UNIVERZITA J. E. PURKYNĚ V ÚSTÍ NAD LABEM

STANOVISKO UNIVERZITY JANA EVANGELISTY PURKYNĚ V ÚSTÍ NAD LABEM K VAROVÁNÍ NÁRODNÍHO ÚŘADU PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST PŘED PRODUKTY SPOLEČNOSTI DEEPSEEK

I. Preambule

Univerzita Jana Evangelisty Purkyně v Ústí nad Labem (dále jen „UJEP“) bere na vědomí varování Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB) ze dne 10. července 2025 (č.j. 4417/2025-NÚKIB-E/350), které upozorňuje na hrozbu v oblasti kybernetické bezpečnosti spočívající ve využívání produktů, aplikací, řešení, webových stránek a webových služeb, včetně aplikačního programového rozhraní (API), poskytovaných společností Hangzhou DeepSeek Artificial Intelligence Basic Technology Research Co., Ltd., nebo jakoukoli její přidruženou entitou (dále jen „produkty DeepSeek“).

Toto varování se týká zařízení přistupujících k informačním a komunikačním systémům kritické informační infrastruktury, informačním systémům základní služby a významným informačním systémům. V souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti (ZoKB), je UJEP jako veřejná vysoká škola povinna zohlednit tuto hrozbu v hodnocení rizik a zavést odpovídající bezpečnostní opatření. Na základě analýzy dostupných informací, včetně technických zjištění NÚKIB a mezinárodních reakcí (např. zákazy v Austrálii, Itálii a USA kvůli rizikům datových úniků, cenzury a vazeb na čínskou vládu), přijímá UJEP stanovisko k varování Národního úřadu pro kybernetickou a informační bezpečnost před produkty společnosti DeepSeek.

II. Závazná opatření pro zaměstnance, studenty a spolupracovníky UJEP

1. Závazná opatření vyplývající z platného ZoKB a na ochranu informačních systémů jsou platná pro všechny zaměstnance, studenty, doktorandy a externí spolupracovníky používající univerzitní zařízení, sítě nebo systémy (včetně mobilních zařízení připojených k univerzitním systémům).

2. Používání produktů DeepSeek (včetně aplikací, webových služeb, API a jazykových modelů komunikujících se servery DeepSeek) je zakázáno na všech zařízeních přistupujících k informačním systémům UJEP nebo využívajících ICT infrastrukturu UJEP. Toto zahrnuje instalaci aplikací, používání webových rozhraní nebo integraci do softwaru (např. v AI nástrojích třetích stran).

3. Varování se nevztahuje na open-source velké jazykové modely DeepSeek, pokud jsou nasazeny „offline“ (bez komunikace se servery DeepSeek) pro účely bezpečnostního testování, výzkumu nebo analýzy.

4. Písemně podané a podepsané (ve všech formách) žádosti o výjimku (např. pro vědecký výzkum) musejí být schváleny manažerem kybernetické bezpečnosti UJEP a musejí zahrnovat analýzu rizik vzhledem ke konkrétní aplikaci. Výjimky budou udělovány pouze na omezenou dobu a s dodatečnými bezpečnostními opatřeními (sandboxing).

5. Ačkoli varování přímo nezakazuje použití produktů DeepSeek na osobních zařízeních, UJEP důrazně doporučuje zaměstnancům a studentům vyhnout se těmto produktům kvůli rizikům úniku citlivých dat souvisejících s univerzitními aktivitami (např. e-maily, výzkumné dokumenty).

6. V případě detekce provede CI UJEP inventarizaci a odstranění produktů DeepSeek z univerzitních systémů.

7. Případné podezření na použití produktů DeepSeek je třeba nahlásit na e-mail: kb@rt.ujep.cz.

III. Porušení závazných opatření

Porušení tohoto stanoviska bude řešeno v souladu s interními předpisy UJEP (včetně disciplinárních opatření).

IV. Závěrečné ustanovení

UJEP bude toto stanovisko pravidelně přezkoumávat na základě aktualizací od NÚKIB.

doc. RNDr. Jaroslav Koutský, Ph.D., rektor

doc. RNDr. Jaroslav Koutský, Ph.D.
Digitálně podepsal doc. RNDr. Jaroslav Koutský, Ph.D.
Datum: 2025.07.17 13:22:46 +02'00'

Příloha č. 1

Klíčová rizika spojená s produkty DeepSeek

Podle varování NÚKIB a dalších zdrojů (jako analýzy CSIS, Forbes a Cisco) představují produkty DeepSeek bezpečnostní hrozbu zejména z následujících důvodů:

1. Nízké zabezpečení
Produkty jsou zranitelné vůči kybernetickým útokům, včetně man-in-the-middle útoků, slabé detekce rootování a používání zastaralých šifrovacích algoritmů (např. 3DES).

2. Ukládání a sdílení dat
Data uživatelů (včetně citlivých dotazů a souborů) jsou ukládána na serverech v Číně (např. Huawei, China Mobile) a sdílena s entitami jako ByteDance (TikTok). Existuje riziko de-anonymizace uživatelů a úniků dat.

3. Právní a politické vazby
Společnost podléhá čínskému právu, které umožňuje vládě přístup k datům a vynucení spolupráce. Pravděpodobné vazby na čínskou vládu zvyšují riziko špionáže a cenzury (např. zkreslování výsledků v prospěch čínských narativů).

4. Technické zranitelnosti
Možnost obnovy citlivých dat z cache, absence ověřování SSL certifikátů a náchylnost k jailbreakingu (obcházení bezpečnostních opatření).

5. Mezinárodní kontext
Podobná rizika vedla k zákazům v jiných zemích a institucích, včetně univerzit (např. Masarykova univerzita v Brně opustila TikTok kvůli bezpečnostním obavám).

Tato rizika mohou ohrozit důvěrnost, integritu a dostupnost dat UJEP, včetně osobních údajů studentů, zaměstnanců a výzkumných dat.

Další informace u manažera kybernetické bezpečnosti na e-mailu: kb@rt.ujep.cz.