## Příloha č. 1

**Zabezpečené nástroje AI:**

- Microsoft 365 Copilot – pouze v rámci přístupu přiděleného pracovištěm CIT k existující univerzitní identitě uživatele
- Gemini – pouze v rámci přístupu přiděleného pracovištěm CIT k existující univerzitní identitě uživatele
- Gemini Notebook (kdysi Notebook LM) – pouze v rámci přístupu přiděleného pracovištěm CIT k existující univerzitní identitě uživatele.
- Beey – smluvně garantovaný systém přepisu nahrávek/rozhovorů do textu (OU licence)
- Whisper – plně zabezpečený on premise nástroj přepisu nahrávek/rozhovorů do textu (OU licence)
- LLM a další AI modely provozované lokálně na infrastruktuře OU nebo v jiném prostředí pod univerzitní správou, přednostně bez připojení k internetu. Pokud je externí připojení nezbytné, musí být omezeno na bezpečné prostředí v EU/EHP.

**Nezabezpečené nástroje AI:**

- Veřejně dostupné nástroje AI, které nejsou OU zpřístupněny jako instituci a ke kterým nebyl přístup přidělen CIT v rámci univerzitní identity uživatele, například (nikoliv výlučně):
    - Microsoft 365 Copilot – v rámci osobní licence
    - Gemini – v rámci osobní licence
    - Gemini Notebook (kdysi Notebook LM) – v rámci osobní licence
    - LLM a další AI nástroje na veřejně dostupných (národních) infrastrukturách
    - ChatGPT – v rámci osobní i univerzitní licence
    - Claude – v rámci osobní i univerzitní licence
    - Perplexity – v rámci osobní i univerzitní licence
    - Canva AI – v rámci osobní i univerzitní licence
    - Midjourney – v rámci osobní i univerzitní licence
    - GitHub Copilot – v rámci osobní i univerzitní licence

**Nebezpečné nástroje AI:**

- DeepSeek
- Neoficiální klony a aplikace AI služeb
- Neověřená rozšíření prohlížeče a mobilní aplikace s přístupem k obsahu uživatele
- Nástroje AI, u nichž CIT, univerzita nebo bezpečnostní autorita stanoví omezení či zákaz použití

Důležité upozornění:

*Před použitím nezabezpečeného nebo nového nástroje AI je uživatel povinen ověřit podmínky jeho používání, zejména jaká data jsou zpracovávána, kde jsou ukládány a zpracovávány vstupy, výstupy, historie chatu, metadata a přiložené soubory, a zda se na zpracování podílejí další poskytovatelé nebo subdodavatelé. Samotné prohlášení poskytovatele, že data nejsou používána k trénování modelu, nepostačuje. Pokud nelze spolehlivě ověřit, že data zůstávají v prostředí ovládaném OU nebo alespoň v prostoru EU/EHP, nesmí být do nástroje vkládány osobní údaje ani neveřejná data OU.*