Why Do You Need
Business Password Manager?

passman.co

If you do not use password manager, your company does not oversee the security of your data, meaning it does not ensure your protection, exposing your business to the following risks:

Unauthorized Access	Hackers, Ransomware	Non-compliance (NIS2, GDPR)
PRIVACY RISK	OPERATIONAL RISK	RISK OF PENALTIES

A co-worker is also a source of danger!

If your colleagues store passwords on sticky notes (attached to monitors or walls), in Excel or Word documents, and others can easily access them.

If your colleagues use easily guessable/identical passwords and password changes are not mandatory.

If you cannot access your systems (the sysadmin is sick or on vacation, or passwords stored in a safe are no longer current).

If you do not change the passwords known by departing colleagues

External IT service providers are also a source of danger!

Your service provider's employees need to access multiple customer systems (including yours too), so they often use the same password for simplicity

Are you sure that your service provider handles your data and passwords correctly?

Do only authorized individuals access your systems when necessary?

Do you know what changes your service provider made to your systems during remote access, or whether they accessed data they shouldn't have?

Do you have access to the admin passwords of your systems at all, or is it only the service provider that knows them?

Who Needs a Password Manager?

Anyone who wants to keep business secrets **safe** (to prevent theft or loss)

Every company where a user uses **more than one password**

For every company that is required to **store customer passwords** as part of its services **and share** these 'secrets' with its employees

Where external **service providers have access** to internal, corporate data

For those subject to **GDPR** regulations

For those subject to **NIS2** regulations

Arpad Boldog
Product Owner
+36 30 297 8382
arpad.boldog@moresimp.com

passman.co