Verze: listopad 2026

GEM CORTEX AI

POLICY-AS-CODE A AI GATEWAY

Produktová obchodní a technická specifikace

Policy-as-Code a AI Gateway tvoří společnou kontrolní vrstvu pro AI agenty a aplikace v návaznosti na GEM Cortex AI. Policy-as-Code převádí schválená pravidla do podoby, kterou lze verzovat, testovat a vyhodnocovat během provozu. AI Gateway a připojené kontrolní body tato rozhodnutí vynucují. V dohodnutém rozsahu tak organizace řídí, která data smí AI použít, kam je může odeslat a jakou akci smí provést.

Sdílená pravidla mají vlastní životní cyklus nezávislý na jednotlivých agentech. Změna limitu nebo oprávnění se spravuje na jednom místě a promítá do připojených aplikací. Rozhodnutí nese použitou verzi, důvod a vazbu na skutečný výsledek.
Nabídka kombinuje platformní komponenty, integrace, formalizaci pravidel a služby GEM pro zavedení a provoz. Konkrétní technologie, napojené systémy, modely, úroveň autonomie a servisní parametry se potvrzují v návrhu řešení a ve smluvním rozsahu dodávky. Technická varianta popsaná v této specifikaci představuje referenční návrh, který se ověří pro konkrétní nasazení.

1. *Výkonné shrnutí a místo v nabídce GEM*

Řešení je určeno organizacím, které chtějí rozvíjet AI v reálných procesech a současně zachovat odpovědnost za přístupy, schvalování, náklady a výsledek. Společná kontrolní vrstva propojuje technické řízení s vlastníky podnikových pravidel.

Pravidlo určuje věcný vlastník procesu, bezpečnosti nebo compliance. Technický tým zajistí jeho převod, testy a připojení ke kontrolním bodům. Agent může připravovat podklady a navrhovat postup, ale oprávnění k chráněné akci vychází ze schválených pravidel a aktuálního ověřeného kontextu.

- ***Jednotná pravidla napříč připojenými agenty a aplikacemi, s evidovaným vlastníkem, verzí a účinností.***
- ***Řízená modelová volání podle identity, účelu, datového profilu a rozpočtu.***
- ***Kontrola podnikových akcí před jejich provedením a jednoznačné předání člověku tam, kde je vyžadováno schválení.***
- ***Dohledatelný průběh od požadavku přes rozhodnutí až po skutečný výsledek.***
- ***Bezpečné změny pravidel prostřednictvím review, testů, postupného zavádění a návratu předchozí verze.***

GEM System a. s. | Štětkova 1638/18, 140 00 Praha 4 – Nusle | sales@gemsystem.cz | www.gemsystem.cz

GEM SYSTEM

GEM CORTEX AI
– POLICY-AS-CODE A AI GATEWAY

Zařazení do produktové rodiny

GEM Cortex AI

Schopnostní blok	Popis schopnosti
1 | Cortex Core	*Orchestrace záměru, runtime cesty, modelu a tenantního kontextu.*
2 | Cortex Access	*SSO, role, workload identity, provider účty, projekty a lifecycle.*
3 | Cortex Knowledge	*Konektory, ingestion, ACL-aware retrieval, citace a lifecycle indexu.*
4 | Cortex Flow	*Workflow, nástroje, approvals, lidské úlohy a stav procesu.*
5 | Cortex Control	*Policy, registr AI, telemetrie, evaluace, budgety a FinOps.*
6 | Cortex Workspace	*Uživatelský kanál pro schválené chatové, znalostní a pracovní úlohy.*

Model Execution tvoří samostatnou architektonickou vrstvu pro modelové adaptéry, lokální inference, routing a fallback.

Řešení lze připojit ke stávajícím agentům, aplikacím a integrační infrastruktuře klienta. Přehled ukazuje návaznost na produktovou rodinu; konkrétní dodávka obsahuje pouze vybrané schopnosti. Označení bloků neurčuje samostatné licence ani povinnost zavést celou produktovou rodinu.

2. Problém klienta a kvalifikace příležitosti

U prvního AI pilotu mohou být pravidla součástí kódu, promptu nebo lokální konfigurace. S růstem portfolia vzniká pracnost změn: týmy dohledávají dotčené aplikace, překládají stejné požadavky různým způsobem a testují každé nasazení zvlášť. Organizace současně obtížně prokazuje, podle čeho konkrétní agent postupoval.

Druhým problémem je roztříštěný přístup k modelům a nástrojům. Chybí společná vazba mezi identitou, účelem, daty a náklady. Agent může mít širší oprávnění, než jeho proces potřebuje, nebo může existovat přímá cesta, která kontrolu obchází. Policy-as-Code řeší přípustnost rozhodnutí; integrace a přístupové kontroly zajistí jeho skutečné vynucení.

Vhodným klientem je podnik s opakovanými rozhodnutími, sdílenými pravidly a dostupnými integračními body. Typickými prostředími jsou finanční služby, pojišťovnictví, dokumentově náročné organizace, veřejné služby a podnikové IT. Podstatný je dopad procesu a rozsah řízení, nikoli samotné odvětví nebo označení aplikace za agenta.

Schopnostní blok	Popis schopnosti	Měřitelný důkaz
1 | CIO a CTO	*Opakované využití kontrol a menší pracnost změn napříč aplikacemi.*	*Doba změny pravidla a počet zásahů do aplikací.*
2 | CISO a bezpečnost	*Kontrola datových cest a oprávnění v připojeném prostředí.*	*Pokrytí kontrolami, negativní testy a evidence výjimek.*
3 | Vedení a compliance	*Doložitelná odpovědnost a přehled o používání AI.*	*Vlastníci pravidel a dohledání konkrétního rozhodnutí.*
4 | Vlastník procesu	*Zachované kompetence a předvídatelné schvalování.*	*Správné eskalace, doba zpracování a přijaté výsledky.*
5 | CFO a nákup	*Transparentní náklady platformy i jednotlivých procesů.*	*Jednotkový náklad a realizovaný přínos proti baseline.*

První příležitost musí mít vlastníka, popsaná pravidla, reprezentativní případy a místo, kde lze akci zastavit. U kreativní asistence nebo jednorázového experimentu může stačit jednodušší profil. Pokud stejnou potřebu bezpečně a ekonomicky pokrývá existující workflow či již licencovaná služba, GEM navrhne její využití nebo doplnění společných kontrol.

3. Problém klienta a kvalifikace příležitosti

Policy-as-Code odděluje otázku, co je za daných podmínek dovoleno, od toho, jak agent vykonává svoji práci. Vykonatelné pravidlo může posuzovat například role, finanční limity, stav schválení, časové podmínky, povolený model nebo klasifikaci dat. Generativní model připravuje podklady; přesný limit nebo oprávnění vyhodnocuje pravidlo nad strukturovanými vstupy.

Stejná verze pravidel nad stejným úplným kontextem má vrátit stejné rozhodnutí. Tato vlastnost usnadňuje testování a rekonstrukci případu. Pravdivost vstupního údaje a správnost převodu směrnice zůstávají samostatnými kontrolami. Výsledek extrakce z dokumentu proto nemusí být dostatečným důkazem pro povolení zápisu.

Dva profily řízení agentů

Referenční návrh rozlišuje asistenční a procesní profil podle autonomie a dopadu. Jde o varianty zapojení kontrolní vrstvy, jejichž použití se ověří pro konkrétní proces.

Profil	Popis schopnosti	Měřitelný důkaz
1 | Asistenční profil	*Shrnutí, návrh textu nebo práce se znalostmi bez autonomní změny systému.*	*Každé modelové volání přes AI Gateway, kontrola identity, dat a spotřeby; výsledek posoudí člověk.*
2 | Procesní profil	*Agent připravuje více kroků a může navrhnout chráněnou akci.*	*Omezení plánu, kontrola modelových volání a nástrojů, nové rozhodnutí před akcí a případné lidské schválení.*

Plný procesní profil se volí podle dopadu a potřeby doložitelnosti. Časovače, fronty, čekání a stav workflow zůstávají v procesní orchestraci. Policy vrstva vyhodnocuje podmínky, které jí orchestrátor a důvěryhodné zdroje předají.

Vynucení musí proběhnout na každé relevantní cestě k modelu, datům nebo chráněné akci v dohodnutém rozsahu. Brána pro modelová volání sama nezastaví zápis do ERP ani používání veřejné AI služby mimo připojené prostředí. Produkční návrh proto mapuje i síťové cesty, servisní účty a klíče, kterými lze kontrolu obejít.

Změna pravidla nevyžaduje úpravu agenta, pokud stávající integrace dodává všechny potřebné atributy a umí rozhodnutí vynutit. Nový typ akce, nové vstupní pole nebo odlišné schvalování může vyžadovat změnu rozhraní. Obsahem dodávky je i vymezení této hranice.

GEM Cortex AI

GEM Cortex AI

Vymezení konkrétní dodávky

Rozsah nabídky určí připojené agenty a aplikace, vybraná pravidla, modelové endpointy, podnikové akce a kontrolní body. Samostatně se potvrdí integrace, schvalovací workflow a provozní služby. Další procesy se zavádějí podle výsledků pilotu a schváleného rozšíření.

PaC využívá podnikovou identitu, kontext a výsledky dalších kontrol. IAM, obsahové guardrails, bezpečnostní skenery a orchestrace mají vlastní odpovědnosti. Jejich úplná náhrada není součástí popsaného principu PaC.

4. Referenční architektura

Technický model v kapitolách 4 až 6 popisuje referenční variantu k validaci pro konkrétní nasazení. Architektura, výběr dodávaných funkcí a rozsah řešení se potvrdí v discovery a návrhu dodávky.

Referenční architektura odděluje správu politik od vyhodnocení konkrétního požadavku. Řídicí rovina spravuje zdroje pravidel, jejich schvalování, testování a publikaci. Provozní rovina obsluhuje požadavky, získává kontext, rozhoduje a vynucuje výsledek.

Role	Význam	Odpovědnost
1 | PAP	*Správa politik*	*Autorství, metadata, review, testy, schválení a distribuce verzí.*
2 | PDP	*Rozhodovací bod*	*Vyhodnotit schválenou sadu pravidel nad strukturovaným kontextem.*
3 | PEP	*Bod vynucení*	*Zachytit požadavek a skutečně povolit, zastavit nebo podmínit jeho provedení.*
4 | PIP	*Zdroj kontextu*	*Poskytnout důvěryhodné role, limity, klasifikaci a aktuální stav případu.*
5 | Auditní vrstva	*Evidence a dohled*	*Propojit rozhodnutí, použitou verzi, splnění podmínek a skutečný výsledek.*

AI Gateway plní roli PEP pro modelová volání. Pro podnikové akce tuto roli plní API gateway, integrační služba, workflow, pipeline nebo přímo cílový systém. Místo vynucení se vybírá podle toho, kde lze operaci spolehlivě zastavit.

Referenční technická varianta využívá Open Policy Agent jako PDP a jazyk Rego pro vykonatelná pravidla. Pravidla a testy vznikají v Gitu, procházejí CI a do provozu se distribuují jako schválené podepsané balíky. Výběr konkrétní technologie a podporovaných verzí je součástí návrhu řešení.

V referenční variantě Git a registr artefaktů nejsou synchronní závislostí každého rozhodnutí. Provozní rozhodovací bod používá již načtenou ověřenou verzi. Provozní návrh vymezí její platnost a chování při nedostupnosti dalších komponent.

Integrace navazují na podnikový adresář, schvalovací workflow, modelové endpointy, datové katalogy a provozní dohled. Lze využít existující API gateway a infrastrukturu klienta. REST API nebo nástrojový protokol, například MCP, poskytují rozhraní; kontrola identity, oprávnění a dopadu akce musí být zajištěna samostatně.

5. Správa pravidel a bezpečné změny

Správa pravidel stojí na věcném vlastnictví, verzování, review, testech a bezpečném zavádění. Referenční návrh tuto správu rozpracovává do následujícího životního cyklu. Konkrétní metadata, nástroje a způsob publikace určí návrh nasazení.

Pravidlo má vlastníka a vazbu na schválený zdroj. Evidence propojuje verzi směrnice, účinnost, kritičnost, schvalování a technickou implementaci, aby bylo možné doložit původ rozhodnutí.

Strojově vyhodnotitelné podmínky se oddělí od částí vyžadujících odborný úsudek. AI může pomoci s rozborem textu nebo návrhem pravidla, ale odpovědný autor zůstává člověk. Nejasná směrnice musí projít věcným upřesněním před převodem do vykonatelné politiky.



Životní cyklus politiky

- *Vlastník potvrdí zdroj, výklad, účinnost a konkrétní příklady požadovaného chování.*
- *Autor připraví pravidlo, metadata a testy povolených, zakázaných, hraničních i neúplných vstupů.*
- *Změna projde věcným a technickým review. U kritických pravidel schvaluje jiná osoba než autor.*
- *CI ověří schéma a složenou sadu politik. Známé případy se přehrají proti nové verzi a vysvětlí se každá změna očekávaného výsledku.*
- *Schválený release vznikne jako verzovaný artefakt s podpisem, otiskem a dohledatelným původem.*
- *Nová verze se ověří ve sledovacím režimu nebo na omezené skupině. Teprve po schválení začne vynucovat nové podmínky.*
- *Provoz sleduje dopad změny a aktivní verze. Životní cyklus zahrnuje recertifikaci, expiraci, návrat předchozího release a vyřazení pravidla.*

Sledovací režim porovnává rozhodnutí a dopady nové verze bez zapnutí jejího blokování. Již platné kontroly při tom zůstávají účinné. Návrat verze pravidel obnovuje předchozí konfiguraci; nevrací automaticky podnikové akce, které již proběhly.

GEM Cortex AI

GEM Cortex AI

Kompozice a výběr pravidel

Společná pravidla organizace se skládají s doménovými a procesními pravidly. Hierarchie má výslovně definované jmenné prostory a způsob agregace výsledků. Základní ochrany musí být součástí každého příslušného rozhodnutí a výjimka je nesmí tiše vyřadit.

V referenční variantě správnou sadu určuje registr a ověřený kontext uvnitř policy vrstvy. Agent si pravidlo nevybírá. Chybějící potřebná politika vede k odmítnutí; kontrola se tiše nepřeskočí.

Referenční návrh počítá s ověřením podpisu a rozsahu artefaktu před aktivací. Zahrnuje ochranu podpisových klíčů, sledování aktivních verzí, recertifikaci a časově omezené výjimky. Tyto mechanismy se validují pro vybrané nasazení.

6. Referenční řízení plánu a akcí

Procesní profil používá kontrolu před prací agenta a nové posouzení před chráněným efektem. Mezi těmito body se může změnit stav případu, oprávnění, částka nebo platnost podkladů. Povolení procesu na začátku proto nepředstavuje oprávnění ke všem navazujícím akcím.

PLAN stanoví rámec práce

Před zahájením práce politika určí přípustné kontroly, nástroje, šablony a limity. Agent dostane vymezený rámec, v němž může připravovat podklady. Plán může například stanovit, které dokumenty vyhodnotit, jaká pole získat a kdy další práce nemá smysl. Tím lze omezit nepotřebné modelové operace ještě před jejich provedením.

Každé následné volání modelu prochází vlastní kontrolou v AI Gateway. Použití nástroje podléhá jeho oprávněním a aktuálním pravidlům. Za běh procesu, čekání a agregaci výsledků odpovídá orchestrace.

DECIDE posoudí konkrétní akci

Bezprostředně před chráněnou akcí rozhodovací bod vyhodnotí výsledky kontrol a aktuální kontext. Technický výsledek PASS u dokumentu nemusí stačit k zápisu: stále mohou chybět oprávnění, platný termín nebo schválení. Neúplný či neurčitý údaj se nesmí tiše změnit na splněnou podmínku.

Výstupem je povolení, zamítnutí nebo povolení vázané na povinné podmínky. Taková podmínka, označovaná jako obligace, může vyžadovat lidské schválení, nižší limit nebo použití jiného povoleného modelu. PEP provede operaci až po splnění požadované podmínky.

Obsah rozhodnutí a auditní vazby

Referenční návrh pracuje se subjektem, akcí, objektem a kontextem. Rozhodnutí doplňuje identifikátor, důvod, verzi politiky a případné obligace. Konkrétní schéma rozhraní se stanoví v návrhu integrace.

Část kontraktu	Požadovaný obsah
1 | Subjekt	*Ověřený uživatel nebo workload, delegace a relevantní oprávnění.*
2 | Akce a objekt	*Konkrétní operace, parametry, cílový systém a identifikátor případu nebo zdroje.*
3 | Kontext	*Účel, prostředí, klasifikace dat, limity, aktuální stav a rozhodný čas.*
4 | Rozhodnutí	*Výsledek, důvodový kód, vysvětlení, decision ID, verze politik a povinné podmínky.*
5 | Provedení	*Doklad splnění podmínek, stav operace a identifikátor výsledku v cílovém systému.*

GEM Cortex AI

Důvěryhodné role, limity a schválení se získávají z podnikových zdrojů. Při rozhodnutí před akcí se vyhodnotí aktuální kontext, který se mohl od začátku procesu změnit.

U obligace vyžadující lidské schválení návrh počítá se zastavením akce a auditní vazbou na rozhodnutí. Schvalovací workflow zůstává v gesci procesního týmu. Pro nástrojové integrace platí požadavky na oprávnění, limity, preview, schválení, idempotenci a audit.

Výchozí pilot pracuje se čtením nebo návrhy. Nevratné a právně významné kroky zachovávají lidskou kontrolu. Rozšíření autonomie vyžaduje samostatné rozhodnutí o konkrétním procesu a ověřené kontrolní body.

7. AI Gateway data a nákladové řízení

AI Gateway sjednocuje modelový provoz připojených aplikací. Každé volání posuzuje v kontextu identity, účelu, datového profilu, povoleného endpointu a nákladové odpovědnosti. Registr modelů eviduje vlastníka, region, povolenou klasifikaci dat, smluvní režim a provozní parametry.

Autorizace volání a obsahová kontrola mají odlišné úlohy. Politika určuje, zda se požadavek smí uskutečnit. Obsahové kontroly, často označované jako guardrails, posuzují vstup a výstup například z hlediska citlivého obsahu nebo povoleného formátu. Směrování vybírá schválený model a měření spotřeby dodává podklad pro FinOps.

- ***Kontrola před odesláním ověří přípustnost datové cesty. Podle zadání se připojí klasifikace, detekce citlivých údajů nebo redakce.***
- ***Směrování a fallback použijí pouze endpointy přípustné pro danou identitu, účel a datový profil.***
- ***Limity omezí velikost požadavku, frekvenci, délku běhu, tokenovou spotřebu a rozpočtový rozsah.***
- ***Měření přiřadí skutečnou spotřebu aplikaci, procesu, projektu nebo nákladovému středisku a propojí ji s dokončenou úlohou.***
- ***Strukturované odmítnutí vysvětlí důvod a umožní aplikaci řízeně požadavek doplnit, odložit nebo předat člověku.***

Tvrdé rozpočtové zastavení se vztahuje na spotřebu procházející řízenou bránou. Odhad před voláním a konečné účtování se mohou lišit; nákladová evidence se proto porovnává s daty poskytovatele. Konkrétní limity a jejich vynucení se ověří v návrhu a pilotu. Optimalizace modelu nebo kontextu se přijímá při zachování požadované kvality.

Ochrana dat zahrnuje oprávnění ke zdrojům před sestavením kontextu modelu. Kontrola odpovědi nemůže zpětně zabránit odeslání nepovoleného vstupu. Nulová retence, region a nepoužití dat pro trénování se potvrzují pro konkrétní službu a smluvní nastavení.

Veřejné chaty, desktopové nástroje a SaaS asistenti potřebují samostatné posouzení integračních možností a podnikových kontrol. U vývojářských copilotů lze ověřovat výsledek na pull requestu a v CI; tím se neprokazuje kontrola veškeré komunikace daného nástroje s poskytovatelem.

8. Audit bezpečnost a provozní odpovědnost

Audit propojuje plán, modelová volání, rozhodnutí před akcí, splnění podmínek a skutečný výsledek. Záznam o povolení nepotvrzuje úspěšné provedení. To musí doložit cílový nástroj nebo podnikový systém. Jednoznačná korelace umožňuje zjistit, kde byl proces zastaven a proč.

Auditní záznam propojuje čas, identitu, proces, akci, rozhodný kontext, decision ID, verzi pravidel, důvod a stav vynucení. Rozsah uchovaných vstupů, možnost zpětného přehrání, dobu uchování a oprávnění k evidenci určí návrh podle klasifikace dat a účelu kontroly.

Běžná telemetrie automaticky neobsahuje plné prompty ani dokumenty. Provozní, auditní a forenzní přístupy se oddělují podle role. Záznamy potřebují ochranu před neoprávněnou změnou, stanovený export a ověření úplnosti včetně zamítnutí a chyb. Evidence podporuje interní audit a regulatorní posouzení; použitelnost právních požadavků a odpovědnost za jejich výklad potvrzuje klient.

GEM Cortex AI

Bezpečnostní požadavky

Návrh posuzuje obcházení PEP, podvrženou identitu nebo kontext, kompromitovaný balík pravidel, manipulaci auditu a nedostupnost rozhodovací služby. Samostatně řeší rizika prompt injection a zneužití nástrojů. Přístup ke klíčům, repozitářům a změnám politik používá minimální oprávnění a oddělení rolí.

Referenční návrh počítá u chráněných akcí s bezpečným zastavením při nedostupném rozhodnutí a s používáním poslední ověřené politiky v definovaném režimu. Chování při výpadcích, platnost politik, případné cache a obnova se posoudí a otestují pro konkrétní provoz.

Model provozu a odpovědnosti

Následující rozdělení představuje referenční model odpovědností. Odpovědnosti a servisní závazky se potvrdí pro vybranou dodávku.

Oblast	Odpovědnost klienta	Odpovědnost GEM ve sjednaném rozsahu
1 | Pravidla a proces	*Věcný výklad, limity, vlastník a schválení autonomie.*	*Formalizace, implementace a technické testy.*
2 | Data a identity	*Klasifikace, účel, oprávnění a přístup ke zdrojům.*	*Integrace a správné předání kontextu.*
3| Platforma	*Volba provozního modelu a zajištění klientských závislostí.*	*Aplikační komponenty, konfigurace a dohodnutá správa.*
4| Akceptace	*Potvrzení správných výsledků a převzetí procesu.*	*Testovací důkazy, odstranění vad a předání.*
5| Incidenty a změny	*Procesní eskalace a schválení věcných změn.*	*Technická diagnostika, obnova a správa verzí.*

GEM CORTEX AI
– *POLICY-AS-CODE A AI GATEWAY*

Infrastrukturu a modelové endpointy provozuje smluvně určená strana. Řešení může běžet v cloudu klienta, jako služba GEM, hybridně nebo v omezeném lokálním prostředí. Každá varianta má vlastní datové toky, kapacitní nároky a odpovědnosti.

Servisní návrh stanoví dostupnost, latenci, kapacitu a parametry obnovy RTO a RPO podle kritičnosti procesu. V dohodnutém provozním rozsahu zahrne monitoring, zálohy, obnovu, návrat verzí a incidentní postupy. Výkon se ověřuje na reálné sadě pravidel a očekávaném provozu.

Máte AI agenty pod kontrolou?

Podle jakého pravidla se agent rozhodl?

Kam mohou odejít firemní data?

Dokážete rozhodnutí doložit auditorovi?

Policy-as-Code a AI Gateway pomáhá vynutit pravidla a doložit rozhodnutí.

GEM Cortex AI

GEM System a. s. | Štětkova 1638/18, 140 00 Praha 4 – Nusle | sales@gemsystem.cz | www.gemsystem.cz

9. Případy užití a první prodejní scénáře

Následující scénáře ukazují oblasti použití společné kontrolní vrstvy. Výběr prvního procesu, jeho integrace a akceptační metriky se stanoví při kvalifikaci a v Pilot Charteru.

Dokumentové a finanční procesy

AI připraví strukturované údaje z dokumentů a ověří přítomnost podkladů. Politika posoudí přesné podmínky, například platnost dokumentu, podpis, časový práh nebo finanční limit. Neúplný případ předá odborníkovi. Zápis nebo finanční akce proběhne v řízeném systému po potřebném schválení.

Pro první pilot se vybere omezený dokumentový proces. Ověří se čas přípravy, předání člověku, rozhodnutí podle pravidel a auditní stopa. Přínos vzniká v rychlejší přípravě a jednotné kontrole, při zachování odpovědnosti za rozhodnutí.

AI asistovaný vývoj a nasazení

Vývojář nebo agent připraví změnu. Pull request a CI pipeline ověří testy, výsledky bezpečnostních skenerů, tajemství v kódu a schválené závislosti. Politika vyhodnotí tyto výsledky a podmínky pro další krok. Člověk schválí změnu a produkční nasazení proběhne v povoleném procesu.

Pilot lze omezit na vybraný repozitář a pipeline. Ověří blokaci změn podle pravidel a dohledatelnost schválení. Agent má přístup jen do povolených repozitářů a prostředí. Policy-as-Code využívá výsledky skenerů jako vstupy.

Zranitelnosti a řízení oprav

Agent třídí nálezy a připravuje návrhy úkolů. Politika zohlední kritičnost aktiva, závažnost nálezu, interní lhůty a eskalační pravidla. Produkční změna vyžaduje schválený postup. Úspěšné doporučení opravy se odděluje od oprávnění ji provést.

Pilot vybere omezenou oblast řízení zranitelností a oprav. Ověří rozhodování podle lhůt a eskalačních pravidel a vazbu na audit. Sdílená pravidla usnadní promítnutí nové interní metodiky do připojených týmů.

Ochrana dat a přístupu k modelům

Aplikace požádá o shrnutí nebo analýzu interního obsahu. Gateway posoudí účel, klasifikaci a povolený endpoint. Znalostní vrstva před předáním obsahu ověří oprávnění uživatele. Pokud vhodná cesta neexistuje, požadavek se zastaví nebo předá ke schválenému posouzení.

Pilot vybere připojenou aplikaci a datový rozsah. Ověří pokrytí modelových volání, přípustnost směrování, fallback a nákladové měření. Pokud rozsah zahrnuje obsahové kontroly, jejich účinnost se ověří samostatně.

Zákaznické procesy a obchodní pravomoci

AI připraví návrh odpovědi, slevy nebo vyřízení reklamace. Pravidla ověří kompetence, limity a stav případu. Závazný příslib nebo změna smlouvy se předá oprávněné osobě a proběhne jako kontrolovaný krok v příslušném systému.

Pilot vybere konkrétní rozhodovací situaci a její schvalování. Ověří dodržení kompetencí, limitů a eskalací. Výsledek přípravy a finální obchodní rozhodnutí zůstávají dohledatelné odděleně.

GEM Cortex AI

Veřejné služby a citlivé agendy

AI třídí podání a připravuje evidenční údaje nebo kontrolní seznam. Pravidla řídí přístupy, předání mezi rolemi a podmínky workflow. Odborné posouzení a právně významné rozhodnutí zůstávají odpovědnému pracovníkovi.

Pilot pracuje s jednou agendou a reprezentativní sadou případů. Ověřuje oprávnění, chybné zatřídění, předání pracovníkovi a auditní vazby. AI nečiní meritorní rozhodnutí.

10. Dodávka implementace a akceptace

GEM začíná konkrétním procesem a ověřitelnou hypotézou hodnoty. Discovery mapuje pravidla, současné přístupy, datové cesty, účty a všechna místa, kde může vzniknout chráněný efekt. Zjišťuje, které kontroly lze využít z existujících systémů a kde je nutná integrace.

Fáze	Obsah práce	Výstup pro klienta
1 | Kvalifikace a discovery	*Proces, vlastník, baseline, pravidla, rizika a integrační možnosti.*	*Vymezení příležitosti a doporučený rozsah.*
2 | Návrh a pilot	*Rozhodovací kontrakt, prioritní pravidla, historická sada a sledovací režim.*	*Pilot Charter a důkaz funkce a dopadu.*
3| Omezená produkce	*Identity, vynucení, schvalování, monitoring, bezpečnost a obnova.*	*Akceptace a provozní převzetí.*
4| Rozvoj a provoz	*Další procesy, recertifikace, FinOps a řízené změny.*	*Měřené portfolio a opakované využití komponent.*

Pilot Charter stanoví vstupy a výstupy, in scope a out of scope, vlastníky, kontrolní body, testovací sadu, náklady a kritéria rozhodnutí go, adjust nebo stop. Reprezentativní případy zahrnují i hraniční a nepřípustné situace. Ladicí a nezávislá ověřovací sada se oddělují.

Pilot ověří vybrané pravidlo od schválení až po použití v připojených kontrolních bodech, správnost rozhodnutí, auditní průběh a provozní dopad. Procesní profil doplní kontrolu konkrétní akce a požadovaného lidského schválení.

Akceptace v dohodnutém rozsahu

Oblasti ověření se vyberou podle profilu a architektury pilotu. Konkrétní scénáře, očekávané výsledky a číselné prahy se schválí v Pilot Charteru.

GEM Cortex AI

Oblast ověření	Důkaz pro akceptaci
1 | Rozhodnutí podle pravidel	*Povolené, zakázané a hraniční případy odpovídají očekávanému výsledku.*
2 | Změna a návrat politiky	*Review, testy, publikace a dohledání použité verze; ověřený návrat.*
3 | Modelová cesta	*Volání připojené aplikace prochází určenou bránou a povolenými modely.*
4 | Procesní akce a schválení	*PEP vynutí rozhodnutí a při požadovaném schválení akce čeká na člověka.*
5 | Výpadky a obnova	*Chování odpovídá dohodnutému bezpečnému režimu a obnově.*
6 | Auditní stopa	*Dohledání identity, verze pravidla, důvodu a výsledku vybraného případu.*
7 | Provoz a ekonomika	*Změřená latence, spotřeba, pracnost a dopad proti baseline.*

Negativní testy ověří, že v dohodnuté sadě nenastane nepovolená akce. Úspěch testovací sady není obecnou zárukou bezchybného budoucího provozu ani automatickou certifikací compliance.

Předávací balíček se stanoví podle fáze a rozsahu dodávky. Zahrnuje vymezení řešení, architekturu a datové toky, bezpečnostní a testovací důkazy, provozní odpovědnosti, ekonomiku a dohodnuté exporty pro ukončení služby.

11. Ekonomika nabídka a měření přínosu

Ekonomika rozlišuje společnou platformu a zavedení jednotlivých procesů. Platforma má počáteční a opakované náklady, zatímco další procesy mohou využít již zavedené identity, distribuci pravidel, bránu a audit. Pravidla konkrétního procesu, jejich schválení a ověření přesto vyžadují vlastní práci.

Nabídka odděluje discovery, platformní implementaci, integrace a procesní onboarding od spotřeby modelů, infrastruktury, podpory a průběžné správy pravidel. Cena závisí zejména na počtu kontrolních cest, kvalitě dokumentace, dostupnosti identit, rozsahu schvalování a požadované úrovni služby. Závazná kalkulace vzniká po kvalifikaci rozsahu.

Fáze	Obsah práce	Výstup pro klienta
1 | Změny pravidel	*Četnost změn, pracnost a počet dotčených aplikací.*	*Společné pravidlo skutečně nahrazuje opakovanou práci.*
2 | Testy a dohled	*Čas regrese, opravy a provozní kontrola.*	*Zůstává požadovaná kvalita a rozsah ověření.*
3| Auditní příprava	*Čas dohledání a sestavení podkladů.*	*Evidence je úplná a použitelná pro daný účel.*
4| Modelová spotřeba	*Volání, tokeny a náklad na přijatý výsledek.*	*Optimalizace zachová kvalitu a adopci.*
5| Procesní průchodnost	*Doba případu, rework a dokončený objem.*	*Organizace využije uvolněnou kapacitu.*

Úspora času se eviduje jako kapacita, dokud se neprokáže její využití nebo snížení skutečného nákladu. Snížení rizika se vyjadřuje samostatným scénářem. Modelovou spotřebu může snížit vhodnější plán, kontext nebo routing; samotné zavedení PaC obecnou procentní úsporu nezaručuje.

Business case porovnává víceleté přínosy s implementací, onboardingem a opakovaným TCO. Pracuje s očekávaným portfoliem, adopcí a reálnými termíny zavádění. Pilot má ověřit jednotlivé předpoklady a zpřesnit kalkulaci. Ekonomika konkrétního klientského návrhu se nepřenáší automaticky na jiné nasazení.

12. Obchodní komunikace a další krok

Hlavní sdělení

GEM Cortex AI dává organizaci společná pravidla pro používání modelů a řízení akcí AI agentů. Pravidla mají vlastníky, verze a testy. Připojené brány a podnikové kontrolní body je uplatní před konkrétní operací a výsledek lze doložit. Klient může rozvíjet další AI procesy nad již zavedenou kontrolní vrstvou.

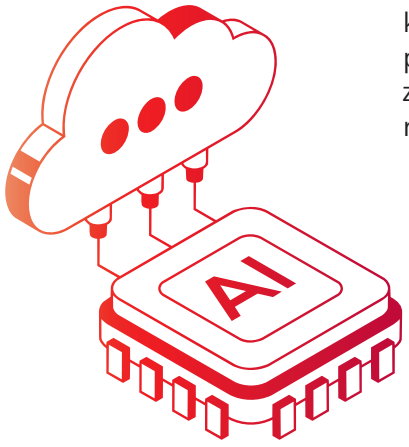
Krátké představení nabídky

Když se změní firemní pravidlo, jeho různé podoby v AI aplikacích vytvářejí práci i riziko. GEM propojí vaše agenty se společnou správou pravidel a řízenou bránou k modelům. Přesné limity a oprávnění se vyhodnotí před akcí, změny projdou testy a rizikový krok se předá člověku. Začneme jedním procesem a ověříme kontrolu, provozní dopad i ekonomiku.

Práce s typickými námitkami

Existující agent nebo workflow lze zachovat, pokud má vhodné integrační body. V discovery se vyberou pravidla, která potřebují společný životní cyklus, a zmapuje se potřebný kontext. Postupná integrace snižuje rozsah změny a umožňuje porovnat nové rozhodování se současným stavem.

Lokální konfigurace není sama o sobě problém. Rozhodující je vlastnictví, testování, publikace a vynucení pravidla. B2B přínos vzniká tam, kde jednotná správa odstraní opakovanou práci a přinese doložitelnou kontrolu napříč více aplikacemi.



Policy engine poskytuje vyhodnocení pravidel. Produkční dodávka k němu doplňuje kontext, kontrolní body, schvalování, bezpečné publikování a provozní odpovědnost. Tento rozsah odlišuje nasazenou platformní službu od samostatné knihovny nebo demonstračního prototypu.

GEM Cortex AI

GEM CORTEX AI
– POLICY-AS-CODE A AI GATEWAY

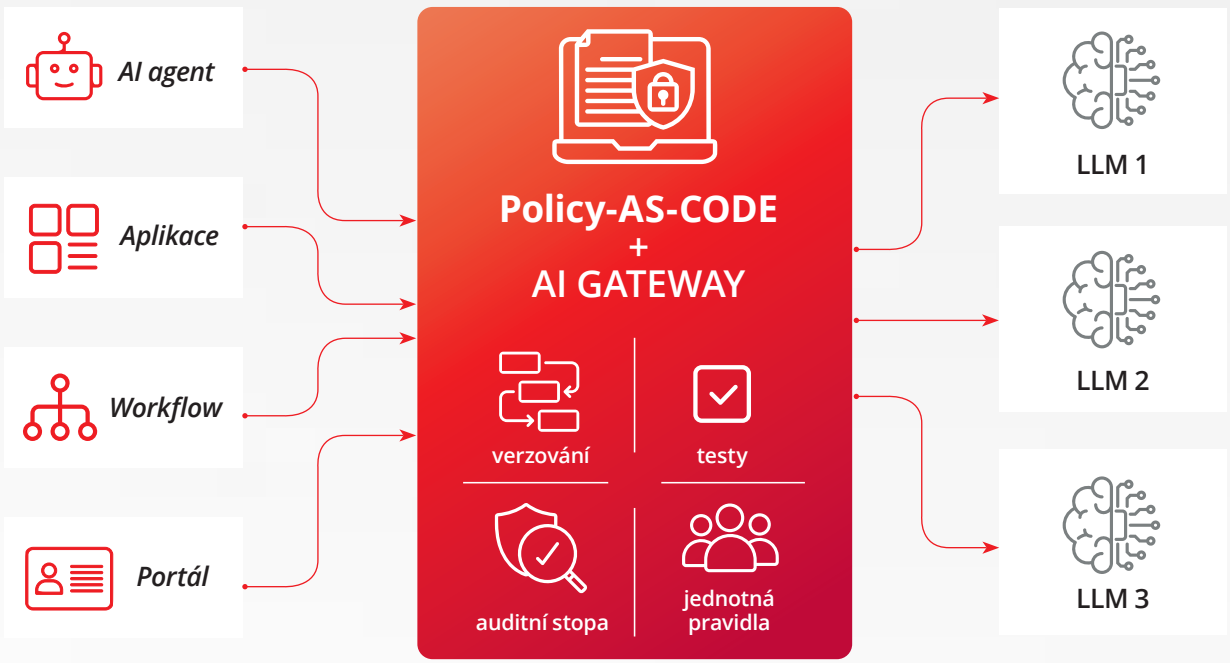
Otázky pro první jednání

- *Který proces a jaké rozhodnutí má řešení zlepšit a kdo za ně odpovídá?*
- *Která pravidla se opakují v aplikacích a kolik práce dnes stojí jejich změna?*
- *Jaká data, modely a podnikové nástroje proces používá a kdo spravuje přístupy?*
- *Kde lze skutečnou akci zastavit a které kroky potřebují schválení člověka?*
- *Lze u konkrétního případu dohledat použitou verzi, důvod a skutečný výsledek?*
- *Jaký důkaz musí pilot dodat, aby klient rozhodl o produkčním zavedení?*

GEM AI architekt a vlastník procesu připraví omezený pilot s konkrétními pravidly, kontrolními body a měřením proti baseline. Výstupem je doložené rozhodnutí o zavedení a rozšíření řešení.

Jedna změna pravidla, *platí pro všechny*

Pravidla oddělená od kódu AI agentů



GEM Cortex AI

GEM System a. s. | Štětkova 1638/18, 140 00 Praha 4 – Nusle | sales@gemsystem.cz | www.gemsystem.cz