Jihočeská univerzita v Českých Budějovicích

Označení dokumentu:	**ISMS-S-007**
Název dokumentu:	**Zásady používání AI na JU**
Typ dokumentu:	Směrnice výboru pro řízení kybernetické bezpečnosti JU
Rozsah:	Směrnice je určena všem uživatelům JU.
Prvek legislativy:	-----
Datum vydání:	17. 09. 2025
Datum účinnosti:	**17. 09. 2025**
Platnost do:	odvolání
Počet stran + příloh:	4 + 0
Verze:	1.0
Význam a benefity:	Význam této směrnice je určit pravidla pro bezpečné a odpovědné využívání AI na JU, zejména s ohledem na ochranu citlivých, osobních a interních dat. Benefit směrnice je zvýšení bezpečnosti při práci s nástroji AI, prevence úniku informací a jasné vymezení odpovědnosti uživatelů za dodržování bezpečnostních opatření.
Uložení:	ISMS část na Wiki JU – wiki.jcu.cz
Ruší dokumenty:	-----
Zpracovatel:	Jan Urbánek - Manažer KB JU
Přezkoumal:	Výbor pro kybernetickou bezpečnost JU
Schválil:	Výbor pro kybernetickou bezpečnost JU

Informační sdělení

Tato směrnice stanovuje pravidla využívání systémů umělé inteligence (AI) pro všechny uživatele JU. AI zahrnuje různé systémy schopné samostatného učení, analýzy a generování dat na základě informací, které do nich uživatelé vkládají.

AI dnes můžeme uplatnit v nespočtu oblastí pro usnadnění našich každodenních osobních či pracovních rutin, jako je například analýza velkého objemu dat, úprava dokumentů, poskytování personalizovaných doporučení, učení, vyhledávání informací a mnohé další.

AI vždy berte jako podpůrný nástroj, jehož výsledky je nutné důsledně kontrolovat a kriticky vyhodnocovat.

Se všemi těmito benefity využití AI existují ale také **informační** a **bezpečnostní rizika**, na která je dobré si dát pozor – více informací níže.

Seznam **povolených** a **ověřených AI nástrojů** pro zpracování **citlivých** nebo **interních dat** JU je uveden v bodě **a)**.

Pravidla pro využití všech ostatních AI nástrojů jsou uvedena v bodě **b)**.

Pravidla napojení AI nástrojů a služeb na data a informace JU jsou uvedena v bodě **c)**.

Varování při využívání specifických AI nástrojů jsou uvedena v bodě **d)**.

Pro studenty směrnice navazuje na opatření rektora R 567 a měli by se řídit stejnými pravidly v případě zpracování citlivých dat v rámci studia a závěrečných prací.

- **Informační rizika s AI**

Informace, které AI poskytuje skrze své výstupy, je nutné vždy **důkladně kontrolovat**, protože výsledky AI nemusí být bezchybné nebo zcela objektivní. Přestože AI dokáže poskytnout rychlé a užitečné odpovědi, nemusí být tyto informace vždy přesné, aktuální nebo správně interpretované. Umělá inteligence může například chybně pochopit zadání, vytvořit nepřesné závěry nebo generovat zastaralé či zkreslené informace.

Z tohoto důvodu je třeba pečlivě **ověřovat správnost získaných dat**, zejména pokud mají být využity pro rozhodování, publikaci nebo další práci.

- **Bezpečnostní rizika s AI**

Bezpečnostní rizika vyplývají ze **zpracování citlivých** či **interních dat**, která mohou skrze využití AI uniknout. Data vložená do AI **nejsou soukromá** a mohou být dále využita pro další trénink systému nebo sdílena s třetími stranami bez vědomí uživatele.

Neuvážené sdílení informací může vést k porušení obchodního tajemství, ohrožení ochrany osobních údajů nebo dokonce způsobit porušení právních povinností či finanční škody.

Uživatelé by proto měli vždy pečlivě zvážit, jaká data do AI zadávají, a u citlivých nebo interních informací používat pouze ověřené nástroje, které poskytují dostatečné záruky ochrany a zabezpečení dat.

a) Využívání AI s citlivými a interními daty na JU

V souladu s interními pravidly JU je pro práci s citlivými nebo interními daty JU povoleno využívat výhradně AI službu **Microsoft 365 Copilot**.

Při práci s těmito typy dat je povoleno přistupovat k této službě pouze s využitím univerzitního účtu.

- Osobní účty jsou přísně zakázané.

JU má s firmou Microsoft uzavřenou smlouvu včetně *Data Protection Addendum* (DPA) a dodržuje principy **Enterprise Data Protection (EDP)**. Toto je označeno zeleným štítkem u Vašeho chatu v pravém horním rohu služby Copilot a znamená:

- Data jsou **šifrována při přenosu i v klidu**, izolována na úrovni nájemce (tenant), chráněna přísnými fyzickými a logickými kontrolami a není k nim umožněn přístup třetím stranám.
- Prompty i odpovědi generované Copilotem **nejsou využity k tréninku základního modelu** ani sdíleny mimo organizaci.
- Copilot plně respektuje stávající **přístupová oprávnění**, přejímá **sensitivity labels**, **retention politiky** a dodržuje firemní nastavení a zásady řízení přístupu.

b) Využívání ostatních AI nástrojů na JU

Pro využívání jakýchkoli jiných AI nástrojů než uvedených v bodě **a)** (například ChatGPT, Gemini, Grok a další) platí následující pravidla:

- Tyto nástroje je možné používat bez omezení pro zpracování běžných, nekritických informací, obecných rad, rešerší, překladů a podobných úkolů.
- Je **přísně zakázáno** vkládat do těchto nástrojů **citlivá**, **osobní** nebo **interní data** JU, neboť u nich JU nemá smluvně zajištěnou dostatečnou úroveň zabezpečení ani kontrolu nad tím, jak jsou tato data dále zpracovávána či ukládána.

V případě pochybností o klasifikaci dat nebo vhodnosti použití konkrétního AI nástroje můžete zaslat svůj dotaz na obecnou frontu pro kybernetickou bezpečnost ve službě Servicedesk JU:

- kyber@rt.jcu.cz

c) Napojení AI nástrojů a služeb na data a informace JU

Při napojení AI nástrojů a služeb na datové zdroje uživatele získává daná AI zpravidla plný přístup k těmto informacím. Uživatel JU by měl silně zvážit bezpečnost, nezbytnost a legitimitu každého takového napojení, protože to může způsobit závažná bezpečnostní rizika a potenciálně vést k úniku citlivých či interních dat JU.

Datových zdrojů, na které je možné napojit AI je nespočet. Na JU jsou důležité například tyto datové zdroje:

- Data ze služeb M365 (např. OneDrive úložiště, SharePoint, e-maily, schůzky/kalendář atd.),
- Data uložená na lokálních discích (USB, HDD) a úložištích JU (např. Synology, QNAP atd.),
- Obsah telefonních hovorů, záznamy hovorů a schůzek (včetně MS Teams a jiných komunikačních platforem využívaných univerzitou),
- Výzkumná data, statistická data a další citlivá data vznikající v rámci výzkumných projektů JU,
- Technická data univerzity (např. logy, interní manuály, technická dokumentace infrastruktury atd.).

Je přísně zakázáno připojovat jakékoli AI nástroje a služby na výše zmíněné datové zdroje uživatelů JU, s výjimkou AI nástroje Microsoft 365 Copilot, pro který je smluvně zajištěna ochrana dat – viz bod **a)**.

V případě nutnosti využití jiných AI nástrojů je silně doporučeno si v rámci projektu či výzkumu smluvně zajistit ochranu dat s poskytovatelem AI nástroje či služby.

V případě dotazů můžete zaslat svůj dotaz skrze obecnou frontu pro kybernetickou bezpečnost ve službě Servicedesk JU:

- kyber@rt.jcu.cz

d) Varování ke specifickým AI nástrojům

1. 10. 07. 2025 – DeepSeek

Dle oficiálního varování vydaného NÚKIB představují nástroje společnosti DeepSeek **vysoké kybernetické riziko**. Toto varování se týká všech produktů, služeb a rozhraní API této společnosti, s výjimkou lokálně provozovaných open-source verzí bez připojení k externím serverům.

Důvod varování je nedostatečné zabezpečení přenosu a zpracování dat., sběr informací umožňuje de-anonymizaci uživatelů.

V prostředí JU nejsou oficiálně provozovány žádné lokální instance DeepSeek pro běžné využití. Na některých součástí JU se mohou vyskytovat různé AI nástroje a služby, které jsou ale využívány pouze výzkumníky a zaměstnanci JU v oblasti výzkumu generativní AI a LLM.

Všechny dostupné služby DeepSeek, které uživatelé JU využívají, jsou plně hostovány a spravovány společností DeepSeek nebo jejími přidruženými subjekty. Tato skutečnost výrazně zvyšuje riziko úniku dat a jejich možného zneužití ze strany třetích subjektů či zahraničních státních orgánů.

Z tohoto důvodu platí pro všechny uživatele JU následující zásady a opatření:

- Je **přísně zakázáno** vkládat jakákoli **citlivá**, **osobní** nebo **interní data** JU do nástrojů **DeepSeek**.

- Tento zákaz se rovněž vztahuje na všechna **citlivá výzkumná data** JU a na data JU, se kterými pracují studenti v rámci svých studijních povinností či výzkumných projektů.

Uživatelé jsou povinni dbát zvýšené opatrnosti při práci s těmito nástroji a vždy pečlivě zvažovat typ a citlivost dat, která do nástroje DeepSeek zadávají.

Studenti by měli zvláště důkladně zvážit, zda je zasílání konkrétních informací do nástrojů DeepSeek opravdu nezbytné a bezpečné.

- Porušení tohoto zákazu bude posuzováno jako závažné narušení pravidel ochrany informací na JU a může vést k disciplinárnímu opatření dle platných interních předpisů JU.