KOVOPROJEKTA
ENGINEERS & CONTRACTORS

POLITIKA KYBERNETICKÉ BEZPEČNOSTI

Účel politiky

Účelem této politiky je stanovit zásady a pravidla pro bezpečné a efektivní využívání digitálních technologií za účelem ochrany dat, zabezpečení kontinuity procesů a minimalizace kybernetických rizik. Současně dokument podporuje etické a odpovědné nasazení umělé inteligence ve společnosti a dbá na to, aby všichni zaměstnanci dodržovali zásady a postupy přijatelného používání nástrojů umělé inteligence. V případě porušení těchto zásad stanovuje politika také vhodná disciplinární opatření i konkrétní kroky minimalizace dopadů, obnovení bezpečnosti a prevenci opakování.

Rozsah působnosti

Tato politika se vztahuje na:

- Všechny zaměstnance společnosti bez ohledu na pracovní zařazení, jakož i na externí spolupracovníky, dodavatele a partnery, kteří v rámci své činnosti přistupují k digitálním technologiím, datům nebo systémům společnosti.
- Veškeré digitální prostředky, systémy a nástroje využívané při projektování, řízení zakázek, komunikaci, datovém sdílení a implementaci umělé inteligence – včetně firemních zařízení (PC, mobilní telefony, servery), cloudových služeb, komunikačních nástrojů, specializovaného softwaru a AI platforem.
- Jakékoli informace, které nejsou výslovně označeny jako vlastnictví jiných stran a které jsou přenášeny nebo ukládány v IT zdrojích společnosti (včetně e-mailů, textových a chatových zpráv a souborů)
- Všechny systémy, nástroje nebo služby včetně nástrojů vybavených generativní AI (např. ChatGPT, Copilot apod.), které vytvářejí textový, obrazový nebo jiný obsah na základě vstupních dat.

Zásady jsou závazné jak při práci v prostorách společnosti, tak při práci na dálku (home office, služební cesty) a platí i při využívání osobních zařízení v rámci modelu BYOD (Bring Your Own Device), pokud jsou používána pro pracovní účely.

Výjimky z politiky

V odůvodněných případech mohou být z této politiky uděleny výjimky, a to pouze:

- Na základě písemného schválení odpovědné osoby (vedení společnosti);
- V rozsahu nezbytném pro zajištění provozní efektivity, bezpečnostního testování, vývoje nebo specifických projektových požadavků;
- Po vyhodnocení rizik a posouzení dopadů na bezpečnost, ochranu osobních údajů a právní soulad.

Každá výjimka musí být řádně zdokumentována včetně důvodu, rozsahu, doby platnosti a zodpovědné osoby. Výjimky nesmí být chápány jako precedent a nesmí ohrozit integritu a bezpečnost systémů či dat společnosti.

Výjimky, které jsou klasifikovány jako vysoce rizikové budou zaznamenány do registru rizik společnosti.

Definice pojmů

Pro účely této politiky se používají následující definice:

- Digitální technologie – jakékoli hardwarové nebo softwarové nástroje, systémy nebo zařízení, které umožňují zpracování, uchovávání, přenos nebo sdílení dat (např. počítače, servery, mobilní zařízení, cloudové služby, CAD/BIM nástroje apod.).

- Umělá inteligence (AI) – technologie schopné vykonávat úkoly, které obvykle vyžadují lidskou inteligenci, včetně strojového učení, generativních modelů, rozpoznávání vzorců, analýzy přirozeného jazyka a rozhodovacích systémů. Do této kategorie spadají např. ChatGPT, Copilot, ale i prediktivní návrhové systémy.
- Systémy umělé inteligence – veškeré softwarové nástroje nebo služby vybavené funkcionalitou AI, zejména ty, které generují texty, obrázky, návrhy, analýzy nebo rozhodnutí bez lidského zásahu.
- Důvěrné informace– jakékoli informace, jejichž neoprávněné zveřejnění, ztráta nebo zneužití by mohly poškodit zájmy společnosti nebo třetích stran, včetně osobních údajů, obchodního tajemství, technické dokumentace, projektových návrhů, finančních údajů, klientských kontaktů apod.
- Přijatelné použití – způsob využívání digitálních technologií a nástrojů AI, který je v souladu s touto politikou, s etickými a právními standardy a se strategickými cíli společnosti.
- BYOD (Bring Your Own Device) – model, kdy zaměstnanec používá pro výkon pracovních úkolů vlastní zařízení (např. notebook, mobilní telefon), přičemž i tato zařízení podléhají pravidlům politiky.
- Phishing – technika sociálního inženýrství, při níž se útočník snaží získat zejména důvěrné informace (např. přihlašovací údaje, finanční data) podvodným způsobem, obvykle prostřednictvím falešných e-mailů, webových stránek nebo zpráv.
- Kompromitovaný účet – uživatelský účet, ke kterému získal neoprávněný přístup třetí subjekt (např. hacker), často v důsledku slabého hesla, phishingového útoku nebo nedostatečného zabezpečení.
- Anonymizace dat – proces úpravy dat tak, aby již nebylo možné identifikovat konkrétní fyzické osoby, a to ani nepřímo, čímž se eliminuje povinnost jejich ochrany podle legislativy o ochraně osobních údajů (např. GDPR).
- Zabezpečená komunikace – jakákoli výměna informací, která je chráněna šifrováním nebo jiným způsobem, aby se zabránilo neautorizovanému přístupu či úniku dat (např. používání VPN, šifrovaných e-mailů apod.).
- Incident kybernetické bezpečnosti / Bezpečnostní incident – jakákoli událost, která ohrožuje důvěrnost, integritu nebo dostupnost systémů a dat, včetně pokusu o neoprávněný přístup, šíření škodlivého softwaru nebo ztráty dat.
- Firemní data – veškeré informace vytvořené, získané nebo uchovávané v rámci činnosti společnosti, bez ohledu na formu (text, obraz, výkres, zvuk) či médium (cloud, pevný disk, papírový dokument), které mají hodnotu pro provoz firmy nebo jejích klientů.
- Etické použití umělé inteligence – nasazení a využívání AI nástrojů způsobem, který respektuje lidskou důstojnost, transparentnost, nediskriminační přístup, ochranu soukromí a odpovědnost za výstupy, které AI generuje.
- Role a odpovědnosti – specifické povinnosti přidělené jednotlivým zaměstnancům nebo rolím v organizaci ve vztahu k naplňování zásad této politiky (např. IT správce dohlíží na zabezpečení systémů, projektový manažer odpovídá za správné sdílení dat v rámci projektů apod.).
- Zásada minimálního přístupu – princip, podle něhož mají zaměstnanci přístup pouze k těm datům a systémům, které jsou nezbytné k výkonu jejich konkrétní pracovní činnosti.
- Bezpečnostní opatření – soubor technických, organizačních a procesních kroků, jejichž cílem je chránit společnost před kybernetickými hrozbami, ztrátou dat, zneužitím nástrojů či narušením provozu.
- Veřejně dostupné AI systémy – Online dostupné nástroje umělé inteligence, které jsou provozovány třetími stranami a mohou být využívány širokou veřejností bez smluvního vztahu se společností. Typicky není zajištěna úplná kontrola nad tím, jak jsou vstupní data zpracována, uložena nebo využita.

Role a odpovědnosti

Za dodržování této politiky jsou odpovědní všichni zaměstnanci společnosti. Klíčové role a jejich odpovědnosti jsou definovány následovně:

- Vedení společnosti
  Schvaluje tuto politiku, uděluje případné výjimky a zajišťuje, že zásady jsou v souladu s celkovou strategií firmy.
- IT oddělení / správce systémů
  Zajišťuje bezpečný provoz digitálních technologií, pravidelné aktualizace a monitoring systémů, spravuje přístupová práva a poskytuje technickou podporu.
- Projektoví manažeři
  Dbají na to, aby projektová dokumentace i komunikace v týmu probíhala bezpečným způsobem a aby použití digitálních technologií bylo v souladu s touto politikou.
- Bezpečnostní a compliance pověřenec (pokud je jmenován)
  Koordinuje školení, vyhodnocuje rizika, sleduje dodržování zásad a vede registr bezpečnostních incidentů a výjimek.
- Zaměstnanci
  Jsou povinni jednat v souladu s touto politikou, absolvovat školení a neprodleně hlásit jakékoli bezpečnostní incidenty či porušení pravidel.

Zásady přijatelného používání digitálních technologií a systémů umělé inteligence

Zaměstnanci jsou povinni používat digitální technologie a nástroje umělé inteligence v souladu s následujícími zásadami:

1. Bezpečné přihlašování a správa účtů

- Používání silných a unikátních hesel
- Nepřihlašujte se ke službám společnosti z veřejných nebo nedůvěryhodných zařízení.
- Přístupové údaje jsou osobní a nesmí být sdíleny.

2. Práce s daty a dokumenty

- Pracovní soubory mohou být ukládány výhradně do schválených úložišť.
- Není dovoleno posílat projektovou dokumentaci nebo jiné důvěrné informace přes veřejné platformy nebo jinou formou nezabezpečené komunikace.
- Důvěrné informace je nutné chránit před zneužitím, neoprávněným přístupem a ztrátou.

3. Používání AI nástrojů

- Nástroje umělé inteligence lze využívat pouze pro účely, které odpovídají přidělené práci a jsou v souladu s touto politikou.
- Není dovoleno vkládat citlivé nebo důvěrné informace společnosti do veřejně dostupných AI systémů (např. bez předchozího schválení nebo ochranných opatření).
- Výstupy generované AI je třeba vždy ověřit – zaměstnanec nese odpovědnost za jejich správnost a vhodnost použití.
- Obsah generovaný umělou inteligencí, který je sdílen nebo publikován, musí mít jasně označen jako výstup Al (např. vodoznakem, poznámkou v textu apod.), pokud je sdílen nebo prezentován jménem společnosti.

4. Používání zařízení a aplikací

- Instalace softwaru smí být prováděna pouze prostřednictvím schválených zdrojů a ve spolupráci s IT oddělením.
- Osobní zařízení v režimu BYOD musí být zabezpečena a splňovat firemní požadavky.
- Firemní zařízení nesmí být používána k nelegálním, nevhodným nebo neetickým účelům.

5. Komunikace a reprezentace společnosti

- Při využívání digitálních a AI nástrojů k tvorbě textů, prezentací či sdělení nesmí dojít k poškození dobrého jména společnosti, zveřejnění nepravdivých informací nebo narušení etiky komunikace.
- Je zakázáno generovat nebo šířit AI výstupy, které by mohly být klamavé, zavádějící nebo manipulativní.

6. Školení a osvěta / Zvyšování povědomí

- Každý zaměstnanec je povinen absolvovat pravidelné školení o bezpečnosti IT, přijatelné práci s AI a ochraně dat.
- Neznalost pravidel této politiky není omluvou pro jejich porušení.

7. Vyhodnocování dat a zpětná vazba

Společnost systematicky vyhodnocuje data související s využíváním digitálních technologií a systémů umělé inteligence za účelem:

- Monitorování souladu s touto politikou,
- Identifikace bezpečnostních incidentů a rizikového chování,
- Zlepšování efektivity nástrojů a pracovních procesů,
- Zajištění odpovědného a etického využívání AI.

Vyhodnocování probíhá v souladu s právními předpisy, zejména GDPR, a s důrazem na ochranu soukromí zaměstnanců. Data jsou analyzována agregovaně a anonymizovaně, pokud to povaha analýzy umožňuje.

Výsledky analýz slouží k optimalizaci procesů, školení, zlepšení zabezpečení a případné aktualizaci politiky.

Zdroje dat:

- Logy přístupů a aktivit v systémech,
- Metadata z využívání AI nástrojů (např. četnost, typy požadavků),
- Výsledky interních auditů a školení,
- Zpětná vazba od zaměstnanců a uživatelů.

Zpětná vazba a nápravná opatření:

- Na základě vyhodnocení mohou být navržena školení, změny v přístupových právech nebo technická opatření.
- Závažné odchylky od politiky jsou řešeny v souladu s disciplinárním řádem.
- Zaměstnanci mají možnost poskytovat zpětnou vazbu k fungování systémů a politiky.

Příklady přijatelného a nepřijatelného používání:

Oblast	Přijatelné chování	Nepřijatelné chování
Přihlašování a hesla	Používání silných hesel, zamykání obrazovky při odchodu	Sdílení hesel, zapisování na papír, ponechání zařízení bez dozoru
Práce s AI	Využívání AI ke generování návrhů, automatizaci reportů po ověření výstupů	Vkládání důvěrných informací do veřejných AI platforem, nekritické přebírání výstupů
Ukládání dat	Ukládání na schválené firemní úložiště s přístupovým řízením	Ukládání souborů na nešifrované flash disky, osobní účty, volně přístupná úložiště
Komunikace	Používání šifrovaných kanálů, reprezentace firmy profesionálním jazykem	Zasílání dokumentů přes osobní e-mail, zveřejnění AI výstupu s logem firmy bez kontroly
Používání zařízení	Práce na zabezpečeném firemním (nebo schváleném) zařízení	Instalace neschválených aplikací, připojování neověřených USB zařízení
Etika a právo	Respektování autorských práv, lidských práv, rovnosti při použití AI	Generování AI výstupů, které by mohly být klamavé, diskriminační nebo nevhodné

KOVOPROJEKTA
ENGINEERS & CONTRACTORS

Řízení bezpečnostních incidentů a porušení zásad

Všichni zaměstnanci společnosti jsou povinni aktivně spolupracovat na odhalování a řešení bezpečnostních incidentů a případného porušení této politiky. Cílem je minimalizovat dopady na společnost, klienty a partnery a předcházet opakování. Společnost považuje včasné rozpoznání a odpovědné řešení bezpečnostních incidentů za klíčový prvek ochrany svých dat, systémů i důvěry klientů. Každý zaměstnanec má odpovědnost incidenty včas hlásit a aktivně přispívat k jejich vyřešení.

1. Oznamovací povinnost / Hlášení incidentu
Zaměstnanec, který zaznamená bezpečnostní incident (např. únik dat), podezřelou aktivitu (např. podezřelé chování AI nástroje, phishing) nebo porušení zásad, je povinen tuto skutečnost neprodleně oznámit odpovědné osobě (např. vedoucímu, IT správci).

2. Vyhodnocení incidentu
Každý oznámený incident je bezodkladně zaznamenán, analyzován a klasifikován podle typu, závažnosti a možných dopadů. V závažných případech může být incident řešen ad hoc vytvořenou skupinou složenou ze zástupců vedení, IT a dalších relevantních oddělení nebo externích specialistů. V případě dopadu na třetí strany (např. klienty) je zajištěna včasná, transparentní komunikace.

3. Opatření
Na základě vyhodnocení incidentu mohou být přijata následující opatření:
- dočasná technická opatření (např. omezení přístupu, izolace zařízení),
- obnova a zabezpečení dat nebo systémů,
- aktualizace procesů a postupů,
- individuální nápravná opatření vůči odpovědným osobám.

4. Disciplinární řízení
Porušení této politiky může být důvodem pro zahájení disciplinárního řízení, včetně písemného napomenutí, omezení přístupových práv, nebo – v závažných případech – ukončení pracovního poměru v souladu s pracovněprávními předpisy.

5. Záznam a poučení
Každý incident je dokumentován z hlediska příčin, důsledků a přijatých opatření. Pokud je to vhodné a adekvátní, je rovněž zaznamenán do registru rizik společnosti.
Společnost provádí pravidelnou analýzu incidentů a využívá poznatky k posílení prevence, zvyšování povědomí a zlepšování vnitřních procesů.

Etické zásady v oblasti kybernetické bezpečnosti

Společnost se zavazuje k etickému a odpovědnému přístupu ke kybernetické bezpečnosti. Cílem je zajistit důvěru zaměstnanců, partnerů a klientů a podpořit kulturu digitální odpovědnosti.

1. Respekt k soukromí a důvěrnosti
Přístup k datům, systémům a síťovým zdrojům musí být vždy odůvodněný, přiměřený a transparentní. Zaměstnanci s oprávněními k důvěrným informacím jsou povinni zachovávat nejvyšší míru důvěrnosti a jednat v souladu s právními předpisy a vnitřními pravidly.

2. Odpovědné zacházení s oprávněními
Zvýšená oprávnění (např. administrátorská práva, přístup ke zdrojovým kódům nebo auditním logům) nesmí být zneužívána ani sdílena. Každý má jednat pouze v rozsahu svých pravomocí a vždy s ohledem na bezpečnostní a etické důsledky.

3. Zamezení zneužití a manipulace

Je zakázáno provádět jakékoli činnosti, které by mohly ohrozit bezpečnost systémů, dat nebo osob – včetně zneužívání přístupů, obcházení technických opatření nebo manipulace s výstupy umělé inteligence.

4. **Transparentnost a informovanost**
   V případě zjištění hrozby, incidentu nebo zranitelnosti je zaměstnanec povinen jednat neprodleně a informovat příslušnou odpovědnou osobu. Zatajování nebo bagatelizace bezpečnostních rizik je považováno za závažné pochybení.

5. **Podpora spravedlivého a bezpečného digitálního prostředí**
   Zaměstnanci se aktivně podílejí na vytváření kultury kybernetické odpovědnosti – dodržují zásady této politiky, respektují ostatní uživatele a přispívají k tomu, aby firemní digitální prostředí bylo bezpečné, spravedlivé a důvěryhodné.

6. **Etické zásady využívání umělé inteligence**
   - AI nesmí být využívána způsobem, který by omezoval svobodu rozhodování, diskriminoval jednotlivce nebo skupiny, či jinak narušoval lidská práva.
   - Společnost dbá na to, aby algoritmy a modely nebyly zatíženy předsudky a nevedly k nespravedlivému zacházení. Využívání AI podléhá pravidelnému přezkumu z hlediska rovnosti přístupu.
   - Společnost implementuje pouze ověřené AI systémy, které splňují požadavky na bezpečnosti, transparentnost a řízení rizik.
   - Společnost zohledňuje environmentální dopady využívání AI (např. spotřebu energie při trénování modelů) a preferuje řešení s nižší ekologickou stopou.

Závěrečná ustanovení

Tato politika nenahrazuje ani neruší jiné existující interní předpisy.

Brno 1.10.2025