Read the roster
Compare it with today's team and tools.

>

02

Check the tool
Look at actual access, not just paper.

>

03

Close the gap
Name who will fix each real issue.

>

04

Keep the receipt
Write what changed and who checked it.

OWNER CHECK		WHAT TO RECORD
Does everyone still need their role?		Remove unused rights through the authorized owner.
Can former staff or guests still get in?		Check logins, sessions, shared links, and saved secrets.
Can the owner still recover the account?		Check the safe recovery route without copying its codes.
Is a private thing in the wrong place?		Use page 7 if a secret or customer data was exposed.

GAP / TOOL , NO SECRET VALUES	OWNER	DUE / FINISHED / PROOF

Keep the related sheets together.
Who Has the Keys holds the people roster. Keys, Bills, and Quotas holds ownership and spending limits, never actual keys. After-Hours List holds the working contact plan. Update the real tool before calling a change done.

Leave unknowns visible.
If nobody could check a tool, record that and assign it. Don't write "all safe" because the sheet is blank. This is a practical owner routine, not a security certificate.

Review date / person who checked

Next review / open item owner

A small, accurate list beats a full-looking one.

Keep names current, limit who can read the sheet, and use the agreed help route when access is unclear.

