Politika používání umělé inteligence (AI Usage Policy)

Verze: 1.0
Platnost od: [DATUM]
Schválil: [JMÉNO A POZICE]
Další revize: [DATUM + 12 MĚSÍCŮ]

1. Účel a rozsah

Tato politika stanovuje pravidla pro používání nástrojů a služeb umělé inteligence (AI) v [NÁZEV ORGANIZACE]. Cílem je zajistit bezpečné, etické a efektivní využití AI technologií při současném dodržení právních požadavků a ochrany citlivých dat.

Vztahuje se na: - Všechny zaměstnance, dodavatele a externí spolupracovníky - Všechny AI nástroje, služby a aplikace používané v organizaci - Zpracování osobních a obchodních dat pomocí AI

2. Schválené AI nástroje

2.1 Oficiálně schválené nástroje

- **ChatGPT Enterprise/Teams** - pro textové úkoly s business licencí
- **Microsoft Copilot 365** - integrované do Office prostředí
- **GitHub Copilot Business** - pro programování s enterprise ochranou
- **[DALŠÍ NÁSTROJE...]**

2.2 Podmínečně povolené nástroje

Nástroje vyžadující předchozí schválení IT a Legal oddělení: - Claude (Anthropic) - pouze s business účtem - Google Bard/Gemini - pouze workspace integrace - **[DALŠÍ NÁSTROJE...]**

2.3 Zakázané nástroje

- Bezplatné verze AI nástrojů bez enterprise SLA
- Nástroje bez jasných podmínek zpracování dat
- AI služby hostované mimo EU bez adequate protection

3. Povolená a zakázaná použití

[ANO] POVOLENO:

- **Produktivita:** Shrnutí meetingů, příprava prezentací, brainstorming
- **Komunikace:** Úprava textů, překlady, korektura gramatiky
- **Analýza:** Zpracování veřejných dat, market research, trend analysis
- **Programování:** Code review, dokumentace, debugging (bez proprietary kódu)

[NE] ZAKÁZÁNO:

- **Citlivá data:** Zpracování osobních údajů, finanční data, zdravotní záznamy
- **Obchodní tajemství:** Strategické plány, ceníky, neveřejné informace o klientech
- **Bezpečnostní informace:** Hesla, API klíče, systémové konfigurace
- **Právní dokumenty:** Smlouvy, právní stanoviska (bez schválení legal týmu)
- **HR data:** Osobní hodnocení, mzdy, disciplinární řízení

4. Zabezpečení a ochrana dat

4.1 Data classification

- **Veřejná data:** Lze zpracovávat všemi schválenými nástroji
- **Interní data:** Pouze enterprise nástroje s DPA
- **Důvěrná data:** Speciální schválení + on-premises řešení
- **Vysoce citlivá:** Zakázáno zpracování externími AI

4.2 Technická opatření

- Použití firemních účtů s centrální správou
- Pravidelné audity používaných nástrojů a přístupů
- Implementace DLP (Data Loss Prevention) rules
- Monitoring a logging AI aktivit

4.3 Data retention a deletion

- Pravidelné mazání chat historie (max. 90 dní)
- Dokumentace dlouhodobě ukládaných AI výstupů
- Proces pro data subject requests (GDPR čl. 17)

5. Etické zásady

5.1 Transparentnost

- Označování AI-generovaného obsahu (kde je to relevantní)
- Informování klientů o použití AI v službách
- Nediskreční označení AI asistence v komunikaci

5.2 Lidský dohled

- Všechny kritické rozhodnutí schvaluje člověk
- AI slouží jako nástroj, ne náhrada lidského úsudku
- Regular human review klíčových AI výstupů

5.3 Bias a fairness

- Testování AI nástrojů na diskriminační tendence
- Diverzifikace zdrojů a nástrojů
- Reporting mechanismus pro problematické výstupy

6. Odpovědnosti a role

6.1 Zaměstnanci

- Dodržování této politiky a školících materiálů
- Hlášení bezpečnostních incidentů nebo pochybností
- Udržování aktuálních znalostí o AI nástrojích

6.2 IT oddělení

- Správa schválených nástrojů a přístupů
- Monitoring compliance a bezpečnostní incident response

- Technická podpora a školení

6.3 Legal/Compliance

- Interpretace právních požadavků
- Hodnocení nových AI nástrojů z pohledu compliance
- Řešení data subject requests

6.4 Management

- Schvalování nových AI investic a nástrojů
- Stanovení business priorities pro AI usage
- Escalation point pro policy violations

7. Incident reporting a sanctions

7.1 Hlášení incidentů

Okamžitě hlásit: - Podezření na data breach prostřednictvím AI - Neautorizované použití AI nástrojů - Výstupy AI obsahující bias nebo diskriminaci

Kontakt: [IT-SECURITY@COMPANY.COM] nebo [PHONE NUMBER]

7.2 Sankce

- **První porušení:** Školení a písemné upozornění
- **Opakované porušení:** Omezení přístupu k AI nástrojům
- **Závažné porušení:** Disciplinární řízení dle HR policy

8. Školení a awareness

8.1 Povinné školení

- Onboarding pro všechny nové zaměstnance
- Roční refresh training pro všechny uživatele
- Specialized training pro power users a administratory

8.2 Materiály

- Interní knowledge base s praktickými příklady
- Regular updates o nových nástrojích a hrozbách
- Q&A session s IT a Legal týmy

9. Policy updates a review

Tato politika bude: - Revidována každých 12 měsíců nebo při významných změnách - Aktualizována při zavedení nových nástrojů - Komunikována všem dotčeným stranám při změnách

Kontakt pro otázky: [AI-GOVERNANCE@COMPANY.COM]

Tento dokument je template pro interní použití. Přizpůsobte jej specifickým potřebám vaší organizace a konzultujte s právním oddělením.