



An Extended Guide · No. 2079

When an Employee Leaves: Shutting Off Access the Same Day

A calm same-day checklist for email,
files, apps, keys, and shared passwords

Tech Made Simple — Service Made Personal

BillsHomeTech.com · (330) 200-8042 · Atwater, Ohio

Free & printable — share it with someone who needs it



Book a visit —
billshometech.com/book

! Read this first — the two things that stop most attacks

Almost every small-business break-in starts in one of two ordinary ways: a password that got stolen or guessed, or a convincing email that talked someone into clicking or paying. You do not have to become a computer expert to stop most of it. Turn on two-step sign-in (also called multi-factor authentication, or MFA) everywhere you can, keep a backup you have actually tested, and give yourself permission to slow down before you click a link, open an attachment, or send a payment. That is the whole game, most days. This guide is about one of those ordinary moments: the day someone leaves. If their access doesn't leave with them, a former login becomes exactly the kind of open door attackers — and the occasional unhappy ex-employee — walk right through.

When someone leaves, their access should leave too

Whether a person quits, retires, or is let go, the safest rule is simple: shut off their access the **same day**. Email, files, apps, remote access, building keys — all of it. This guide gives you a calm, repeatable checklist so no door is left open.

I'm Bill, and I run Bill's Home Tech here in Portage County, Ohio. I've spent 30+ years helping small businesses with their technology, in plain language. Offboarding sounds like a big corporate word, but for a small shop it's really just a tidy to-do list you run each time someone goes.

The goal isn't to treat anyone like a suspect. Most people leave on good terms. It's that access left switched on — even for a trusted former employee — is a risk that sits there quietly, and the day to close it is the day they leave, not 'sometime soon.'

★ I'll build your checklist once, so it's easy forever

I can walk your systems with you once, write down every place a person could have access, and turn it into a one-page same-day checklist you reuse every time. Call or text me at (330) 200-8042.

The same-day checklist

If you do nothing else, do these on the day someone leaves. Work down the list and don't stop halfway.

- ☐ **Disable their email** — block sign-in, then set up forwarding or an auto-reply.
- ☐ **Cut cloud file access** — Microsoft 365, Google Workspace, Dropbox, shared drives.
- ☐ **Shut off every business app** they could log into — accounting, point-of-sale, scheduling, CRM.
- ☐ **Kill remote access** — VPN, remote-desktop, and any remote-support tool.
- ☐ **Change any shared passwords** they knew (and this is why shared logins are a problem — more on that inside).
- ☐ **Remove admin roles and MFA devices** tied to their accounts.
- ☐ **Collect devices** — laptop, phone, keys, fobs — and remove work access from any personal device.
- ☐ **Change building keys, alarm and door codes** they knew.
- ☐ **Transfer ownership** of their mailbox and files before you delete anything.

! Same day — not 'when we get to it'

The gap between someone leaving and their access being cut is pure risk. Most of the time nothing happens; the one time it does, it's expensive. Running this list the same day costs you an hour and closes the window.

Why 'same day' really matters

It's tempting to leave an account on for a few days 'just in case.' Here's why that few days is the dangerous part.

An active login for a person who no longer works for you is a door with no one watching it. Even when someone leaves on perfectly good terms, their password may be reused somewhere that later gets breached, or saved in a browser on a personal device, or simply guessable. The account doesn't know the person quit — it keeps working until you switch it off.

And on the rare occasions a departure isn't friendly, those first hours are exactly when a frustrated former employee might copy files, send an email as the company, or quietly keep a way back in. You don't have to assume the worst about anyone to close the door — you just close it, every time, the same day.

! A former login is an unwatched door

Every account you leave active after someone leaves is a door standing open with nobody minding it. The single most protective habit in offboarding is simply speed — cut access the day they go.

Start with email — it's the master key

Email is usually the first thing to lock down, because it's how most other accounts get reset.

Think about how many services let you reset a password by sending a link to your email. That's why a former employee's live mailbox is so powerful: whoever controls it can quietly reset their way into other accounts. Block sign-in to the mailbox first, before you work through the rest of the list.

Blocking sign-in is different from deleting. You want to stop the person from logging in **right now**, while keeping the mailbox itself intact so you can forward it, set an auto-reply, and hand off anything important. Delete only after you've captured what you need.

- Block or disable sign-in to the account immediately.
- Set a forward to a current employee, or an auto-reply pointing customers to the right person.
- Reset the account password so old saved copies stop working.
- Remove the person's phone or app as an MFA method on the account.

Files: cut access, but transfer ownership first

Here's the step people forget in the rush — and then regret a month later.

When you disable someone's account, the files and emails they owned can get locked away or scheduled for deletion along with it. So before you fully close an account, **transfer ownership** of their documents, shared folders, and mailbox to the owner or whoever takes over their work. Then cut their access.

In Microsoft 365 and Google Workspace there are admin tools to hand a departing person's files and mail to someone else. The exact steps and menu names change over time, so check your current admin center — or let me do the handoff cleanly so nothing gets lost.

✓ Capture, then cut — in that order

The right sequence is: grab what you need (ownership of files and mail), then remove access. Flip that order and you can end up locked out of a customer list or an invoice history you suddenly need.

The apps and back doors beyond email

A person's access usually sprawls further than you'd guess. Walk the whole list, not just the obvious ones.

Business apps

Think through every service the person could sign into: accounting, point-of-sale, scheduling, your website or online store, a CRM, social media, payment processors, shipping accounts. Each one is a separate login to turn off. A written inventory of your apps makes this quick instead of a memory test.

Remote access — the quiet back doors

Remote access is the category most often missed and most dangerous to leave open: VPNs, remote-desktop connections, and remote-support tools that let someone reach your systems from anywhere. Shut these off deliberately. A former employee with working remote access effectively still has a key to the building.

! Remote access left on is the easiest door to forget

Email and files are obvious; a VPN or remote-support tool is easy to overlook because you can't see it from the front counter. Put it high on your checklist so it never slips through.

Don't forget the physical keys and codes

Offboarding isn't only digital. The real-world keys matter just as much as the passwords.

- Collect **building keys, fobs, and badges** on the last day.
- Change any **door codes, alarm codes, or gate codes** the person knew — a returned key doesn't help if the code is still the same.
- Collect company **devices**: laptop, phone, tablet, external drives.
- Retrieve or deactivate **credit cards, fuel cards, and company accounts** in their name.
- Recover anything that lets them act as the business — a company phone number, a signing authority, a vehicle.

✓ Codes are keys too

Physical keys get returned; shared codes get remembered. If a departing person knew the alarm code or the back-door keypad, change it. It takes five minutes and closes a door a returned key wouldn't.

Shared logins are the enemy of a clean exit

If several people share one login, offboarding gets messy fast. Here's why — and the fix.

When your team shares a single login — one 'office' account for the accounting software, one password everyone uses for the point-of-sale — you can't cleanly cut one person off. The moment someone leaves, you have to change that shared password and re-share the new one with everyone who stays. Miss one and the door's still open; the departing person likely still knows the old one.

Individual, named accounts make offboarding simple: you disable one person's account and everyone else carries on untouched. If you take one structural lesson from this guide, let it be this — move away from shared logins. It pays off every single time someone comes or goes.

! Every shared password a leaver knew must be changed

A shared login the departing person used is a password that walked out the door in their head. Change every one of them on their last day — and plan to replace shared logins with individual accounts so you never have to scramble like this again.

Pull back admin roles and sign-in devices

If the person held any special power, that's the first thing to take away — and their phone shouldn't still be a key to your systems.

A departing employee who had administrator rights can do far more damage than one with an everyday account, so remove any admin or elevated roles immediately — in the cloud and on individual computers. Our guide 'Who's the Admin?' explains why keeping admin power separate and scarce makes this step easy.

Also remove the person's phone, app, or security key as an MFA method on any account. Otherwise you can disable a password but leave their device sitting there as a trusted second factor — and on shared or service accounts, that second step might still let them in. For the strongest accounts, hardware keys and passkeys are covered in our passkeys guide.

✓ Admin access comes off first

Order matters when time is short: strip admin rights and MFA devices before the smaller stuff. The powerful access is where a left-open door does the most harm.

Two kinds of departures

The checklist is the same either way, but how you run it depends on whether you saw the departure coming or it happened in an instant.

A planned departure (notice given)

When someone gives notice or retires, you have the luxury of preparing. Use it — a smooth handoff protects both the business and the relationship.

- Prepare the handoff in advance: who takes over their files, mailbox, and duties.
- Transfer ownership of documents and knowledge while the person is still around to help.
- Schedule the access cut-off for their actual last working hour — not days later.
- Do a friendly exit: collect devices and keys, thank them, and part on good terms.

A sudden departure (let go, or walked out)

When a departure is abrupt or tense, speed is everything and the order flips — you cut access first and sort out the handoff afterward.

- Cut access **immediately**, starting with email, remote access, and admin roles — before anything else.
- Change shared passwords and door/alarm codes right away.
- Transfer ownership of their files and mailbox from the admin side once access is cut.
- Collect company devices and remove work access from any personal device — see our guide on personal devices at work.

★ Want a plan ready before you need it?

The best time to build your offboarding checklist is before anyone leaves. Tell me what systems you use and I'll map out every door to close, so a sudden exit is calm instead of frantic. Call (330) 200-8042.

The secret is a map you make ahead of time

You can't shut off access you've forgotten exists. The real work happens before anyone leaves.

Sit down once and write a simple list of every place a person could have access: each email and cloud account, every business app, remote-access tools, building keys and codes, company cards and devices. This is your offboarding map. When someone leaves, you're not trying to remember 73 different logins under pressure — you're just walking a list you already trust.

Keep the map current as you add new tools, and note which accounts are shared (a flag to fix) and who holds admin rights. Ten minutes of upkeep now turns every future departure into a calm half-hour instead of a nagging worry about what you missed.

✓ Build it on a normal day

Make the map when nothing is urgent and nobody's leaving. A list built calmly is far more complete than one scribbled on the day you're also handling a resignation.

Getting your devices and data back

Hardware walks out the door easily. Have a plan for both company devices and personal ones that touched work.

Company-owned devices

Collect every company laptop, phone, tablet, and drive on the last day, and don't wipe them until you've confirmed nothing important lives only on that device. Then reset them properly before they're reused or stored.

Personal devices used for work

If the person used a personal phone or home computer for work email or files, you need the ability to remove just the work access without touching their personal stuff. That's why a little planning around personal devices pays off — our guide on personal devices at work covers setting this up so removal is clean and drama-free.

✓ Know this before you need it

The time to figure out how to pull work access off a personal phone is **before** someone leaves, not during an awkward last-day conversation. Set it up while everyone's happy.

Keep a short record of what you did

A two-minute note protects you if a question ever comes up later.

After you run the checklist, jot down what you did and when: date and time access was cut, which accounts were disabled, which shared passwords and codes were changed, what devices came back, and who the person's files and mailbox were handed to. Nothing fancy — a dated note in the person's file is plenty.

If there's ever a dispute, an insurance question, or simply a 'did we ever turn off their VPN?' six months later, that little record answers it instantly. It also helps you spot any step you skipped while it's still easy to fix.

✓ The checklist is also the record

The simplest system is to print your offboarding checklist, check each box as you go, write the date on top, and file it. The thing you used to do the work becomes the proof you did it.

It's not only employees

Anyone you gave access to should lose it when the relationship ends — not just people on payroll.

Contractors, bookkeepers, a web designer, a former IT helper, a seasonal worker, even a volunteer — if you ever handed them a login, a folder, or remote access, that access needs to come off when they're done. These are the easiest to forget because they were never 'staff,' and they often held fairly powerful access.

Add outside helpers to your offboarding map right alongside employees, and review that list periodically for anyone whose work ended months ago but whose access quietly lingers. Unused access is just risk with no benefit.

! Old vendor access is a classic open door

A login left active for a vendor whose project ended last year is exactly the kind of forgotten door that gets a small business in trouble. If you're not sure who still has access, that uncertainty is the problem to fix.

The mistakes that leave a door open

Nearly every access that lingers too long traces back to one of these. Now you'll catch them.

- **Waiting 'a few days'** to cut access instead of doing it the same day.
- **Deleting the account before transferring files and mail** — and losing data you needed.
- **Forgetting remote access** (VPN, remote-support tools) because you can't see it from the front desk.
- **Not changing shared passwords and door codes** the person knew.
- **Leaving their phone as an MFA device** on company accounts.
- **Overlooking vendors and contractors** who still have logins.

! The forgotten step is the one that bites

A departure handled 90% of the way is a departure with one door still open. A written checklist exists precisely so you finish all the way every time, even on a busy day.

Set things up now so exits are always easy

A few habits, put in place today, make every future departure simple no matter how it happens.

- ❑ Give every person their **own named account** — no shared logins.
- ❑ Keep admin rights **scarce and separate** from everyday accounts.
- ❑ Keep a living **offboarding map** of all accounts, apps, keys, and codes.
- ❑ Set up the ability to **remove work access from personal devices** cleanly.
- ❑ Keep your business files in **shared company storage**, not only on one person's device.
- ❑ Decide in advance **who takes over** a departing person's files and duties.

Every one of these makes the same-day checklist faster and more reliable. Set them up once, on a calm day, and future departures stop being something you dread.

If a departure turns tense

Most exits are friendly. For the rare one that isn't, here's the calm order of operations.

If you have reason to worry — a termination, a bitter resignation, someone who stormed out — the priority is speed and sequence. Cut the powerful access first: email, admin roles, remote access, MFA devices. Then change shared passwords and door and alarm codes. Then work through the rest of the checklist.

Stay professional and factual throughout. You're not punishing anyone; you're closing doors, which is ordinary good practice you'd do for a friendly departure too — just faster. If anything feels like it crosses into a legal matter, that's a question for your attorney, not your tech helper.

! Cut the keys-to-the-kingdom access first

When a departure is tense, the order is everything: admin rights, email, and remote access come off before anything else, because those are the accounts that could do real harm in the first hour.

Decide who owns this — before you need them

In a small shop, 'someone will handle it' often means no one does. Name the person now.

Decide ahead of time who runs the offboarding checklist when a person leaves — usually the owner or a trusted manager who holds the admin access to actually cut the accounts. The person who does the work needs both the checklist and the keys; make sure those two things live with the same trusted person, or that any gap is covered.

If you lean on an outside IT helper for the technical parts, that's fine — but the owner should still hold the master keys and be able to trigger an urgent cut-off without waiting on anyone. Our guides on admin accounts and hiring IT help both come back to this: the owner keeps the keys.

★ Let's make sure the right person can act fast

I'll help you confirm that whoever handles departures actually has the access to do it quickly — and that you, the owner, are never stuck waiting on someone else to close a door. Call (330) 200-8042.

A quick check a week or two later

One short follow-up catches anything the first pass missed.

A week or two after someone leaves, take five minutes to double-check: is their email still forwarding where it should, did any app you forgot turn up, are there any sign-in attempts on their old accounts, and did every device and key actually come back? Fresh eyes a bit later often spot the one login that slipped through on a hectic last day.

This is also a good moment to confirm the handoff worked — that whoever took over their files and duties can actually reach everything they need. Closing a departure cleanly is as much about the person staying as the person leaving.

✓ Watch for sign-in attempts

If you see failed sign-in attempts on a departed employee's old accounts, that's a sign to make doubly sure every door is shut and every shared password was changed.

The checklist, grouped in one view

Keep this by your offboarding map — it's every category at a glance.

Category	What to do	Same day?
Email	Block sign-in, forward	Yes
Files	Transfer, then cut	Yes
Apps	Disable each login	Yes
Remote access	Turn off VPN/tools	Yes
Shared secrets	Change passwords/codes	Yes
Physical	Keys, cards, devices	Last day

★ **Want this as a printable checklist for your office?**

I'll turn your real systems into a one-page same-day checklist you can print and reuse every time someone comes or goes. Call or text (330) 200-8042.

Common Questions

The questions I hear most from owners about shutting off access when someone leaves.

Q: Isn't cutting access the same day a bit cold?

It's just good practice, and you can do it kindly. Cutting access protects the business and the departing person both — nobody wants their old login blamed if something goes wrong later. Pair it with a warm, respectful exit.

Q: What if I delete their account and then need their files?

That's exactly why you transfer ownership of files and mail **before** disabling or deleting the account. Capture what you need first, then cut access. If you've already deleted it, there may be a recovery window — check your admin center quickly.

Q: We share a few logins — is that really a problem?

It makes every departure a scramble, because you must change each shared password and hope you caught them all. Moving to individual, named accounts is the single best change you can make for clean exits.

Q: Do I need to change the alarm and door codes?

If the departing person knew them, yes. A returned key doesn't help if the code they memorized still works. Changing codes takes a few minutes and closes a door a key return wouldn't.

★ Facing a departure right now?

Give me a call and we'll run your checklist together, same day, so nothing gets left open. Calm, thorough, and in plain English. Call or text (330) 200-8042.

You don't have to do this alone

You just have to remember that a friendly, patient person is one call away.

I hope this guide made shutting off access when an employee leaves feel a little less daunting and a lot more doable. Keep it with your other business papers, come back to a page whenever you need it, and don't worry about memorizing anything.

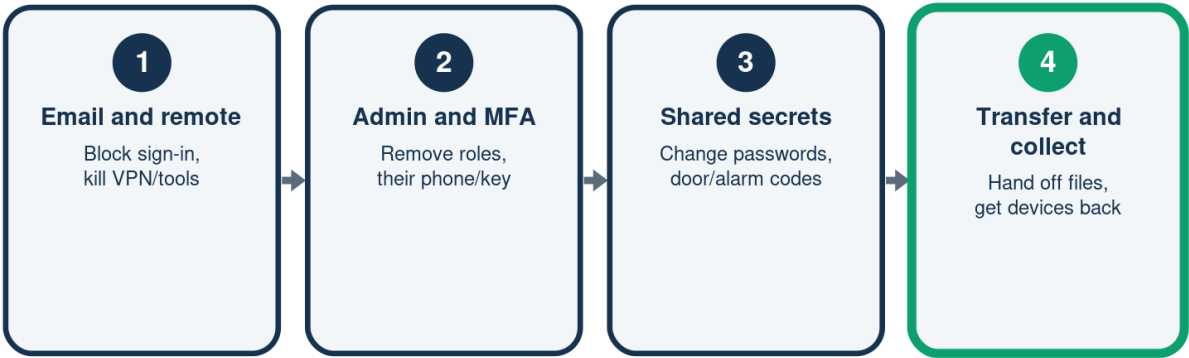
When you'd rather have a hand, that's exactly what I do. I come to your business, work at your pace, and never make you feel rushed or silly for asking. A first visit is a flat \$99, and for the parts that don't need me on-site I can often help right on your screen for \$49. Every visit comes with a 30-day, come-back-free guarantee. I'm a tech helper, not a lawyer or your insurance agent — for the legal and insurance pieces I'll help you understand the questions and line up the right professional.

★ Bill's Home Tech — real help, close to home

Call or text me at (330) 200-8042, or visit BillsHomeTech.com. Serving Atwater and all of Portage County. 30+ years of patient, plain-English tech help — and if you're ever not 100% happy with a visit, I'll make it right or refund it. That's a promise. — Bill

The Same-Day Order

Cut the powerful access first



Transfer ownership of files and mail before you delete an account.

Shared vs. Named Logins

Why individual accounts make exits clean

	Shared login	Named account
Cut one person off	Reset for all	Disable just them
Know who did what	No	Yes
Leaver still knows it	Likely	No
Offboarding effort	A scramble	One click

Individual accounts are the single best change for clean departures.

Where Access Hides

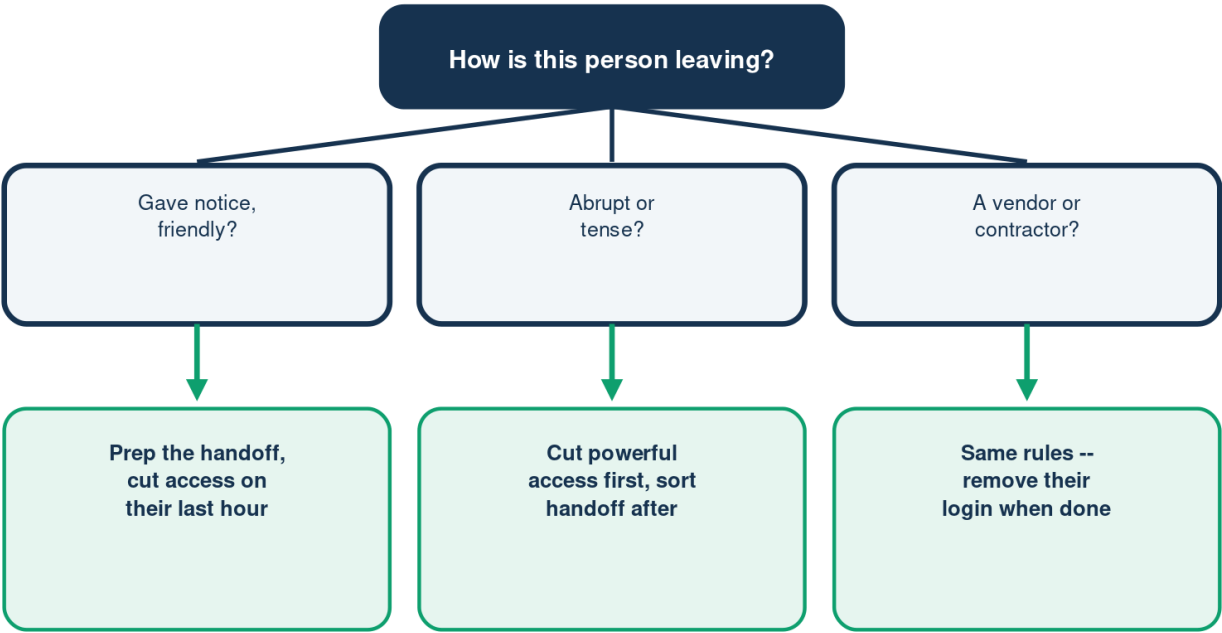
Walk the whole list, not just email

	Examples	Action
Email and files	Gmail, Drive	Block, transfer
Business apps	Accounting, POS	Disable each
Remote access	VPN, tools	Turn it all off
Keys and codes	Doors, alarm	Collect, change
Personal devices	Phones, home PC	Remove work access

A map made ahead of time means nothing gets forgotten on the day.

Planned or Sudden?

Same checklist, different speed



Either way, never leave a former login switched on overnight.

Illustration - a schematic, not to scale. Your setup may differ.



Need a Real Person?

You do not have to remember all of it.
You just have to remember you can call.
Friendly, in-person tech help -- I come to you.

BILL'S PROMISE

If you are not 100% happy with a visit, I will
make it right -- or refund it. No awkwardness,
no fine print. That is how I would want to be treated.

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

— Bill

Prefer help without a visit?

Bill can screen-share and fix many things remotely — a flat \$49, free for Support Plan members.



A Note From Bill

A quick note from Bill.

I write these guides to make home tech a little less frustrating, and I do my best to keep every step accurate and up to date. Still, every home, device, and setup is a bit different, so I can't promise a guide will match yours exactly or fix your particular problem. These guides are for general information only — they're not professional, legal, or financial advice, and they don't replace your device's own manual or the manufacturer's instructions. Please go slow, use your own good judgment, and use everything here at your own risk. If a step involves electrical wiring, a gas appliance, a water heater, plumbing, or climbing a ladder — or if anything just doesn't feel safe — please stop and call a licensed professional (or give me a call at 330-200-8042). Bill's Home Tech and Bill Davis can't be responsible for any damage, data loss, or injury that comes from using these guides. Thanks for reading, and stay safe out there.

— *Bill*



Book a visit —
billshometech.com/book

Use of these guides is subject to our Terms of Use (billshometech.com/terms-of-use).

(330) 200-8042 · BillsHomeTech.com

Bill@BillsHomeTech.com · Mon–Sat 9:00 AM – 7:30 PM

For general information only — not professional advice. Use at your own risk. For electrical, gas, water, or ladder work, please call a licensed professional. — Bill's Home Tech