Virtual Dynamics
MANAGED IT SERVICES

PASSWORDS · MFA · PASSKEYS

Passwords, minus the headache.

You don't need a better memory. You need a better system. Here's what CISA and the official U.S. password standard (NIST) recommend now, on one page. 🔐

LONG
At least 16 characters.
Longer is stronger. Length does more than any symbol ever will.

RANDOM
Words, not birthdays.
A passphrase of 4 to 7 unrelated words works well, like *HorsePurpleHatRunBay*.

UNIQUE
One per account.
A different password everywhere, so one leak doesn't open every door.

Old rules you can retire per NIST SP 800-63B-4

- ✕ ~~Changing every password on a schedule, just because.~~
- ✕ ~~"Must include a capital, a number and a symbol."~~
- ✕ ~~Sites that block password managers or autofill.~~

- ✓ Change it when there's a sign it leaked.
- ✓ Length wins. Services must require at least 15 characters when a password is the only lock.
- ✓ Services must allow password managers and autofill. They should also allow paste.

Get the office a password manager

It makes and remembers the long ones. What to look for:

- ☐ Shared folders by team (front desk, billing, providers)
- ☐ Turn off a person's access in one click when they leave
- ☐ MFA on the password manager itself
- ☐ Works on phones and every browser your team uses
- ☐ The business owns the account, not one employee

Turn on MFA. Then go passkey.

CISA says turn on MFA (a second check at sign-in) for every account that offers it. Start with email and banking.

Heads up, Microsoft 365 offices: Microsoft retires its own text-message and voice sign-in codes on **Feb 1, 2027** for most users (July 1, 2027 for Global Administrators and external users). After those dates, people whose only second factor is a text or voice code will be required to set up a **passkey** — unlocked with a face, fingerprint or PIN — before they can sign in.

Change it today if...

- › You got a breach alert (for example from Have I Been Pwned)
- › Someone who knew it has left the team
- › You typed it into a page you're now not sure about
- › You reused it on any other site
- › It lives on a sticky note on the monitor 🙂
- › A site or app you use announces a breach

Sharing a login with the team? Share it through the password manager, not a group text or an email. Better yet, give each person their own account wherever the software allows it. Then you can see who did what, and remove one person without changing everyone's password.

Sources: CISA Secure Our World, "Use Strong Passwords" (long: at least 16 characters; random passphrase of 4–7 unrelated words, example from CISA; unique; use a password manager) and "Turn On MFA" (CISA lists these pages as archived content); NIST SP 800-63B-4, Digital Identity Guidelines: Authentication (15-character minimum for single-factor passwords; no composition rules; no scheduled changes, but change on evidence of compromise; allow password managers and paste); Microsoft Learn, SMS and voice authentication retirement and passkeys (FIDO2) pages; Help Net Security (Nov 12, 2026) on Have I Been Pwned breach alerts.

Want a hand rolling this out?

We'll help your team switch to passwords that are easier, not harder.

(888) 531-1109
vdcmsp.com