

Small business IT | Easy | 2 min read

A password policy that actually works

Strict password rules that nobody can follow lead to sticky notes and reused passwords. A better policy is short, realistic and backed by tools.

The core of a good policy

- Everyone uses a **password manager** to create and store passwords.
- Every account has a **different** password. Reuse is how one leak becomes ten.
- **Two-step sign-in** is switched on for email, banking, accounting software, cloud storage and anything holding customer data.
- Long passwords beat complicated ones. Three random words strung together is easier to remember and harder to guess than a short mix of symbols. The NCSC recommends this approach.

What to stop doing

- Forcing staff to change passwords every month. Change a password when there is a reason, such as a suspected leak.
- Sharing one login between several people.
- Writing passwords on notes stuck to screens.
- Using personal details such as pet names or birthdays.

Putting it in place

1. Choose one business password manager and set it up for everyone.
2. Have each person create a strong master password, and keep it to themselves.
3. Turn on two-step sign-in, using an authenticator app where possible rather than text messages.
4. For tools that must be shared, use the manager's sharing feature so you can remove access later.
5. Write your policy on one page and go through it with new starters.

If something goes wrong

Tell staff to report suspected problems straight away, and make sure nobody is blamed for reporting. Change the password on the affected account and any account that used the same one.

When to get more help

Ask for help if you want to choose a manager for the team, if accounts have already been taken over, if some systems do not support two-step sign-in, or if you need to clean up lots of old shared logins.

Still stuck? Email admin@visiontech336.com and tell us what you can see on the screen. Menus and button names can differ slightly between versions and makes. If something does not match, stop and ask rather than guess. Please never send passwords or card details.