Ambis Univerzita

CVP – P – 14	Výtisk č.:
	Počet stran: 11

Účinnost od:	**Doba platnosti:**	**Rozsah platnosti:**
1. 8. 2026	do odvolání	Ambis Univerzita, a. s.

Č. j.: AMBIS-IS/19086/2026/175779/AMBIS-1

Název dokumentu:

Informační bezpečnost AI technologií

Schvaluji:

Dr. Martina Mannová
Digitálně podepsal Dr. Martina Mannová
Datum: 2026.07.17 15:00:39 +02'00'

Dr. rer. nat. Martina Mannová
členka představenstva

Radek Stavinoha
Digitálně podepsal Radek Stavinoha
Datum: 2026.07.21 11:11:58 +02'00'

Radek Stavinoha
člen představenstva

Počet příloh:	1	**Názvy příloh:** příloha č. 1 – šablona pro posouzení rizika použití AI.
Číslo vydání:	1.	
První		**Nahrazuje:** ---

Čl. I
Účel dokumentu

(1) Tato směrnice stanovuje pravidla pro bezpečné a kontrolované využití technologií umělé inteligence ve společnosti Ambis Univerzita, a.s. (dále jen „**Ambis**“). Cílem těchto pravidel je minimalizace rizik spojených s užitím AI technologií a zajištění souladu s platnou legislativou.

Čl. II
Vymezení pojmů

(1) **AI** – Technologie a systémy umělé inteligence.

(2) **AI Act** – Nařízení Evropského parlamentu a rady (EU) č. 2024/1689 ze dne 13. června 2024, kterým se stanoví harmonizovaná pravidla pro umělou inteligenci a mění nařízení (ES) č. 300/2008, (EU) č. 167/2013, (EU) č. 168/2013, (EU) 2018/858, (EU) 2018/1139 a (EU) 2019/2144 a směrnice 2014/90/EU, (EU) 2016/797 a (EU) 2020/1828 (akt o umělé inteligenci).

(3) **AI technologie** – systémy založené na strojovém učení, velkých jazykových modelech nebo automatizovaných rozhodovacích procesech.

(4) **GPAI (General Purpose AI)** – univerzální modely (např. generativní LLM) podle AI Act.

(5) **LLM (Large Language Model)** - model umělé inteligence trénovaný na velkém množství vzorových dat, který dokáže generovat, analyzovat a zpracovávat text podobně jako člověk.

(6) **Halucinace AI modelu** – AI technologie se snaží předvídat další krok a někdy kvůli tomu dochází k vytvoření nepravdivé informace, vymyšlených detailů nebo logicky nesprávných odpovědí

(7) **Malicious AI** – škodlivá AI platforma, která je zneužívána pro kybernetické útoky nebo odcizení informací

(8) **Deepfake** – digitálně vytvořený nebo upravený obsah (obraz, video nebo audio), které pomocí věrně napodobuje skutečnou osobu nebo situaci tak, že může být obtížné rozeznat, že jde o falzifikát.

(9) **Systém vysokého rizika** – AI využívající se v HR, rozhodování o lidech, monitoringu osob či dalších procesech (dle EU AI Act)

(10) **Riziková využití** – jakékoli použití AI, které může ovlivnit osoby, bezpečnost nebo kritické procesy, případně jakékoli využití podle definice EU AI Act Annex III (Systémy vysokého rizika)

(11) **PII** – Personal Identifiable Information – Osobní údaje o fyzických osobách s výjimkou veřejných údajů této povahy (např. jména autorů)

(12) **Kooperativní prostředí** – prostředí Evropské Unie a NATO

(13) **Pračka dat** – non-AI nástroj nebo proces, který vyfiltruje data před jejich vložením do AI nástroje; působí jako ochrana před nechtěným zpracováním osobních údajů a jiných citlivých dat

(14) **MKB** – Manažer kybernetické bezpečnosti

(15) **DPO** – Data Protection Officer – Pověřenec pro ochranu osobních údajů

(16) **Whitelist / Blacklist** – seznam povolených a zakázaných technologií dle příslušného bezpečnostního standardu

Čl. III
Legislativa a regulace

(1) Tento článek shrnuje legislativní a normativní požadavky, které určují limity a povinnosti při využívání AI technologií ve společnosti.

(2) Regulace Evropské unie:

a. AI Act je regulatorní nařízení Evropské unie, které stanovuje požadavky na vývoj, využívá a bezpečnost AI technologií.

(3) Relevantní legislativa v České republice

a. Zákon o umělé inteligenci – připravovaná implementace AI Act v ČR,
b. Zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**ZoKB**“),
c. Zákon č. 110/2019 Sb., o zpracování osobních údajů.

Čl. IV
Předpokládané způsoby využití AI na Ambis

(1) Tento článek vymezuje povolené způsoby využití (scénáře) AI technologie na Ambis.

(2) Uživatelské scénáře:

- vyhledávání obecných informací z veřejných zdrojů pomocí LLM,
- vyhledávání interních informací v uživateli dostupných dokumentech, interních systémech a reportech,
- generování obsahu v podobě textů, obrázků, videa, syntetických dat, překladů apod.,
- využití AI při řešení projektů a analytických úloh,
- využití AI při zpracování zadání, hodnocení nebo přípravě výstupů.

(3) Systémové scénáře:

- automatizace interních procesů (HR, obchod, logistika, nákup apod.),
- automatizace zákaznických procesů,
- automatizace zpracování dokumentů,
- automatizace kybernetické ochrany a aktivní obrany.

(4) Vědecké scénáře:

- Využití AI jako zdroje informací při řešení projektu,
- Využití AI ke zpracování zadání, řešení projektu či jeho hodnocení a zpracování závěrečné zprávy,
- Samostatný projekt o technologii AI (vazba na klasifikaci organizace dle ZoKB).

Čl. V
Identifikovaná rizika při využívání AI

(1) Níže uvedená rizika je nutné řídit z hlediska kybernetické bezpečnosti.

(2) Obecná rizika:

a. nevědomé použití chráněného obsahu (autorská práva, licence, obchodní tajemství),
    - nízká kvalita výstupu:
    - zkreslená nebo manipulovaná data,
    - technologie naučená na chybných vstupních datech bude generovat chybné výstupy,

- nekompletní data – technologie nemusí vnímat priority stejně jako uživatel a může vynechat podstatné informace,
- halucinace AI technologie,

b. systémová, technologická a regulatorní omezení použité AI technologie.

(3) Uživatelská rizika:

a. riziko souhlasu – nekritické přijímání výstupů AI („AI souhlasí se vším“),
b. riziko zahlcení informacemi – velké množství informací uživatele snadno svede z cesty („králičí nora“),
c. riziko „AI-AI smyčky“ – uživatelé si navzájem posílají informace generované a analyzované pouze AI technologií, což vede to k degradaci obsahu a ztrátě přehledu o řešeném problému.

(4) Organizační rizika

a. ohrožení ochrany osobních údajů,
b. ohrožení dobrého jména společnosti nebo autora,
c. kompromitace důvěrných nebo strategických informací,
d. spuštění vědeckého projektu v oblasti AI se zaměřením, které způsobí přechod do Vyššího režimu podle ZoKB.

(5) Systémová rizika

a. Interní únik dat – internímu pracovníkovi je AI technologií poskytnuta informace, která mu má být nedostupná (např. z důvodu pracovního zařazení),
b. externí úniky dat:
   - učení modelu na interních datech a jejich následné zveřejnění může ohrozit interní inforace, osobní údaje nebo chráněný obsah,
   - AI technologie zaměřená na špionáž může systematicky krást informace,
c. zneužití uživatelského účtu k AI technologii:
   - odcizení nebo zveřejnění chráněných informací,
   - získání informací pro kybernetický útok,
d. malicious AI:
   - supply-chain útoky na free nebo komunitní platformy (vytěžení dat, doručení malware),
   - platformy zaměřené na kybernetické útoky,
   - platformy zaměřené na odcizení informací,
e. kapacitní limity – nedostatek prostředků pro provoz technologie (např. nedostatečný prostor pro logy, nevyhovující infrastruktura).

Čl. VI
Rozsahy řízení rizik AI technologií

(1) Ambis na základě očekávaných způsobů využití a identifikovaných rizik rozhodla o řízení těchto rizik ve 4 rozsazích (scope). Rozsahy jsou samostatně definovány a pro každý z nich jsou stanovená nutná opatření z hlediska kybernetické bezpečnosti. Zařazení zpracování do konkrétního rozsahu se řídí aktuálním stavem zpracovávaných dat, účelem a dopadem použití, zařazení se tedy může v průběhu zpracování změnit.

(2) Externí (veřejný) rozsah

- ve veřejném rozsahu probíhá zpracování dat pouze z veřejných zdrojů, nebo ze zdrojů, které již byly oprávněně zveřejněny.využitá AI technologie musí pocházet z kooperativního prostředí (EU, NATO).

(3) Interní rozsahy:

a. BĚŽNÝ ROZSAH:

- v běžném rozsahu je možná práce s daty:
  - z interních a veřejných zdrojů a při kterém
  - nedochází ke zpracování PII,
  - využitá AI technologie musí pocházet z kooperativního prostředí (EU, NATO).

b. RIZIKOVÝ ROZSAH

- pouze v Rizikovém rozsahu je možné:
  - zpracování dat včetně PII
  - anebo využít AI k rozhodování o osobách,
  - využitá AI technologie
    - musí pocházet z kooperativního prostředí (EU, NATO),
    - musí respektovat nastavená uživatelská a systémová oprávnění v rámci úložišť dat (databáze, souborová úložiště).

c. VĚDECKÝ ROZSAH

- AI technologie je předmětem vědeckého projektu a využití neodpovídá rozsahu a ani b.

Čl. VII
Základní pravidla pro využívání AI technologií

Ambis stanovuje tyto povinné zásady, kterými se musí řídit všichni uživatelé AI technologií:

a. Uživatelé mohou používat pouze interně schválené AI technologie (tzv. AI Whitelist).

b. Pro každou schválenou AI technologii musí uživatelé respektovat pravidla jejího využití, především seznam typů dat, které do ní mohou vkládat.

c. Uživatelé mají zákaz vkládat následující typy údajů do neschválených AI platforem:

- přihlašovací údaje,
- osobní údaje,
- chráněný obsah – informace chráněné obchodním tajemstvím, autorskou ochranou nebo licenčním ujednáním.

d. Uživatelé nesmí používat zakázané AI technologie (tzv. AI Blacklist). Především nesmí:

- instalovat nebo používat vzdáleně tyto technologie na jakémkoli firemním zařízení,
- vkládat jakákoli firemní data do těchto technologií na jiných zařízeních (např. soukromé PC, telefon).

e. Uživatelé mají povinnost ověřovat výstupy AI, především s ohledem na správnost a ochranu citlivých informací.

f. Uživatelé nesmí neověřený výstup z AI technologie publikovat jako řízený nebo jinak autoritativní dokument.

g. Výstupy vytvořené nebo podstatně upravené pomocí AI se označují v rozsahu vyžadovaném AI Actem nebo jiným právním předpisem, zejména jde-li o deepfake obsah nebo AI generovaný či upravený text publikovaný za účelem informování veřejnosti o věcech veřejného zájmu. Ambis nad rámec zákonné povinnosti přiměřeně označuje i další veřejně publikované výstupy a studijní, metodické, výukové, odborné nebo obdobné materiály, pokud AI významně ovlivnila jejich obsah, závěry nebo výslednou podobu. Označení musí být srozumitelné, přiměřené formátu a tím není dotčena povinnost ověřovat výstupy AI ani odpovědnost autora nebo garanta za jejich správnost a odbornou kvalitu.

Čl. VIII
Organizační a procesní opatření

(1) Pro prověření a následné schválení AI technologie se zavádí tento **Schvalovací proces**:

a. předběžný návrh využití s definicí přínosů,

b. posouzení dodavatele,

c. analýza rizik AI technologie,

d. záznam do Evidence AI technologií,

e. schválení využití technologie MKB.

(2) Podle způsobu využití (běžné, interní, rizikové, vědecké) může být proces rozšířen a další položky (např. specifická analýza rizik, DPIA, schválení DPO).

(3) V rámci přípravy předběžného návrhu může být navrhovatelem provedeno testování jakékoli AI technologie, pokud budou dodrženy následující podmínky:

a. nejedná se o technologii uvedenou na Blacklistu,

b. testování se bude přednostně provádět mimo interní infrastrukturu Ambis (cloudové prostředí),

c. nebo v interní infrastruktuře ve spolupráci s provozním / IT oddělením,

d. pro testování budou použita syntetická data,

e. budou dodrženy všechny požadavky kybernetické bezpečnosti ve stejném rozsahu, jako v produkčním prostředí.

(4) Schválená technologie bude zařazena v kategorii Whitelist a není nutné ji znovu posuzovat při schvalování nového projektu.

(5) Neschválená technologie může být zařazena do kategorie Blacklist. Technologie v této kategorii se nesmí využívat ve Veřejném, Běžném nebo Rizikovém rozsahu.

(6) Manažer kybernetické bezpečnosti zajistí vedení **Evidence využívaných AI nástrojů** a pravidelné sledování jejich kyberneticko-bezpečnostních parametrů minimálně v rozsahu:

a. dodavatelský řetězec,

b. zranitelnosti,

c. certifikace,

d. lokalita dat,

e. whitelist/blacklist.

(7) Na zajištění bezpečného používání AI technologií včetně vzdělávání zaměstnanců Ambis se podílí AI Lab, který je organizačně začleněn pod prorektorát pro strategii a rozvoj Ambis.

Čl. IX
Obecné využití AI technologie

(1) Tato část stanovuje minimální technické požadavky, které musí splňovat všechny povolené AI technologie.

(2) Všechny AI systémy musí být při užití v Ambis nasazené s ochranou autentizace:

a. Uživatelské / Interaktivní přihlášení:
   - silných hesel a multifaktorové autentizace (MFA)
   - nebo využití SSO autentizace propojené s platformou Microsoft365.

b. Systémové přihlášení (API):
   - velmi silná hesla,
   - ochrana certifikáty,
   - šifrovaný přenos dat od počátku autentizace.

(3) MKB schvaluje využití technologie na základě předběžného záměru využití dle článku VIII.

(4) Posouzení rizik využití jakékoli AI technologie musí brát do úvahy ostatní technologie a data zapojené v celém procesu zpracování dat.

Čl. X
AI technologie ve Veřejném rozsahu

Pro využití AI technologie ve Veřejném rozsahu se zavádí tyto požadavky na kybernetickou bezpečnost:

a. bezpečná autentizace,
b. AI technologie musí být uvedena ve Whitelistu s autorizací pro Veřejný rozsah nebo vyšší,
c. použití „pračky dat“ – filtru na PII a citlivá interní data,
d. schválení MKB pro:
   - záměr projektu,
   - rozsah zpracovávaných dat
   - schválení bezpečnostního rozsahu.

Čl. XI
AI technologie v Běžném rozsahu

Pro využití AI technologie v Běžném rozsahu se zavádí tyto požadavky na kybernetickou bezpečnost:

a. bezpečná autentizace,
b. autorizace přístupu k interním informacím,
c. AI technologie musí být uvedena ve Whitelistu s autorizací pro Běžný rozsah nebo vyšší,

d. AI technologie nesmí v rámci učení poskytovat zpracovávaná data do veřejných modelů a procesů. Může se učit na zpracovávaných datech za účelem zkvalitnění interního zpracování dat.
e. použití „pračky dat“ – filtru na PII a citlivá interní data,
f. schválení MKB pro:
g. záměr projektu,
   - rozsah zpracovávaných dat,
   - schválení bezpečnostního rozsahu,
   - využitou technologii.

Čl. XII
AI technologie v Rizikovém rozsahu

(5) Jakékoli využití AI technologie v těchto oblastech nebo procesech je považováno za vysoce rizikové:
   a. řízení lidských zdrojů,
   b. zákaznické procesy se zpracováním osobních dat zákazníků (např. přijímací řízení, hodnocení studentů),
   c. rozhodování o fyzických osobách (pracovníci, zákazníci),
   d. monitoring fyzických osob.

(6) Pro využití AI technologie v Rizikovém rozsahu se zavádí tyto požadavky na kybernetickou bezpečnost:
   a. bezpečná autentizace,
   b. autorizace přístupu k interním informacím,
   c. AI technologie musí být uvedena ve Whitelistu s autorizací pro Rizikový rozsah,
   d. AI technologie nesmí v rámci učení poskytovat zpracovávaná data do veřejných modelů a procesů. Může se učit na zpracovávaných datech za účelem zkvalitnění interního zpracování dat.
   e. kontrola rozsahu zpracovávaných PII a balanční test a konzultace s DPO,
   f. použití „pračky dat“ – filtru na PII, které nejsou předmětem zpracování,
   g. povinné pilotní testování,
   h. schválení MKB pro:
      - záměr projektu,
      - rozsah zpracovávaných dat,
      - schválení bezpečnostního rozsahu,
      - využitou technologii.

(7) Další požadavky:
   a. Procesně musí být zajištěno informování dotčené osoby o rozhodování pomocí AI technologie.
   b. 1x ročně musí být provedena kontrola provozu a analýzy rizik,
   c. musí být zajištěno logování a archivace logů minimálně za 1 rok zpětně,
   d. pro využití k rozhodování o fyzických osobách musí být transparentně zajištěna auditovatelnost procesu rozhodování po dobu platnosti rozhodnutí nebo minimálně po dobu 1 roku,
   e. musí být stanoveny postupy pro obnovu technologie,

f. musí být stanoven postup reakce na incidenty.

(8) Schvalovací proces se pro Rizikové využití rozšiřuje o tyto body:

a. pro každý způsob využití (samostatný projekt nebo proces) musí být provedena:

- specifická analýzy rizik a návrh bezpečnostních opatření,
- posouzení dopadu na ochranu osobních údajů (DPIA),
- posouzení dopadu na základní práva osob (FRIA) v případě, že dochází k automatizovanému rozhodování AI technologií,
- a stanovení způsobu a četnosti lidské kontroly a validace výstupů.

b. Pro každé rizikové využití musí být zajištěn souhlas DPO s konkrétním zpracováním.

c. DPO zajistí aktualizaci záznamů o způsobech zpracování osobních údajů.

d. pro každé rizikové využití musí být zajištěn souhlas MKB.

Čl. XIII
AI technologie ve Vědeckém rozsahu

(1) Pro využití AI technologie ve vědeckém rozsahu se zavádí tyto požadavky na kybernetickou bezpečnost:

a. bezpečná autentizace,

b. AI technologie bez omezení,

c. AI technologie nesmí mít přístup k interním datům a systémům,

d. AI technologie musí být provozována v prostředí separovaném od interních dat a systémů,

e. použití „pračky dat“ – filtru na PII a citlivá firemní data,

f. Schválení MKB pro:

- záměr projektu,
- rozsah zpracovávaných dat,
- schválení bezpečnostního rozsahu,
- separaci.

(2) MKB provede posouzení projektu s ohledem na možnost zařazení Regulovaných služeb do režimu vyšších povinností podle ZoKB.

Čl. XIV
Práva fyzických osob

Ve vztahu k AI technologiím musí být respektována práva fyzických osob definovaná směrnicí GDPR a nad tento obecný závazek zavádí tato práva:

- právo pracovníka odmítnout využívání technologií umělé inteligence,
- právo fyzické osoby být předem informován o využití AI v rizikovém rozsahu,
- právo fyzické osoby na vysvětlení role AI v rozhodnutí,
- právo fyzické osoby odmítnout proces automatizovaného rozhodování.

Čl. XV
Zakázané technologie a postupy

Technologie a praktiky, které organizace nesmí používat:

- sociální skórování fyzických osob,

- biometrický dohled a identifikace osob,
- biometrická kategorizace osob,
- rozpoznávání emocí osob na pracovišti nebo ve vzdělávacím prostředí,
- generování deepfake obsahu bez souhlasu dotčené osoby,
- autonomní rozhodování AI bez lidského dohledu,
- využívání AI k manipulaci nebo klamání uživatelů,
- využívání AI ke zneužití zranitelnosti osob (např. děti, senioři),
- využívání AI pro predikci kriminality jednotlivců na základě profilování
- využívání free/community AI nástrojů pro zpracování interních dat,
- technologie uvedené na Blacklist seznamu a jakékoli technologie a nástroje z nich odvozené (chatboty, aplikace, API, embedded funkce v aplikacích, pluginy, odvozené komerční i open-source modely).

Výjimky ze zakázaných technologií a postupů může schválit MKB v případě, že požadovaná výjimka neodporuje platné legislativě.

Čl. XVI
Školení a povinnosti uživatelů

Pravidla pro školení uživatelů v oblasti bezpečného využívání AI technologií:

- organizace školení je v kompetenci personálního oddělení ve spolupráci s provozním oddělením a MKB.
- školení musí zahrnovat oblast AI gramotnosti, zejména:
- porozumění principům fungování AI systémů,
- schopnost identifikovat rizika, omezení a možné dopady AI,
- zásady bezpečného a odpovědného používání AI,
- porozumění zavedeným pravidlům používání AI systémů.
- školení může být součástí obecného školení o kybernetické bezpečnosti,
- každý uživatel AI technologie musí absolvovat vstupní školení a potom pravidelně 1x za 2 roky.

Čl. XVII
Přílohy

(1) příloha č. 1 – šablona pro posouzení rizika použití AI.

Čl. XVIII

Související předpisy

(1) Regulace Evropské unie:
   a. AI Act je regulatorní nařízení Evropské unie, které stanovuje požadavky na vývoj, využívá a bezpečnost AI technologií.

(2) Relevantní legislativa v České republice
   a. Zákon o umělé inteligenci – připravovaná implementace AI Act v ČR,
   b. Zákon č. 264/2025 Sb., o kybernetické bezpečnosti (dále jen „**ZoKB**“),
   c. Zákon č. 110/2019 Sb., o zpracování osobních údajů.

(3) Směrnice o informačním systému

(4) Bezpečnostní standardy

Čl. XIX
Závěrečná ustanovení

(1) Projekty, které jsou ovlivněny touto směrnicí a které jsou realizovány ke dni účinnosti této směrnice, musí být uvedeny do souladu s ní nejpozději do 1 roku od počátku její účinnosti.

(2) Všichni zaměstnanci jsou povinni se s tímto vnitřním předpisem seznámit. Za seznámení zaměstnanců jsou odpovědní vedoucí zaměstnanci v oblastech své působnosti.

(3) Tento předpis je zveřejněn na Úřední desce Ambis a všichni členové akademické obce a další zaměstnanci Ambis mají právo kdykoli do něj nahlížet.

(4) V tomto předpisu je pro označení zúčastněných osob používáno genderově neutrální maskulinum.

(5) Tento předpis je platný ode dne podpisu, jeho účinnost je uvedena na titulní straně.

Čl. XX

Rozdělovník

(1) Výtisk č. 1 – správcovský výtisk

(2) Výtisk č. 2 – výtisk na zápůjčku