1. Vysvětlení zadávací dokumentace

dle § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ")

Identifikační údaje zadavatele:	**město Ivančice** Sídlo: Palackého náměstí 196/6; 664 91 Ivančice IČO: 00281859
Název veřejné zakázky:	**„Kybernetická bezpečnost Ivančice"** (dále jen předmětná zakázka)
Osoba oprávněná za zadavatele jednat:	Milan Buček, starosta města
Registrační číslo projektu:	CZ.31.2.0/0.0/0.0/23_093/0009398
Spisová značka:	S-MI6387/2025
Identifikační údaje zástupce zadavatele:	AJL, s.r.o. Sídlo: Markova 1965/6, Velké Meziříčí, PSČ: 594 01; IČO: 26933179 Ing. Jiří Žák; Tel.: 604 273 438; e-mail: zak@ajl.cz; ID schránky: attj59a

Vysvětlení zadávací dokumentace:

Zadavatel z důvodu administrativní chyby doplňuje přílohu č. 2 zadávací dokumentace následovně:
V kap. 3.2. VÍCE-FAKTOROVÁ AUTENTIZACE A SINGLE SIGN-ON (SSO) – PRO 160 UŽIVATELŮ (ID2), v tab. č. 2, doplňuje požadavky uvedené v následující tabulce.

č.	Specifikace požadavků.	Účastníkem nabízená hodnota, výrobce a typ.	Splněno [ano/ne]
	Správa privilegovaných identit (PIM)		
37.	Systém musí v této oblasti umožňovat centrální správu účtů a jejich hesel v rámci zabezpečeného úložiště se správou přístupu k těmto účtům (Password Management). Dále zaznamenávání aktivit privilegovaných účtů v rámci relací navázaných přes tento systém formou nahrávky obrazovky a formou kompletního výpisu logů ohledně dění v jednotlivé instanci.		
38.	Řešení poskytuje nástroj pro správu privilegovaných účtů, řízení přístupu k těmto účtům a monitoring veškerých aktivit privilegovaných účtů. Uživatelské přístupy jsou řízeny bezpečnostní politikou, kdy má vybraný uživatel práva přístupu pouze k definovaným účtům a systémům. Účty a systémy, ke kterým nemá práva přístupu, nejsou pro uživatele viditelné.		
39.	Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.		
40.	Řešení umožňuje víceúrovňové schvalování správcovských přístupů k cílovým systémům - přístupy lze omezit dle vybraného účtu, nebo na daný časový úsek. Schvalování přístupu lze vynutit odděleně pro přístup přihlašovacím údajům privilegovaného účtu, nebo pro připojení na koncový systém. O nových žádostech, schválení a zamítnutí budou uživatelé upozornění emailem, vytvořením ticketu v helpdesk systému, atp.		
41.	Řešení zaručuje vysokou bezpečnost přenášených a uložených informací (confidentiality, integrity, availability). Uložené informace, včetně nahrávek a spravovaným přihlašovacích údajů, jsou uloženy v jedné centrální a vysoce zabezpečené databázi. Řešení musí umožňovat omezení práv správce systému tak, aby neměl sám přístup k uloženým přihlašovacím údajům, logům, nebo nahrávkám, bez autorizace vlastníků dat.		
42.	Správa řešení je umožněna pomocí jednotné centrální správy - konzole.		

č.	Specifikace požadavků.	Účastníkem nabízená hodnota, výrobce a typ.	Splněno [ano/ne]
43.	Řešení nabízí plnou integraci se stávající Microsoft Active Directory/ Azure AD. Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS AD a druhým faktorem.		
44.	Nástroj umožňuje vynutit silnou autentizaci uživatelů pro přístup k uloženým údajům i pro bezpečné vzdálené připojení. Silnou autentizací je míněna minimálně možnost kombinace jméno/heslo + druhý faktor (RSA ID, Radius server, telefon, email, Yubikey, Google autheticator,...) (zadavatel umožňuje nabídnout rovnocenné řešení).		
45.	Řešení umožňuje vyhledávat privilegované účty v operačních systémech/LDAP/Active Directory a přidat je (manuálně i automaticky) do systému řízení přístupu dle bezpečnostní politiky. Vyhledávání účtů nevyužívá instalaci agentů na koncová zařízení.		
46.	Řešení umožňuje automatickou výměnu hesel a SSH klíčů privilegovaných účtů po ukončení relace (jednorázové heslo), nebo v pravidelných intervalech dle bezpečnostní politiky. Rotaci hesla/SSH klíče lze vynutit i uživatelem. Hesla a SSH klíče se vyměňují bezagentsky.		
47.	Systém umožňuje pravidelné vyhledávání účtů, které nejsou řešením spravovány, ale jsou používány pro přístupy na koncové systémy. Systém takové účty dokáže vyhledat, upozornit na jejich použití a případně automaticky zařadit do správy. Řešení zároveň umožňuje detekci nespravovaných účtů v reálném čase a automatické uložení a vynucení změny hesla.		
48.	Řešení umožňuje zprostředkovat uživateli bezpečné připojení na vybrané webové aplikace, přístup do cloudu a sociální sítě pomocí webového prohlížeče. Řešení umožní uživateli přihlášení do vybrané webové aplikace pomocí standardního (neprivilegovaného) účtu, systémové rozhraní následně zprostředkuje přihlášení do koncové aplikace pomocí silného "privilegovaného" účtu. Uživatel nemusí znát hesla privilegovaných účtů a je mu umožněno transparentní SSO.		
49.	Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS, není tedy například nutné otevírat z klientské stanice RDP/SSH protokoly.		
50.	Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.		
51.	Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.		
52.	Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.		
53.	Systém musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů v reálném čase pomocí Syslog.		
54.	Systém musí podporovat HA.		
55.	Analýza stávajícího stavu – stanovení soupisu privilegovaných účtů a klíčových systémů a zdrojů zadavatele, stanovení pravidel přidělování přístupů, schvalovací workflow, definice politik rotace hesel, možnosti dočasných hesel a politiky hesel, analýza potřeb v oblasti reportingu a statistických výkazů.		
56.	Příprava HW a SW prostředí - prostupnosti v infrastruktuře, otevření požadovaných portů, otevření DMZ.		
57.	Instalace systému do infrastruktury zadavatele.		
58.	Konfigurace systémů dle výstupů procesní a systémové analýzy a současně napojení superadmin účtu, nastavení politik bezpečnosti, enrollment uživatelů a enrollment zdrojů.		
59.	Tvorba a realizace testovacích scénářů před uvedením systému do produkce.		

č.	Specifikace požadavků.	Účastníkem nabízená hodnota, výrobce a typ.	Splněno [ano/ne]
60.	Kategorizace a prioritizace: Nastavení kategorií, podkategorií a úrovní priority.		
61.	SLA Management: Definování SLA politik a upozornění na porušení časových lhůt.		
62.	Automatizace: Pravidla pro automatickou distribuci ticketů na základě kategorie, priority nebo techniků.		
63.	Databáze řešení: Ukládání častých otázek a řešení problémů.		
64.	Kategorizace znalostí.		
65.	Strukturovaná správa článků podle témat.		
66.	Technici mohou vyhledávat řešení z portálu a posílat jako formou odpovědi žadateli		
67.	Systém umožňuje tvorbu pravidel pro automatizaci zpracování požadavků.		
68.	Automatické přiřazování ticketů konkrétním technikům nebo týmům.		
69.	Systém umožňuje eskalace požadavků na základě časových pravidel nebo neřešených problémů.		
70.	Vytváření předdefinovaných šablon pro různé typy požadavků.		
71.	Systém umožňuje nastavení rolí techniků s různým typem oprávnění: Přidělování rolí technikům (např. admin, technik).		
72.	Technici mohou spravovat úkoly a sledovat své přidělené tickety.		
73.	Sdílení ticketů mezi techniky a týmy.		
74.	Přehled o výkonnosti týmu, splnění SLA a počtu požadavků.		
75.	Možnost vytvoření vlastních reportů podle potřeb.		
76.	Dashboardy - přehledné vizualizace klíčových ukazatelů výkonnosti (KPI).		
77.	Procesní a systémová analýza – definice ukládaných dat, definice oprávněních příslušných uživatelů		
78.	Příprava HW a SW prostředí.		
79.	Instalace systému do infrastruktury zadavatele		
80.	Konfigurace systémů dle výstupů procesní a systémové analýzy a současně stanovení přístupů a rolí.		
81.	Tvorba a realizace testovacích scénářů před uvedením systému do produkce.		
82.	Uvedení do produkčního prostředí.		
83.	Celý systém musí být nativně integrovatelný do IT infrastruktury zadavatele, snadno obsluhovatelný a konfigurovatelný lidskými zdroji zadavatele bez nutnosti žádat o konfigurační úpravy dodavatele.		
84.	Veškeré konfigurační nástroje musí být zadavateli dostupné bez nutnosti zapojení dodavatele.		
85.	Celý systém musí být přístupný z jednotné konzole.		
86.	Zadavatel požaduje stálou (tzv. perpetual) SW licenci, která bude pokrývat IT infrastrukturu popsanou výše.		
87.	Licence musí také pokrývat minimálně 3 interní administrátory (privilegované účty) a 5 externích administrátorů (privilegovaných účtů).		
88.	Podpora výrobce dodávaného SW na dobu 5 let.		

Zadavatel v souvislosti s tímto 1. vysvětlením zadávací dokumentace prodlužuje lhůtu pro podání nabídek, která tímto rozhodnutím končí dne **2. 9. 2025 v 9:00 hodin**. Otevírání nabídek bude zahájeno ihned po uplynutí lhůty pro podání nabídek.

V Ivančicích dne dle el. podpisu.
Podpis oprávněné osoby zadavatele:

Ing. Jiří Žák

Digitálně podepsal Ing. Jiří Žák
Datum: 2025.08.01 14:41:40 +02'00'

……
Milan Buček, starosta města