CICADA | RESOURCES

LESSON 04 OF 04 · 7 MIN · WORKING KNOWLEDGE

Rolling out a password manager

The tool is the easy part. Here's the week-one plan that gets people using it without a mutiny.

Why rollouts fail

Common reasons: no owner, no plan, a free personal plan with no admin recovery, a weak master password, and no decision about shared work. People keep using the old spreadsheet because nobody moved the accounts that matter.

Pick a business plan with shared vaults, admin controls and MFA. Name an owner. Set a date.

A week is enough

01 **Day 1:** set up the business vault, enable MFA, store recovery offline, add a second admin.

02 **Day 2:** move banking, accounting, payroll and payment platforms.

03 **Day 3:** email, domain, website, social media.

04 **Day 4:** invite staff, install apps and extensions, import and then securely delete browser exports.

05 **Day 5:** create shared vaults for shared responsibilities; retire shared logins where possible.

Shared vaults, not shared logins

A shared vault lets the right people access a credential without putting it in a chat message, and gives you an audit trail. It is a compromise, not the ideal. Named accounts are still better wherever the system supports them.

Set emergency access so the business can recover if the owner is unavailable. Test it once, then leave it alone.

> **THE MASTER PASSWORD**
>
> It must be long, unique and memorised. Never store it in the vault, a document or an email. Write recovery codes on paper and keep them somewhere physically secure.

Key takeaways

- ✓ Use a business plan with admin controls and MFA.
- ✓ Move critical accounts first; don't wait for a big-bang migration.
- ✓ Shared vaults for shared work, named accounts wherever possible.
- ✓ Set up and test emergency access.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.