
FROM THE MEHRUTHERM BLOG · CYBERSECURITY

When the One Person Who Knew the System Leaves

In many small businesses and towns, one person quietly holds all the logins and know-how. When they leave, it can leave with them. How to fix that first.

Himanshu Mehru · Founder, Mehrutherm

June 24, 2026

In most small organizations there is one person who just knows how things work. They set up the email, they know the website login, they are the one who gets the printer talking to the computers again. Everyone else is grateful, and a little vague on the details.

It works beautifully, right up until that person leaves.

Then comes the scramble. Nobody knows the password to the thing that everybody needs. The accounts are tied to a personal phone or a personal email. The knowledge that kept everything running was never written down anywhere, because it lived in one head, and that head just walked out the door. This is one of the most common and most avoidable problems we see, in businesses and in town offices alike.

KEY TAKEAWAYS

- In a lot of small organizations, **one person quietly holds the keys to everything.**
- When they leave, **the logins, the know-how, and the recovery path can leave too.**
- The fix is dull and cheap: **write down how things work, and own the accounts as an organization, not as a person.**
- Do it **while that person is still around to help**, not after they are gone.

Why This Happens to Good Organizations

This is not a sign of a badly run shop. It is the natural result of being small and busy.

When you have a handful of people and a long to-do list, you do not stop to document who controls the domain or where the backups live. One capable person handles it, and because they handle it well, nobody else ever needs to learn. The arrangement rewards you every single day, which is exactly why the risk stays invisible until the day it does not.

The technical term for this is a "single point of failure": one piece that, if it disappears, takes a lot down with it. In a small organization, that single point of failure is usually a person, not a machine.

What Actually Gets Lost

When the keeper of the keys leaves, it is rarely one thing that goes missing. It is a cluster.

The logins. The website, the email accounts, the domain registration, the social pages. If these were set up under a personal account, regaining control can range from a long afternoon to a genuine ordeal.

Many accounts send their "reset your password" codes to a phone number or email that belonged to the person who left. Lose that, and even the official way back in is closed.

The quiet stuff: which renewal is due when, who the vendor contacts are, how the one slightly unusual thing gets done. None of it was secret. It just never got written down.

While all of the above gets untangled, ordinary work stalls. For a business that can mean missed leads. For a town it can mean residents who cannot do something they need to do.

THE WORST TIME TO LEARN THIS LESSON

The hardest version of this is when the departure is sudden or unfriendly. You do not get a calm handover. You get a locked door and a list of things you cannot access. Everything in this article is far easier to do while the person is still on good terms and still around to answer questions.

The solution is not clever or expensive. It is just the stuff that always gets skipped because nothing is on fire yet.

Wherever possible, the important accounts should belong to the business or the town, registered to an organization email that does not depend on any one employee. People come and go; the account stays. When someone leaves, you remove their access, you do not lose the account.

Not a manual. A simple, living list: what accounts exist, what each one is for, who the vendor is, and when things renew. Keep it somewhere safe that more than one trusted person can reach. The goal is that if anyone vanished tomorrow, someone else could pick up the thread.

Check where each account sends its recovery codes. If the answer is "the phone of the person who set it up," fix that now, while you still can. Recovery should point at the organization, not an individual.

When someone joins, they get what they need. When someone leaves, their access leaves the same day. This is good security as well as good continuity, and we cover it alongside the other fundamentals in cybersecurity basics every small business and town should have.

How much each fix tends to cost you

Write down how things work

Low effort



Review who has access

Low effort



Fix account recovery paths

Some effort



Move accounts to the organization

Some effort



A rough guide, not a precise measure. None of this is expensive or difficult. It is mostly a matter of doing it once, on purpose, before you need it.

For local governments, this is not just convenient, it is part of running things properly. The people in the offices change. Clerks move on, terms end, volunteers step back. The town's website, email, and records have to outlast all of them, because residents depend on them continuously. When access and knowledge live with whoever happens to hold the role today, every transition becomes a small crisis. Building continuity in from the start is simply good governance.

Here is the quiet benefit of having someone look after this for you: continuity stops depending on any single person, including any single employee.

That is a real part of what we do for the businesses and towns we look after. The accounts are owned properly, the important details are written down and kept current, the recovery paths point where they should, and there is always more than one way back in. When someone moves on, things keep running, because the setup was never balanced on one person to begin with. (If you are choosing who builds or runs your site, what to ask before you let anyone build your website covers the questions that surface this early.)