Název veřejné zakázky: **KYBEZ města Litvínov - Rozšíření IDM EOS; § 20 Řízení přístupových oprávnění vyhlášky č. 82/2018**

systémové číslo: P25V00000043

# Předmět veřejné zakázky

Předmětem veřejné zakázky je dodávka a implementace technologií ke zvýšení úrovně kybernetické bezpečnosti informačních systémů (IS) a komunikačních systémů (KS) zadavatele. Dodavatel, se kterým bude uzavřena smlouva, poskytne zadavateli požadované dodávky a související služby specifikované v této příloze.

Přehled oblastí, které jsou předmětem dodávky:

| **Zajišťovaná oblast** | **Stručný popis položky** |
| --- | --- |
| Řízení identit a přístupových práv | Centralizace a automatizace správy uživatelských účtů a oprávnění napříč systémy. |
| Prevence lidských selhání | Zavedení nástrojů pro školení, testování a analýzu chování uživatelů v kontextu bezpečnostních událostí. |

Dodavatel je povinen navrhovat řešení v souladu s nejlepšími dostupnými technologickými praktikami, doporučeními výrobců a relevantními normami kybernetické bezpečnosti.

Není-li u technického parametru uvedeno, že jde o minimální či maximální hodnotu, lze nabídnout technické řešení, které poskytuje vyšší užitnou hodnotu, pokud tím nebude ohrožena kompatibilita, interoperabilita nebo integrace v rámci cílového prostředí.

# Stávající a cílový stav

Zadavatel aktuálně využívá systém pro správu identit (IDM) Proxio EOS od společnosti Marbes, který slouží k řízení přístupů uživatelů do následujících systémů:

| **Název** | **Působnost** | **Dodavatel** |
| --- | --- | --- |
| Active Directory | IDM EOS je primárním systémem pro synchronizaci s AD. | Microsoft |
| MS Exchange | Zakládání a správa e-mailových schránek. | Microsoft |
| Fluxpam 5 | IS Fluxpam 5 je personálním systémem a pro IDM primárním zdrojem organizační struktury. | Flux, spol. s r.o. |

V rámci této zakázky je cílem rozšířit IDM o řízení přístupů a oprávnění pro další informační systémy městského úřadu:

| **Název** | **Působnost** | **Dodavatel** |
| --- | --- | --- |
| GINIS | Spisová služba, evidence obyvatel, agenda voleb, ekonomické moduly účetnictví, správa pohledávek, vymáhání, evidence smluv a evidence majetku. | GORDIC spol. s r.o. |
| VITA | Správní agendy: stavební úřad, přestupkové řízení. | VITA software s.r.o. |
| IQ Metropolis | Výkon činností městské policie. | In Qool, a.s. |
| ArcGIS | Geografický informační systém | ESRI |
| PWS Plus VOX | Varovný systém města | PWS PLUS s.r.o. |
| PowerKey | Docházkový systém | ADVENT, spol. s r.o. |

Druhým záměrem navrhovaného řešení je významné posílení kybernetické bezpečnosti v oblasti uživatelského chování, jelikož právě uživatelé představují podle řady výzkumů nejrizikovější prvek bezpečnostního prostředí.

Tento cíl bude podpořen novou koncepcí Identity Managementu (IDM), která je modulárně navržena a skládá se z několika funkčně vymezených částí. Tyto moduly budou propojeny navazujícími procesy, což zajistí efektivní správu, flexibilitu a rozšiřitelnost systému. Modularita zároveň umožní snadnou správu jednotlivých oblastí dle konkrétních potřeb a přístupových práv.

Výsledný systém bude realizován jako centralizovaný portál, jenž poskytne jednotné rozhraní pro přístup ke všem modulům. Cílem je vytvořit uživatelsky přívětivé, přehledné a sjednocené prostředí, kde budou všechny funkční části dostupné podle rolí a oprávnění uživatelů.

Každý modul bude plnit svou specifickou funkci, ale zároveň bude vizuálně i technicky integrován do společného portálu (včetně přehledného dashboardu), který zajistí snadnou orientaci, efektivní práci se systémem a komfortní uživatelský zážitek.

# Implementační služby

## Obecné požadavky

Zadavatel požaduje provedení následujících implementačních činností na dodaných komponentech a případně dalších zařízeních. Rozsah služeb zahrnuje minimálně tyto kroky:

* **Zpracování prováděcí dokumentace**, která musí být před zahájením realizace dodávek schválena zadavatelem. Tato dokumentace bude zahrnovat:
  + předimplementační analýzu,
  + návrh cílového konceptu řešen.
* **Dodávku a implementaci řešení** v souladu se schváleným cílovým konceptem.
* **Zajištění projektového řízení** po celou dobu realizace zakázky.
* **Zpracování školicích materiálů a realizaci školení** pro 3 administrátory v sídle zadavatele v rozsahu 2 pracovních dnů.
* **Zajištění zkušebního provozu** v délce minimálně 14 kalendářních dnů. Během tohoto období musí být k dispozici technická podpora alespoň dvou specialistů na dodané řešení, s maximální dobou dojezdu 3 hodiny od nahlášení požadavku v pracovních dnech mezi 8:00 a 17:00.
* **Předání systému do ostrého provozu**. Akceptace bude provedena pouze v případě úspěšného ukončení bezproblémového zkušebního provozu.

Veškeré náklady spojené s implementačními službami a školením musí být zahrnuty v nabídkové ceně (neuvádějí se samostatně).

Všechny dodané dokumenty musí být vyhotoveny výhradně v českém jazyce a předány v elektronické podobě ve standardních formátech používaných zadavatelem (např. MS Office).

## Požadavky na zpracování prováděcí dokumentace

Dodavatel před zahájením implementačních prací zpracuje prováděcí dokumentaci, která bude vycházet z předimplementační analýzy a bude obsahovat veškeré aktivity nezbytné pro úspěšnou realizaci předmětu plnění.

Předimplementační analýza bude reflektovat aktuální prostředí zadavatele a navrhované řešení dodavatele. Minimálně bude zahrnovat tyto oblasti:

* Analýzu stávající konfigurace a vazeb na související systémy,
* Identifikaci požadované součinnosti ze strany zadavatele.

Na základě této analýzy bude vytvořen cílový koncept, který zohlední výchozí stav i technické parametry nabízeného řešení. Cílový koncept bude obsahovat minimálně:

* podrobný popis cílového stavu a funkcionality jednotlivých částí řešení,
* přehled nutných a doporučených optimalizačních a konfiguračních změn navázaných systémů,
* způsob zajištění jednotlivých dodávek a služeb, včetně časového harmonogramu,
* způsob zajištění jednotlivých dodávek a služeb, včetně časového harmonogramu,
* detailní návrh implementačního postupu,
* způsob zajištění informační bezpečnosti,
* projektový harmonogram s vyznačením klíčových milníků,
* popis vazeb na stávající systémy a jejich konfiguraci,
* návrh akceptačních kritérií a testovacích scénářů,
* specifikaci školení, jejich obsahu a rozsahu,
* přehled a strukturu provozní dokumentace.

Po předání dokumentace bude mít zadavatel lhůtu 10 pracovních dnů na její připomínkování. Dodavatel je povinen všechny připomínky vypořádat – buď jejich zapracováním, nebo formou písemného a odůvodněného odmítnutí v případě, že je považuje za nevalidní. Zadavatel nebude dokumentaci opravovat, ale pouze vyznačí věcné nebo formální nedostatky.

Prováděcí dokumentace musí být výslovně schválena zadavatelem před zahájením dalších etap plnění.

Po realizaci implementace bude dokumentace aktualizována dle skutečně provedeného stavu, včetně všech konfigurací, nastavení a analytických výstupů. Tato aktualizovaná dokumentace bude nedílnou součástí dokumentace předávané v rámci akceptačního protokolu.

# Požadované parametry technického řešení

## Obecné požadavky

Zadavatel při výstavbě, správě a provozu technologií důsledně uplatňuje princip technologické neutrality. To znamená, že využívá taková řešení, která neomezují možnost nasazení technologií od různých výrobců. Stejný přístup musí dodržovat i řešení nabízené v rámci této veřejné zakázky.

Nabízené řešení nesmí být závislé na jediné technologii nebo komponentě, která by omezovala jeho budoucí rozšiřitelnost nebo interoperabilitu.

U každého softwarového produktu, který uchazeč zahrne do nabídky, musí být výslovně uvedeny veškeré licenční a výkonové požadavky spojené s jeho instalací a provozem. Součástí nabídky musí být rovněž specifikace hardwaru, na kterém bude řešení provozováno.

Licence musí umožnit přístup minimálně pro 250 uživatelů. Poskytnutá licence bude trvalá.

Standardní podpora a záruka spočívající v nároku zadavatele na bezplatnou dodávku každé nové verze veškerého dodávaného SW a bezplatné provedení všech oprav veškerého dodávaného SW, a to vše po dobu min. 24 měsíců ode dne převzetí předmětu plnění bez výhrad stvrzeného podpisem akceptačního protokolu zadavatelem bez výhrad.

Veškeré navržené komponenty musí být v souladu se zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, a odpovídajícími prováděcími předpisy, zejména vyhláškou č. 82/2018 Sb.

## Technické požadavky

|  |  |  |  |
| --- | --- | --- | --- |
| **Zajišťovaná oblast** | **Funkcionalita** | **Účastník splňuje ANO/NE** | **Detail naplnění požadavku (vyplní účastník)** |
| **Rozšíření řízení a evidence přístupových oprávnění do IS** | IDM EOS bude napojeno v rozsahu správy na AIS GINIS: Načtení seznamu konfiguračních skupin z GINIS a jejich přiřazení oprávněným uživatelům   * Založení pracovních pozic v GINIS * Založení aplikačních rolí k pracovním pozicím do GINIS * Založení agend a činnostních rolí z RPP k pracovním pozicím do GINIS * Založení uživatele do GINIS * Založení (synchronizace) uživatele do GINIS |  |  |
| IDM EOS bude napojeno v rozsahu evidence přístupů a oprávnění na:   * AIS ArcGIS * AIS PWS Plus VOX * AIS PowerKey |  |  |
| IDM EOS bude napojeno v rozsahu řízení přístupových oprávnění na:   * AIS IQ Metropolis * AIS VITA |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| **Zajišťovaná oblast** | **Funkcionalita** | **Účastník splňuje ANO/NE** | **Detail naplnění požadavku (vyplní účastník)** |
| **Zastřešující portál** | Musí být provozovaný na vnitřní infrastruktuře (on-premise). |  |  |
| Řešení musí obsahovat redakční systém umožňující zadávat texty pomocí editoru. Po přihlášení musí poskytnout rozhraní, přes které si uživatelé budou moci spravovat obsah stránek. |  |  |
| Přehledné a responzivní uživatelské rozhraní dostupné z internetového prohlížeče. |  |  |
| Škálovatelnost pro přidávání dalších modulů v budoucnu. |  |  |
| Rozdělení uživatelských rolí administrátor a uživatel. |  |  |
| Řešení musí být bez nutnosti instalovat komponenty na koncovém zařízení, vyjma prohlížeče nebo jeho aktualizace na novější verzi. |  |  |
| Řešení musí disponovat systémem notifikací a "hlídacího psa", které bude možné administrovat pro každého uživatele. |  |  |
| Řešení musí být přímo propojeno s IDM pro ověření uživatele. Uživatel tak nebude nepotřebovat další samostatné heslo pro přístup. Integrace musí umožnit:   * Automatizované přebírání informací z IDM. * Využití struktury IDM k definici organizační struktury. * Ověřování uživatelů přistupujících k portálu pomocí IDM (SSO). * Synchronizace uživatelů, skupin, zařazení z IDM. * Definice rolí. * Nastavení oprávnění a rolí pro uživatele a skupiny na úroveň jednotlivých záznamů. * Uživatelsky volitelnou editaci uživatelů a skupin pro externí přístup. * Vytváření a editace organizační struktury. * Řízení přístupu a oprávnění k funkcím a službám pomocí rolí. * Řízení oprávnění principem dědičnosti, tj. podřízený objekt má stejně nastavená práva jako jeho nadřízený objekt. Tato oprávnění musí být možné libovolně měnit. |  |  |
| Řešení musí umožňovat správu organizační struktury a přístupových oprávnění samotnými oprávněnými pracovníky bez nutnosti zásahu IT nebo správce IDM. Musí tedy umožňovat:   * Automatické přiřazování oprávnění vybraným osobám. * Přiřazování pracovní náplně ke konkrétním uživatelům. * Automatické přidělování oprávnění k přístupu do určených aplikací na základě vybrané pracovní náplně. * Vyhledávání uživatele. * Editaci již přidělených pracovních náplní. * Převzetí pracovních naplní z jiných osob či organizačních jednotek. * Editaci uživatelů (obrázek, podpis, základní informace, kontakty, přidělené externí identity nebo vkládat libovolná editační uživatelská pole). |  |  |
| **Modul rozcestník** | Modul musí zajistit přehledné prostředí pro personalizované spouštění aplikací, do kterých má na základě oprávnění uživatel přidělený vstup. |  |  |
| Jednotlivé odkazy na aplikace musí být ve formě dlaždic. |  |  |
| **Modul dashboard** | Modul musí být umístěn na hlavní pracovní ploše a musí být zpracován přehlednou formou. |  |  |
| Modul musí poskytovat souhrn informací, který se zobrazí po přihlášení:   * Úkoly k vyřízení. * Informace z projektů, ve kterých je uživatel členem týmu |  |  |
| Modul musí obsahovat notifikační kalendář: - osobní kalendář, do kterého se promítají další záznamy (úkoly a jejich lhůty, zápisy z porad, projekty a jejich lhůty) |  |  |
| Úkoly a události musí být řazeny podle termínu. |  |  |
| **Modul aktualit** | Modul umožňuje vkládat novinky, aktuality nebo důležitá upozornění pro informování uživatelů. |  |  |
| Modul musí umožnit snadno a rychle informovat celé oddělení, odbor nebo také úřad. Tyto informace se budou zobrazovat v dashboardu. |  |  |
| Modul musí umožnit vytvoření a distribuci tzv. důležitého upozornění, které slouží ke sdělení důležitých informací týkajících se např. upozornění na výpadek elektrického proudu či technologická odstávka IT prostředků. Tato upozornění se budou zobrazovat v dashboardu v odlišném grafickém stylu než standardní informace a musí být možné časově omezit jejich zobrazení. |  |  |
| **Modul žádostí** | Modul musí umožnit podání, schválení a vypořádání žádostí. |  |  |
| Modul musí umožnit uživatelské vytváření žádostí k vnitřním procesům úřadu, například žádost o využití služebního vozidla, rezervace místnosti či elektronických zařízení. |  |  |
| Modul musí umožnit schválení vytvořené žádosti využitím workflow. Role schvalujících ve workflow jsou definovány s využitím organizační struktury. |  |  |
| Po odeslání žádosti do workflow musí být nadřízenému vytvořen úkol o schválení a zaslána notifikace se žádostí o schválení. |  |  |
| Po schválení/zamítnutí musí být zaslána notifikace žadateli. |  |  |
| **Modul zápisů a úkolů** | Úkoly musí být možné zadávat ručně a zároveň automaticky z aplikace Konsiliář (dodavatel HD Media s.r.o.) prostřednictvím WS a vyčítáním JSON nebo XML. Součástí předávaných dat musí být úkol, obsah úkolu, vlastník úkolu, autor úkolu, termíny a lhůty. |  |  |
| Modul musí umožnit řazení úkolů podle priority či termínu a potvrzovat jejich splnění. |  |  |
| Modul musí umožnit:   * Zadání a zobrazení vlastních úkolů (sám sobě). * Zadávání úkolů pro podřízené pracovníky. * Zobrazení úkolů od nadřízeného pracovníka. * Zobrazení úkolů z jiných zdrojů (Konsiliář). * Zobrazení všech zadaných úkolů na úvodní stránce v dashboardu. * Možnost zadat míru splnění úkolu, která se prezentuje v rámci úkolu infografikou. |  |  |
| Zápisy musí poskytovat možnost zobrazovat dokumenty, strukturovat dokumenty, prohledávat je a archivovat tak, aby byly kdykoliv k dispozici. Musí umožnit:   * Členění do složek. * Řízení oprávnění přístupu na úroveň složky nebo dokumentu. * Fulltextové vyhledávání. * Sekvenční schvalovací workflow. * Notifikace o požadavku na schválení na úvodní stránce. * Diskuzi k dokumentům. * Zobrazení PDF dokumentu onsite. * Vytváření libovolných souvislostí (mezi dokumenty, kontakty, projekty). |  |  |
| **Modul směrnic** | Směrnice a předpisy jsou uchovávány v archivu a lze snadno dohledat, kdy byl který dokument v platnosti. |  |  |
| Modul musí umožnit zobrazení všech platných směrnic. |  |  |
| Modul musí disponovat následujícími funkcemi:   * Evidence dokumentů. * Členění do složek. * Řízení oprávnění přístupu na úroveň složky nebo dokumentu. * Fulltextové vyhledávání. * Notifikace o směrnici na úvodní stránce. * Diskuze k dokumentům. * Zobrazení PDF dokumentu onsite. |  |  |
| Modul musí umožnit zobrazit a evidovat informace o tom, kdo danou směrnici viděl, kdo potvrdil její přečtení, případně musí umožnit kontrolu přečtení doplnit na závěr dotazníkem. |  |  |
| **Modul vzdělávání a testování** | Součástí modulu musí být systém evidence a nabídky vzdělávání. Modul přímo obsahuje následující bezpečnostní školení a kurzy:   * Kurz Kybernetické bezpečnosti. * Kurz GDPR. * Kurz BOZP. * Kurz PO. * Kurz První pomoc. * Školení referentských řidičů. * Školení vstupního vzdělávání. * Školení základů práce se spisovou službou. |  |  |
| Modul musí umožnit vedení evidence nutných školení a kurzů zaměstnanců v souladu s platnou legislativou. |  |  |
| Modul musí sledovat platnosti provedených školení a kurzů. |  |  |
| Modul musí disponovat nástrojem pro provádění e-learningových školení a kurzů. |  |  |
| Modul musí disponovat nástrojem pro zakončení e-learningových školení a kurzů formou testu. Nástroj musí umožnit automatické vyhodnocení testu. |  |  |
| Modul musí disponovat nástrojem pro automatické vygenerování závěrečného certifikátu ve formátu pdf. |  |  |
| Modul musí umožnit předání a zaevidování informace o absolvovaném školení/kurzu do příslušné evidence. |  |  |
| Modul musí disponovat nástrojem pro tvorbu vlastních kurzů, školení a testů. |  |  |
| Modul musí zasílat notifikace uživateli, který je předmětem události, ale i jeho nadřízenému (tedy jinému uživateli, který má specifickou roli ve vztahu k uživateli, který je předmětem události).  Jednotlivé notifikace je možné dle nastavení časového intervalu seskupovat. Tedy zajistit, aby v případě možnosti výskytu většího množství událostí, které mají na sebe navázanou notifikaci, v krátkém časovém úseku přišel uživateli pouze jeden e-mail shrnující všechny tyto události (například v případě přiřazení 10 vzdělávacích objektů, aby přišel 1 mail o 10 přiřazeních místo 10 mailů o 1 přiřazení). |  |  |
| Modul umožňuje vytvářet bloky jednotlivých vzdělávacích objektů (složené z libovolného množství například kurzů, testů, prezenčních školení, dokumentů, videí…). Bloky mohou obsahovat i další podřízené bloky. S blokem je možné pracovat jako se samostatným objektem. Je tak například možné uživateli či skupině uživatelů přiřadit přístup k celému bloku, namísto nutnosti specificky přiřazovat přístup k jednotlivým vzdělávacím objektům, které tento blok tvoří. |  |  |
|  | Modul disponuje algoritmy, které podle detailně připraveného plánu zasílají pracovníkům testovací emaily nebo email s průvodkou testu. Modul výsledky testování zaměstnanců vyhodnocuje. |  |  |
| V případě, že modul vyhodnotí, že zaměstnanec udělal bezpečnostní chybu, zařadí jej do elearningového kursu. |  |  |
| Modul obsahuje statistiky testování, bezpečnostních incidentů a bezpečnostní rekvalifikace. Součástí jsou reportovací sestavy v BI. |  |  |
| **Modul kontaktů** | Modul pro vyhledání a zobrazení interních a vybraných externích kontaktů. Modul obsahuje skupiny kontaktů pro jednotlivé bezpečnostní a krizové situace. |  |  |
| Modul obsahuje telefonní seznam pracovníků úřadu, který musí umožnit:   * Evidenci interních kontaktů. * Synchronizaci kontaktů z IDM s následnou uživatelskou editací obsahu. * Fulltextové vyhledávání. * Členění do složek (struktura složek musí reflektovat organizační strukturu úřadu). * Oprávnění na úroveň složek nebo jednotlivých záznamů. |  |  |
| Modul obsahuje seznam externích kontaktů, který umožňuje evidovat informace o dodavatelích, partnerech a jiných subjektech. Seznam externích kontaktů musí na základě synchronizace s IDM umožnit:   * Evidenci kontaktů a základních informací o kontaktu (jméno, název, adresa, email apod.) vč. uživatelsky definovaných metadat. * Fulltextové vyhledávání. * Řízení oprávnění přístupu až na úroveň jednotlivých kontaktů. * Vytváření souvislostí mezi kontakty. * Vizualizaci souvislostí mezi kontakty. * Vazbu kontaktu na projekty (investor, objednatel, dodavatel). * Plánování aktivit s kontakty. * Vložení informace o splnění aktivity s kontaktem (telefon, vyřízení požadavku apod.). * Uživatelsky volitelné členění kontaktů do složek. * Řízení oprávnění přístupu po složkách. |  |  |
| **Obecně pro všechny výše zajišťované oblasti** | Licence bude trvalá (perpetual). |  |  |
| Podpora min. 24 měsíců spočívající v nároku na nové a opravné verze. |  |  |
| Názvy modulů jsou orientační a nezávazné. Požadované funkcionality se mohou prolínat v nabízeném řešení a nemusí být takto striktně rozděleny. Všechny uvedené funkcionality však musí být součástí nabízeného řešení. |  |  |