# Passportal Site Blog 1

NOTE: This blog is written for you to post to your own website blog. To avoid the potential confusion of multiple MSPs presenting this as original content of their own, we’ve written an introduction which you can customize, that sets up the series and make it clear that someone could find the same blog online and not think it’s plagiarized.

All content is meant to be copied and pasted. All items in BLUE, or highlighted in blue, are for your reference only. Any items highlighted in yellow, you’ll need to customize. Feel free to tweak any of the following provided material to fit better with your business goals.

[INTRO]

This blog gets at a really important topic for businesses, especially smaller businesses that don’t have a lot of extra resources for dealing with IT admin. Using a centralized access control system to make sure your systems aren’t accessible by people who have left your company is really important to overall security.

[ALTERNATE HEADLINES]

# Do you know who has access to your systems?

When you took their keys back, did you cancel their passwords, too?

You control access to your office. Why not your IT?

[BLOG COPY]

The last time an employee left your business, did you revoke their access to your IT systems? Are you sure? Do you have a way to check?

What kind of information could your former employees get if they still hold valid credentials (even though they no longer work there)? Depending on your business, the answer could include client data, proprietary research, or your financial information.

A former employee could use un-revoked credentials to view or download information that might help their new employer lure clients away from you or steal your ideas, which could be very bad for your bottom line. An employee who left angrily (perhaps because they were fired) could be even more dangerous, and might use their login to implant ransomware, viruses, or other malware.

Even if the departed employee would never do anything to harm you themselves, if theircomputer or records were compromised, someone else could get those same credentials—and that individual might not be so well-meaning.

**Protect yourself with centralized access control**

There are a number of ways to help make sure your business isn’t exposed to malicious password use after an employee leaves, and they all fall under the umbrella of “access control”: controlling who can view and change what, when and how.

Good access control starts with company policy. It should be part of your HR offboarding routine to cancel an outgoing employee’s credentials the same way you delete their door code and take back their keys.

That said, when it comes to passwords, revoking credentials manually can be time consuming, depending on how many systems a person had access to and how many unique passwords they used. Manual revocation is also subject to human error: it’s easy to forget a system or miss a step such that an account you thought was closed remains open.

The safer option is to establish a centralized password management and access control system that gives you complete visibility into the use of all your systems, and a single point to activate or revoke permissions. At a glance, you’ll be able to see who has credentials to what systems, and when an employee leaves your company, you can instantly revoke their privileges for anything on your network.

With good access control procedures, you can be more confident in the overall security of your data and systems.

[MSP CUSTOMIZABLE CLOSING]

If you have questions about access control and what might be right for your business, [I’d/we’d] be happy to talk them over with you. And keep an eye out for [my/our] next blog on how to make sure your password approach is compliant with laws and regulations.

# Email for Blog 3

[SUBJECT LINE OPTIONS:]

Do you know who has access to your IT systems?

Keep confidential information confidential

When employees leave, do they take their passwords with them?

[ALTERNATE HEADLINES]

Because active passwords should be for employees only

Keep closer track of who has passwords to your business systems

Close the door on malicious password use

[EMAIL COPY]

It’s standard business practice to take back an employee’s keys when they move on from your company. But a surprising number of businesses don’t do the same with digital passwords. And sometimes those passwords can provide ex-employees with access to highly sensitive information and systems that they should not have.

So how do you protect your business from unauthorized IT access? The answer is to establish better control over who holds valid passwords — and to revoke any credentials assigned to people who no longer work at your company. Our latest blog offers some tips on how to do this without adding hours of admin time.

Read our blog on centralized system access control today.

# Social Media Posts for Blog 3

[FACEBOOK/LINKEDIN]

**Do you know who has access to your systems?**

How many of your former employees still have active passwords that could give them access to your most sensitive data and systems? Missed steps in exit processes could mean employees who haven’t worked for you in months — or years — can still log into some of your systems, leaving you vulnerable. Find out how to create a rock-solid access control system to help keep yourself protected from the moment an employee leaves your company.

[TWITTER]

Do you know who has access to your systems? A proper access control system can make sure you don’t have to wonder. [Insert blog URL]