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

1. **Implement a password tool with granular permissions.** Make sure employees have only the level of access they absolutely need.

2. **Use centralized software to help ensure client information is properly documented, safeguarded, and accessible in the case of employee exit.**

3. **Shut down access immediately when someone leaves, and monitor accounts for unauthorized access attempts.**

4. **Keep passwords fresh by rotating credentials regularly via a centralized system.** This can prevent hackers from exploiting old passwords.

5. **Password and documentation management can be a lot to handle, and it can lead to employees becoming overwhelmed and falling into bad habits.**

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

- **Follow the principle of least privilege.**
- **Standardize knowledge sharing.**
- **Revoke access and audit credential usage following a departure.**
- **Automate password and documentation management.**
- **Rotate passwords regularly.**

---

[1] N-able™ 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.

---

[2] of employees admit to retaining access to at least one application from a former employer.

[3] of employees admit to logging into and using an account from their former employer.

[4] of hacking-related breaches leveraged either stolen and/or weak passwords.

[5] Over 70% of employees re-use passwords at work.

---

N-able™ 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.

---

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