BEZPEČNOST AI VE FIRMĚ · CHECKLIST

12 bodů, než ve firmě zapnete Microsoft 365 Copilot

Pro firmy, které zvažují placený Microsoft 365 Copilot (práce s firemními daty přes Microsoft Graph). Projděte s IT nebo s externím správcem, ideálně před pilotem.

Podle Microsoftu Copilot zobrazuje jen firemní data, ke kterým má uživatel alespoň právo ke čtení. Oprávnění neobchází, ale zviditelní každou chybu v nich: weby a týmy sdílené s celou firmou, odkazy pro všechny v organizaci, weby bez vlastníka. Zaškrtněte, co platí.

A. NEŽ HO ZAPNETE

1. ☐ **Verze:** je jasné, zda jde o Copilot Chat (firemní data přes Microsoft Graph nepoužívá), nebo o Microsoft 365 Copilot, který firemní data čte automaticky?
2. ☐ **Firemní účet:** přihlašují se všichni účtem Microsoft Entra, ne osobním účtem Microsoft?
3. ☐ **Sdílení s celou firmou:** máte přehled obsahu sdíleného se skupinou Everyone except external users, veřejných týmů a odkazů pro všechny v organizaci?
4. ☐ **Citlivé weby:** jsou vytipované weby a týmy se mzdami, HR, financemi, vedením, smlouvami a zdravotními údaji a ověřeno, kdo k nim má přístup?
5. ☐ **Vlastníci:** má každý web a tým vlastníka, který ví, kdo v něm má být? Neaktivní weby jsou archivované nebo smazané?
6. ☐ **Výchozí odkaz:** je výchozí typ odkazu pro sdílení nastavený na konkrétní lidi, pro organizaci i pro citlivé weby?

B. OMEZENÍ A OCHRANA

7. ☐ **Dočasné vyřazení:** citlivé weby, které nestihnete opravit, jsou vyřazené z Copilotu (Restricted Content Discovery) a je určen termín opravy oprávnění? Funkce oprávnění nemění.
8. ☐ **Štítky citlivosti:** mají nejcitlivější dokumenty štítek (Microsoft Purview)? Štítek webu nebo týmu se na soubory nedědí.
9. ☐ **Pilot:** spouští se Copilot nejdřív na malé skupině, která hlásí, co našla navíc?

C. PROVOZ A LIDÉ

10. ☐ **Audit a uchovávání:** je zapnutý audit, víte, kde se dohledají dotazy a odpovědi (eDiscovery, Purview), a je rozhodnuto, jak dlouho se uchovávají?
11. ☐ **Hlášení:** vědí lidé, že Copilot vidí, co vidí oni, a komu hlásit, když najde dokument, který by vidět neměli?
12. ☐ **Registr a směrnice:** je Copilot zapsaný v registru AI nástrojů a v AI směrnici jako schválený nástroj, včetně pravidel pro citlivá data?

Stop pravidlo: pokud u bodů 3 a 4 odpovíte „ne“, Microsoft 365 Copilot zatím plošně nezapínejte. Nejdřív zjistěte, co je sdílené s celou firmou.

Zdroj: aiscale.cz/bezpecnost-ai/copilot-sdileni-dat/ · Vychází z dokumentace Microsoft Learn (Copilot privacy, Copilot overview, SharePoint Advanced Management, Restricted Content Discovery, Microsoft Purview), stav 6. 11. 2026

Verze listopad 2026 · informativní materiál, nejde o právní poradenství