5 TIPS FOR PREVENTING HARM AFTER AN EMPLOYEE LEAVES

Poor password management can open businesses to significant risk, especially when employees leave. Consider the following:

- OF EMPLOYEES RE-USE PASSWORDS AT WORK¹
  - OVER 70%

- OF EMPLOYEES ADMIT TO RETAINING ACCESS TO AT LEAST ONE APPLICATION FROM A FORMER EMPLOYER²
  - 89%

- ADMIT TO LOGGING INTO AND USING AN ACCOUNT FROM THEIR FORMER EMPLOYER³
  - 49%

So how do you ensure a smooth, safe transition following an employee departure? Follow these five tips:

1. STANDARDIZE KNOWLEDGE SHARING
   Use centralized software to help ensure client information is properly documented, safeguarded, and accessible in the case of employee exit.

2. FOLLOW THE PRINCIPLE OF LEAST PRIVILEGE
   Implement a password tool with granular permissions. Make sure employees have only the level of access they absolutely need.

3. ROTATE PASSWORDS REGULARLY
   Keep passwords fresh by rotating credentials regularly via a centralized system. This can prevent hackers from exploiting old passwords.

4. REVOKE ACCESS AND AUDIT CREDENTIAL USAGE FOLLOWING A DEPARTURE
   Shut down access immediately when someone leaves, and monitor accounts for unauthorized access attempts.

5. AUTOMATE PASSWORD AND DOCUMENTATION MANAGEMENT
   Password and documentation management can be a lot to handle, and it can lead to employees becoming overwhelmed and falling into bad habits.

Password management software relieves the burden while keeping your business safe.

SolarWinds® Passportal + Documentation Manager lets you safeguard accounts with strong passwords, quickly revoke access when needed, and maintain documentation even after someone leaves. Request a demo today.


70% of hacking-related breaches leveraged either stolen and/or weak passwords.

Keep Your MSP safe after employee departures.