Příloha č. 1 – Technická specifikace Díla včetně technické části nabídky Zhotovitele

a) Technická specifikace Díla

1. Zkratky, pojmy

Zkratka	Vysvětlení
2FA	Dvou faktorová autentizace
AD	Microsoft Active Directory
HA	Režim vysoké dostupnosti (High Availability), např. prostřednictvím redundance.
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technologies)
IDM	Správa uživatelských účtů (Identity Management).
IS	Informační systém
Jump server	Server zprostředkující veškerou komunikaci do vnitřní sítě izolující přístup uživatele (např. Windows terminál).
Koncový systém	Koncový systém, jehož privilegované účty a relace jsou řízeny pomocí PIM/PAM řešení (např. databáze, aplikace, komunikační a bezpečnostní prvky atd.).
LDAP	Lightweight Directory Access Protocol
OS	Operační Systém
OTP	Jednorázové heslo (One time password)
PAW	Privileged Access Workstation na bázi řešení Microsoft
PIM	Privileged Identity Management
PAM	Privileged Access Management
PIM/PAM	Poptávané řešení v oblasti správy privilegovaných účtů a přístupů (Privileged Identity and Access Management)
Privilegovaný účet	Uživatelský účet informačního systému s širokou nebo neomezenou množinou administrátorských oprávnění, který je zpravidla nepersonalizovaný a může být sdílen mezi vícero uživateli.
RDP	Protokol na přenos vzdálené plochy (Remote Desktop Protocol)
Řešení	Celkové poptávané řešení v oblasti správy privilegovaných účtů a přístupů (Privileged Identity and Access Management)
SSH	Zabezpečený protokol pro připojení k serverům
SSO	Systém jednotného přihlášení (Single Sign-On)

SW	Software
Dodavatel	Subjekt, který byl v rámci tohoto zadávacího řízení o dodávku řešení PIM/PAM vybrán jako vítězný
Uživatel PIM/PAM	Uživatel PIM/PAM je administrátor (interní či externí), který používá PIM/PAM řešení pro přístup k spravovaným koncovým systémům.
Zadavatel	Městská část Praha 1, Vodičkova 681/18, 110 00 Praha 1

2. Účel

Účelem tohoto dokumentu je definovat požadavky na dodávku systému pro řízení přístupu PIM/PAM (Privileged Identity and Access Management – systém pro evidenci, celkové řízení a kontrolu privilegovaných účtů) a s tím souvisejících všech technických komponent potřebných pro správnou funkci. Tento dokument (dále rovněž „Technická specifikace“) je součástí zadávací dokumentace zadávacího řízení „Zvýšení kybernetické bezpečnosti - systém pro řízení přístupu“.

3. Kontext nasazení poptávaného Systému

ICT prostředí Zadavatele je tvořeno množstvím informačních systémů a rozlehlou ICT infrastrukturou. Jednotlivé prvky tohoto prostředí obsahují privilegované účty, které jsou využívány pro jejich administraci, běžnou obsluhu, nebo se jedná o servisní účty. K těmto privilegovaným účtům mají přístup jak interní zaměstnanci, tak externí dodavatelé, kteří se podílejí na provozu a správě ICT systémů Zadavatele.

Cílem Zadavatele je celkově posílit úroveň bezpečnosti, minimalizovat rizika spojená s možným zneužitím nebo nesprávným užitím těchto privilegovaných účtů na všech relevantních ICT a zajistit tak vyšší úroveň ochrany svých kritických systémů. Zároveň sjednotit a formalizovat procesy a začít řídit přístup k privilegovaným účtům pomocí poptávaného technického řešení.

Cílové řešení musí umožnit díky implementaci nástroje PIM/PAM kontrolovat interní i externí (dodavatelské) privilegované účty a u takových vynutit bezpečnou autentizaci s omezením povolených protokolů, zajistit nahrávaní relací (sessions), vynutit schvalovací procesy a další opatření s tím spojená.

4. Struktura a náležitosti technické části nabídky

Uchazeč je povinen v rámci své nabídky vypracovat i technickou část, která bude obsahovat popis následujících oblastí:

1. Položkový seznam SW a případných HW komponent nabízeného řešení ve formě tabulky. U každé uvedené položky (komponenty řešení) bude specifikována technologie na které je komponenta realizována a její licence ve vztahu k Zadavateli (kdo je poskytovatelem licence a v jakém režimu),
2. Diagram navrhované architektury celého nabízeného řešení na dvou úrovních:
    a. Aplikační - ze kterého bude patrný vztah všech navrhovaných SW komponent a jejich vztahů (komunikace). Předpokládá se zpracování jako 1 schéma ve formátu JPG/PNG.
    b. Technologické - ze kterého bude patrný vztah všech navrhovaných HW komponent a jejich vztahů (komunikace) a vztahů k SW komponentám, tj. jaké servery budou potřeba, co je virtuální co fyzický HW, jaký SW na konkrétních serverech bude instalován. Předpokládá se zpracování jako 1 schéma ve formátu JPG/PNG.

3. Návrh harmonogramu projektu implementace (formou Ganttova diagramu), ve členění na etapy dodávky, specifikující vlastní činnost, její počátek a konec a vzájemnou návaznost. Předpokládá se zpracování jako tabulka v excelu nebo JPG/PDF export z libovolného projektového nástroje.

5. Předmět zadávacího řízení – specifikace Díla

Předmětem zadávacího řízení je analýza stávajícího stavu a dále návrh vhodného budoucího stavu – tedy vytvoření koncepce přihlašování privilegovaných uživatelů, nasazení, pořízení potřebných licencí nástroje/platformy, jeho nasazení, testovací provoz, provedení akceptačních testů, ostrý provoz, servisní podpora a rozvoj celkového řešení pro ochranu a řízení privilegovaných účtů (PIM/PAM).

Jako celkový rozsah poptávaného, Zadavatel požaduje:

Dílo

	Činnost	Výstup / Akceptační kritérium
5.1	Návrh architektury řešení PIM/PAM a zpracování před-implementační analýzy	Je dokončený a Zadavatelem akceptovaný dokument.
5.2	Příprava ICT prostředí na straně Zadavatele	Připravené virtuální servery, konektivita, prostupy a další zdroje pro zprovoznění řešení PIM/PAM
5.3	Poskytnutí licencí a instalace PIM/PAM řešení	Zadavatel má k dispozici počet účtů požadovaných v rámci specifikace.
5.4	Integrace s AD/LDAP, prostupy	Nástroj PIM/PAM je integrovaný s AD/LDAP a rozděleny přístupy a role
5.5	Integrace s dalšími infrastrukturními systémy	Systém je integrován se systémy: NTP SMTP Log Management/SIEM
5.6	Integrace s koncovými systémy	Systém je integrován na uvedené systémy.
5.7	Základní implementace	Nástroj PIM/PAM řídí všechny privilegované účty, přístupy a oprávnění.
5.8	Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup	Dokument s navrženým procesem.
5.9	Vytvoření procesu pro nouzový přístup ke koncovému systému v případě celkového nebo částečného výpadku PIM/PAM řešení	Dokument s navrženým procesem.

5.10	Nastavení dodaného PIM/PAM řešení dle technických požadavků	Nástroj PIM/PAM nastavený dle schválené před-implementační analýzy.
5.11	Nastavení reportingu	Jsou funkční reporty v souladu s technickou specifikací.
5.12	Testování řešení PIM/PAM	Nástroj PIM/PAM je otestovaný a plně funkční dle předem schválených akceptačních scénářů. Testy neodhalily žádné incidenty kategorie A a B. Penetrační testy a testy zranitelností neodhalily žádné zranitelnosti/chyby kategorie „kritická“.
5.13	Plán obnovy po havárii (DRP)	Je dokončený a Zadavatelem akceptovaný dokument.
5.14	Dokumentace	Aktuální řídící dokumentace v elektronické podobě (DOCX, XLSX), včetně dokumentace skutečného provedení a příruček jsou dokončené a Zadavatelem akceptované.
5.15	Školení pracovníků Zadavatele	Realizace on-site školení pro interní a externí pracovníky
5.16	Akceptace základní implementace	Plně funkční Nástroj PIM/PAM v rozsahu základní implementace.
5.17	Pilotní provoz a předání do produkčního užívání	Po dobu 15 dnů zpětně k datu vyhodnocení nenastalo více než 3 incidenty kategorie A a ty byly uzavřeny v souladu s SLA parametry dle smlouvy.

Služby podpory

5.18	Realizace Služeb servisní technické podpory

Služby rozvoje

5.19	Realizace služeb metodické podpory Zadavatele

Body 5.1 až 5.17 výše představují realizaci Díla ve smyslu smlouvy o dílo, bod 5.18 výše zahrnuje jak Služby podpory a bod 5.19 Služby rozvoje ve smyslu smlouvy o dílo. Služby podpory jsou blíže specifikovány v čl. 5.18 této přílohy a Služby rozvoje v čl. 5.19 této přílohy.

Popis jednotlivých činností z přehledové tabulky výše

5.1. Návrh architektury řešení PIM/PAM a zpracování před-implementační analýzy

Dodavatel v rámci tohoto kroku provede analýzu a návrh celkové koncepce používání, správy a řízení privilegovaných účtů, které budou do Nástroje PIM/PAM připojeny. Dodavatel navrhne optimální způsob, jak různé typy privilegovaných účtů řídit a spravovat a toto řešení udržovat v čase.

Dodavatel zpracuje dokument, který bude v následující struktuře a bude minimálně obsahovat:

1. Architektura nástroje PIM/PAM
    a. Základní popis nabídnutého nástroje PIM/PAM.
    b. Architektonický model nasazení nástroje PIM/PAM s vysvětlením komponent.
    c. Technologické požadavky na zajištění provozu.
    d. Popis konfigurace komponent nástroje PIM/PAM.
    e. Detailní popis zálohování a obnovy nástroje PIM/PAM, řešení DR scénářů včetně návrhů testovacích scénářů zahrnujících totální výpadek a obnovy do provozního stavu (bude součástí akceptačních testů).
2. Implementace nástroje PIM/PAM
    a. Návrh harmonogramu projektu a procesních kroků pro implementaci nástroje PIM/PAM včetně návrhu konfigurace nástroje PIM/PAM v jednotlivých fázích implementace a definice finální podoby dodávaného nástroje PIM/PAM. Harmonogram bude obsahovat specifikaci výstupů každé etapy.
    b. Návrh postupu testování a návrh konkrétních testovacích scénářů, které pokryjí všechny oblasti testů viz 5.12. tohoto dokumentu.
    c. Návrh procesu technické profylaxe nástroje PIM/PAM ze strany vybraného dodavatele, případně za součinnosti s výrobcem.

5.2. Příprava ICT prostředí na straně Zadavatele

Zadavatel požaduje vybudovat jedno prostředí – produkční. Produkční prostředí bude postupně rozvíjeno v souladu s harmonogramem projektu.

Vybudování testovacího prostředí je ponecháno na doporučení dodavatele. Není cílem Zadavatele vybudovat robustní prostředí, jehož údržba bude nákladná a díky členění interní sítě připojovaných systémů, které by nebyly propojeny do tohoto testovacího prostředí, by ani nemuselo být možné všechny potřebné oblasti testovat.

5.3. Poskytnutí licencí a instalace PIM/PAM řešení

Dodavatel ve své nabídce stanoví a položkově uvede veškeré potřebné licence (SW modulů) vlastního PIM/PAM řešení, jakož i případných jiných komponent, které shledá potřebnými pro jím navržené řešení.

Dodávka všech požadovaných softwarových licencí nezbytných pro provoz Díla na dobu dvanácti (12) měsíců ve formě nevýhradní licence nebo předplatného. Současně s nabízenými licencemi bude poskytnuta i podpora (maintenance) od výrobce po stejnou dobu platnosti; to se vztahuje na všechny softwarové i hardwarové komponenty zahrnuté v nabídce, u nichž je podpora vyžadována. V případě, že není možné nabídnout licence a/nebo podporu na dobu dvanácti (12) měsíců, musí být nabídnuta libovolná delší doba, která uvedené období pokryje.

Dodavatel dále navrhne parametry serverů, potřebných pro běh všech navržených SW komponent řešení, a to formou přehledové tabulky parametrů. Zadavatel předpokládá nasazení do virtuálního prostředí na platformě VMware, které nyní provozuje. SW komponenty dodané v rámci řešení budou instalovány ve výrobcem poskytované poslední stabilní verzi dostupné v době realizace projektu. Dodavatel dále zajistí nasazení a aktivaci všech licencí, resp. licenčních klíčů, pokud bude potřeba. Architektura instalovaného PIM/PAM řešení, včetně identifikace komponent, přehledu instalovaných verzí a použitých licencí a licenčních klíčů bude součástí instalační dokumentace.

5.4. Integrace s AD/LDAP, prostupy

Dodavatel provede nezbytné nastavení řešení tak, aby mohlo být napojeno na MS AD. Zároveň specifikuje požadavky na stranu správy MS AD.

5.5. Integrace s dalšími infrastrukturními systémy

Dodavatel provede integraci na základní infrastrukturní systémy, potřebné pro spolehlivý běh celého řešení, uvedenými v kap. 8.

5.6. Integrace s koncovými systémy

Níže uvedená tabulka uvádí přehled koncových systémů, u kterých je požadováno, aby byly postupně integrovány do PIM/PAM řešení, přístup k jejich privilegovaným účtům byl řízen prostřednictvím PIM/PAM a byly nahrávány relace, přičemž provedení detailní analýzy integrací je součástí Díla v analytické části.

Typ	Koncový systém	Protokol / použití
OS	MS Windows (fyzické a virtuální servery)	RDP, SMB, PowerShell Remoting
	Linux (fyzické a virtuální servery)	SSH
Databáze	Oracle, MS SQL 2016	JDBC, ODBC

		MS SQL studio, DBeaver
Virtualizační prostředí	VMware	HTTPS (vSphere Web Client/API), SSH
Adresářové služby	MS Active Directory, HCL Domino	LDAP, LDAPS, RDP
Storage	IBM Storwize 7300 (Produkce), IBM Storwize 5200(BCK), Synology NAS	SMB/CIFS, NFS, SSH, HTTPS
Vzdálená správa HW	iDRAC (Dell) rozhraní fyzických serverů, SCCM(Intune) u koncových PC	HTTPS, RDP, SSH
Síťové a komunikační prvky	Core Switch + Access Switch od HP enterprise (mohu zaslat detailněji seznam), FW - Fortigate, SAN od IBM (rebrend cisco), Huawei WiFi (zastaralé)	SSH, HTTPS, SNMP
Bezpečnostní prvky	Greycortex, FW FortiGate, AddNet, F5, FortiAnalyzer, Nessus, Bitdefender,	HTTPS, SSH, SNMP

5.7. Základní implementace

Dodavatel provede, v souladu s navrženou etapizací, připojení koncových systémů. U těchto koncových systémů budou připojeny všechny v analýze zjištěné komunikační protokoly, které budou v před-implementační analýze v součinnosti se Zadavatelem odsouhlaseny, jako potřebné v produkčním provozu.

Připojování systémů je možné rozdělit na dílčí pod-etapy, kdy součástí každé takové bude:

a) Dílčí detailní analýza připojovaných typů koncových systémů,

b) Nastavení vlastního prostředí a potřebná úprava PIM/PAM řešení pro připojení,

c) Akceptační testování nově připojovaných koncových systémů.

5.8. Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup

Dodavatel navrhne vhodnou podobu procesu pro schvalování žádosti o privilegovaný přístup. Tento proces upraví v součinnosti se Zadavatelem do takové podoby, aby byl použitelný a nasaditelný v prostředí Zadavatele v době spuštění produkčního provozu projektu. Tento proces bude plně auditován/logován.

5.9. Vytvoření procesu pro nouzový přístup ke koncovému systému v případě celkového nebo částečného výpadku PIM/PAM řešení

Dodavatel navrhne postup pro případ celkového nebo částečného výpadku PIM/PAM řešení – nouzový přístup k cílovému systému v takovém případě. Tento proces bude plně auditován/logován.

5.10. Nastavení dodaného PIM/PAM řešení dle technických požadavků

Dodavatel provede potřebnou konfiguraci PIM/PAM řešení a všech komponent dle požadavků této technické specifikace. V této etapě se bude jednat především o:

a) Technická konfigurace jednotlivých komponent řešení,

b) Navržení a nasazení mechanismu vynucování a kontroly přístupu ke koncovému systému výhradně přes nahrávaný kanál,

c) Nastavení parametrů bezp. politik,

d) Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup,

e) Vytvoření procesu pro nouzový přístup ke koncovému systému v případě celkového nebo částečného výpadku PIM/PAM řešení,

f) Nastavení zálohování konfigurace a dat,

g) Nastavení automatizovaných procesů v oblasti HA/DR

5.11. Nastavení reportingu

Dodavatel provede nastavení reportovací komponenty řešení, aby obsahovala Zadavatelem použitelné a v před-implementační analýze specifikované základní reporty/výstupy.

5.12. Testování řešení PIM/PAM

V rámci etapy před-implementační analýzy budou Dodavatelem navrhnuty testovací scénáře, které budou pokrývat následující oblasti a parametry řešení. V této fázi budou poté fakticky provedeny testy dle navržených scénářů ve všech oblastech.

Dodavatel k realizaci testů zajistí:

- Nástroje a komponenty potřebné pro testování,
- Přípravu návrhu testování a hodnotících kritérií,
- Přípravu testovacích scénářů,
- Přípravu prostředí a testovacích dat (v součinnosti se Zadavatelem),
- Testovací protokoly s výstupy testů,
- Seznam defektů a způsob a harmonogram jejich odstranění.

Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad. Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného PIM/PAM řešení. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Funkční testy

Funkční testy ověří, že implementované PIM/PAM řešení poskytuje bezchybně všechny požadované funkcionality uvedené v této Technické specifikaci, včetně řádné integrace s koncovými systémy Zadavatele. Funkční testy ověří plnou dostupnost koncových systémů dle požadavku na implementaci v rámci jednotlivých etap. Funkční testy musí také zahrnovat scénáře i pro nově navržené procesy, viz 5.8 a 5.9.

Testy zajištění kontinuity (DR testy)

Úlohou testů je ověřit dostupnost PIM/PAM řešení v případě výpadku jednotlivých komponent a ověřit funkčnost Dodavatelem navrženého nouzového přístupu na koncový systém a k databázi hesel v případě nedostupnosti PIM/PAM řešení.

5.13. Plán obnovy po havárii (DRP)

Dodavatel zpracuje postup, který bude aplikován v případě výpadku hlavní instance řešení PIM/PAM a doba výpadku překročí odsouhlasenou kritickou hranici. Postup zároveň bude zahrnovat případ, kdy dojde k neopravitelné havárii řešení a bude nutné jej obnovit ze záložní lokality/kopie.

Dodavatel zpracuje nový interní dokument, který bude v následující struktuře a bude minimálně obsahovat:

- Scénáře obnovy po havárii
- Kompletní výpadek celého nástroje PAM
- Výpadek bezpečného úložiště dat včetně fatálního výpadku, jak primárního, tak sekundárního nodu
- Výpadek webového portálu a scénáře pro přístup k úložišti dat
- Výpadek konektivity a řešení přihlašování privilegovaných uživatelů
- Výpadek přístupu administrátorů k síťovým prvkům (je nutné se k nim připojovat pomocí lokálního fyzického připojení privilegovaným účtem)

5.14. Dokumentace

Dokumentace dodaná v rámci PIM/PAM řešení musí obsahovat jak originální dokumentaci dodávanou výrobcem PIM/PAM řešení, tak i dokumenty popisující nasazení PIM/PAM řešení v prostředí Zadavatele.

Dokumentace produktu k PIM/PAM řešení musí být předána v elektronické podobě (formát PDF nebo MS Word) a musí být provedena v českém jazyce. Dokumentace od výrobce PIM/PAM musí obsahovat minimálně uživatelskou příručku.

Dokumentace popisující nasazení PIM/PAM řešení v prostředí Zadavatele musí být předána v elektronické editovatelné podobě ve formátu MS Word a musí být provedena v českém jazyce. Minimální požadavky na rozsah a obsah dodávané dokumentace je následující:

- Instalační dokumentace:

- Detailní popis instalačních postupů, a to včetně testovacího prostředí.
- Popis architektury,
- Komunikační matice komponent,
- Instalované verze,
- Licence,
- Instalační postup.

- Implementační dokumentace:
  - Popis nastavení komponent PIM/PAM řešení;
  - Popis způsobu integrace (jednotlivých typů koncových systémů);
  - Popis konfigurace zálohování PIM/PAM řešení;
- Uživatelská příručka:
  - Popis uživatelského rozhraní PIM/PAM řešení z pohledu uživatele,
  - Popis uživatelských postupů při práci s PIM/PAM řešením.
- Administrátorská příručka:
  - Popis uživatelského rozhraní PIM/PAM řešení z pohledu administrátora,
  - Popis základních úkonů nutných pro údržbu PIM/PAM řešení a standardní profylaktické testy.
- Zajištění kontinuity provozu:
  - Popis postupu obnovy ze zálohy,
  - Doporučení pro archivaci (nahrané uživatelské relace a související data),
  - Popis postupu v případě havárie jednotlivých komponent včetně postupu obnovy do provozního stavu,

Popis postupu nouzového přístupu ke koncovému systému v případě nedostupnosti/omezené funkčnosti PIM/PAM řešení.

5.15. Školení pracovníků Zadavatele

Dodavatel musí zajistit proškolení odpovědných osob Zadavatele na úrovni administrace řešení v rozsahu umožňujícím provádět:

- Běžný rutinní provoz a údržbu dodávaného PIM/PAM řešení včetně provedení příslušných konfiguračních změn,
- Řešení obvyklých problémů,
- Správu uživatelských oprávnění,
- Analýzu zaznamenaných uživatelských relací,
- Zálohování a obnovu konfigurace a dat,
- Tvorbu pohledů a reportů.

5.16. Akceptace základní implementace

Provedení akceptačních prací dle výsledků akceptačních testů a předání do pilotního provozu.

5.17. Pilotní provoz a předání do produkčního užívání

Po definovanou dobu dle Smlouvy bude řešení provozováno v pilotním režimu, ve kterém platí jiné SLA parametry. Po uplynutí této doby a pokud po dobu 30 dnů zpětně k datu vyhodnocení nenastalo více než 3 incidenty kategorie A a ty byly uzavřeny v souladu s SLA parametry dle smlouvy, bude nasazení označeno za produkční provoz. Tato chvíle bude považována za počátek pro poskytování následných služeb technické podpory provozu.

5.18. Služby servisní technické podpory

Zadavatel požaduje poskytování následujících služeb podpory:

- Služba servisní technické podpory
- Služba metodické podpory Zadavatele

Pro komunikaci v rámci služeb podpory bude se Zadavatelem používán systém Service desk, jehož provoz zajistí Dodavatel. Zadavateli v tomto systému budou zřízeny patřičné účty pro jeho pracovníky. Komunikačním jazykem je český jazyk.

	Služba servisní technické podpory	Služba metodické podpory Zadavatele
Režim poskytování	8 × 5 v pracovní dny	8 × 5
Provozní hodiny	8:00-16:00	8:00-16:00
Reakční lhůta	Dle kategorie chyby	NBD
Doba odstranění vady na produkčním prostředí	Dle kategorie chyby	N/A
Dostupnost systému (měřeno měsíčně)	99,6%	N/A

Dodavatel zabezpečí služby servisní technické podpory pro systém, aby byl zajištěn jeho bezvadný běh a řešení nalezených problémů. Služby servisní technické podpory počínají běžet až od podpisu protokolu o dokončení převzetí díla.

Dodavatel je povinen do 30 pracovních dnů od dostupnosti nového změnového balíčku (opravného balíčku, aktualizace nebo nové verze SW produktu) informovat o této skutečnosti Zadavatele, včetně analýzy dopadů instalace. Zadavatel rozhodne, jestli bude požadovat instalaci, či instalaci odložit a požadovat ji později v průběhu plnění. Po schválení Dodavatelem navržených termínů ze strany Zadavatele, provede Dodavatel instalaci změnového balíku v domluveném termínu, a to nejprve na testovací prostředí a po otestování na produkční prostředí. Dle potřeby poté aktualizuje Dokumentaci (má-li instalace vliv na funkcionalitu nebo jiné zásadní parametry systému).

Provedení aktualizace všech komponent Systému bude provedena minimálně jednou ročně.

V rámci služeb servisní technické podpory budou prováděny pravidelné profylaktické prohlídky a to nejméně jedenkrát za 2 měsíce. Výstupem profylaktické prohlídky je souhrnná zpráva o stavu systému doplněná o případné nálezy a nápravná opatření. Dodavatel následně implementuje nápravná opatření, po dohodě a v součinnosti se Zadavatelem.

Kategorizace chyb:

Kategorie vady	**Popis**	**Reakční lhůty v pracovní době**	**Doba odstranění vady na produkčním prostředí**
Kategorie A	Systém nebo jeho část/služba není použitelná ve svých základních funkcích a parametrech nebo se vyskytuje funkční závada znemožňující činnost a řádné užití Systému nebo jeho části/služby. Tento stav ohrožuje nebo znemožňuje běžný provoz Systému, případně může Zadavateli nebo dalším subjektům způsobit větší finanční nebo jiné škody. Tento stav může ohrozit běžný provoz Zadavatele a nelze jej dočasně řešit organizačním opatřením.	4 hodiny	Do 24 hodin
Kategorie B	Funkčnost Systému nebo jeho části/služby nebo rozsah služeb Zadavatele je ve svých funkcích a parametrech degradována tak, že tento stav omezuje běžný provoz Systému nebo omezuje řádné užití Systému nebo jeho části/služby anebo služeb Zadavatele. Existuje náhradní pracovní postup pro obejití závady, případně organizační opatření.	8 hodin	Do 72 hodin
Kategorie C	Ostatní – drobné závady, které nespadají do kategorie A a/nebo B.	16 hodin	Do 120 hodin

Zařazení nahlášené vady do jednotlivých kategorií navrhuje Zadavatel. Reakční lhůtou se rozumí doba od zahájení požadavku do doby potvrzení zahájení jeho řešení.

5.19. Služba metodické podpory Zadavatele

Realizace služeb metodické podpory v celkovém předpokládaném objemu 12 MD.

Dodavatel zabezpečí služby metodické podpory pro klíčové pracovníky Zadavatele. Službou se rozumí podpora garantovi řešení za stranu Zadavatele, zejména v podobě řešení koncepčních otázek pro rozvoj systému. Službami metodické podpory se předpokládá poskytování zejm. následujících činností:

1. Analýzy a tvorba koncepce pro strategický rozvoj systému.
2. Řešení metodických/technických otázek ze strany Zadavatele.
3. Konzultační pomoc při konfiguraci Systému.

6. Funkční požadavky na systém

Funkční požadavky na systém jsou uvedeny v samostatné Příloze 2 ZD Katalog požadavků.

7. Počet uživatelů

Níže uvedená tabulka uvádí přehled počtu Uživatelů, kteří budou využívat PIM/PAM řešení:

Předpokládaný počet uživatelů přistupujících skrz PAM (mají vždy účet v AD)	Interní administrátoři: min. 20 osob Externí administrátoři: min. 50 osob (aplikací, infrastruktury, bezp. prvků) Technické účty (účet aplikace, služby): cca 50 Technickým účtem se rozumí účet konkrétní aplikace nebo scriptu, který využívá privilegovaný přístup pro své fungování. Cílem je umět poskytovat přihlašovací údaje těmto aplikacím.
Počet současně připojených uživatelů v běžném provozu	Průměrně 10
Počet současně připojených uživatelů ve špičce	Výjimečně až 20
Průměrná délka uživatelské relace za den (tj. kontinuální nepřerušené jedno spojení na aplikaci/prvek)	2 hodiny
Zabezpečený přístup k webovým aplikacím	Min. 20 osob

Celkový počet řízených aplikací/prvků	Min. 250

8. Integrace na okolní IS

Je požadováno sytém integrovat na níže uvedené IS, přičemž provedení detailní analýzy integrací (např. přenosový protokol, přesný formát předávaných dat, atp.) je součástí Díla v analytické části.

Systém	Popis
Microsoft AD	Doménový řadič za účelem poskytnutí informací o identitách/účtech. Přímá integrace nativním protokolem.
NTP server	Pro synchronizaci systémového času. Možno využít z MS AD.
SMTP	Email server pro odesílání notifikací. Pomocí protokolu SMTP.
Provozní monitoring	Pro kontrolu běhu a výpadků. Pomocí protokolu SNMP.
Log management / SIEM	Pro zasílání logů o své činnosti. Odesílání pomocí protokolu syslog / TLS syslog.
Okolní IS s řízenými účty	Viz kap. 0

b) Technická část nabídky Zhotovitele

Technická část nabídky dle čl. 14.2.2 ZD

Popis nabízeného řešení

BeyondTrust Total PASM je řešení kategorie Privileged Access Management (PAM) pro řízení privilegovaných účtů a přístupů administrátorů a externích správců. Klíčovou komponentou je Password Safe pro centrální správu hesel a účtů. Řešení umožňuje zejména:

- správu a řízení využití privilegovaných účtů (včetně sdílených účtů) a bezpečné ukládání přístupových údajů do centrálního vaultu,
- auditní stopu a dohledatelnost činností administrátorů a externích správců (včetně záznamu a řízení relací),
- zprostředkování řízeného vzdáleného přístupu (např. RDP, SSH, web) včetně přístupu dodavatelů prostřednictvím webového portálu,
- integraci s podnikovými službami (identity/AD/LDAP, čas, notifikace, logování/SIEM a monitoring),
- možnost postupného rozšiřování konektorů a spravovaných cílů dle potřeb Zadavatele.

Položkový seznam SW a HW komponent nabízeného řešení

Nabízené řešení je dodáváno jako kompletní (all-in-one) ve formě virtuálních appliance (VM). Z tohoto důvodu není součástí nabídky samostatný HW server ani separátní systémové SW komponenty (operační systém, databáze) – vše je zahrnuto v dodaných appliance. Provoz bude zajištěn na virtualizační infrastruktuře Zadavatele.

Položka (komponenta)	Popis / účel komponenty	Technologie (realizace)	Poskytovatel licence	Licenční režim / vztah k Zadavateli	Množství
BeyondTrust Appliance B Series (VM)	Appliance pro Password Safe – centrální vault, správa účtů a rotace hesel	Virtuální appliance (VM image) provozovaná na virtualizační platformě Zadavatele	BeyondTrust (dodávka prostřednictvím autorizovaného kanálu)	Předplatné (subscription) – licence poskytnutá Zadavateli na dobu trvání předplatného	1

BeyondTrust Appliance U Series 2022 (VM)	Appliance pro Privilege Remote Access (PRA) – vzdálený přístup, řízení relací, Jumpoint	Virtuální appliance (VM image) provozovaná na virtualizační platformě Zadavatele	BeyondTrust (dodávka prostřednictvím autorizovaného kanálu)	Předplatné (subscription) – licence poskytnutá Zadavateli na dobu trvání předplatného	1
Total PASM – Per Asset Subscription	Licencování dle počtu spravovaných aktiv (assetů)	SW funkcionalita v rámci nasazených appliance	BeyondTrust	Předplatné 'per asset' - licence poskytnuta Zadavateli pro definovaný počet aktiv	250 aktiv

*Poznámka k HW komponentám: Součástí nabídky není samostatný HW – řešení je provozováno jako VM na infrastruktuře Zadavatele (výpočetní výkon, paměť, úložiště a síťové prostředky dle požadavků na sizing).

Požadavky na zdroje (výpočetní a diskové kapacity)

Komponenta	vCPU	RAM	Diskový prostor
BeyondTrust Password Safe (PASM / PAM Core)	4	16 GB	500 GB
BeyondTrust Privileged Remote Access (PRA)	4	16 GB	300 GB

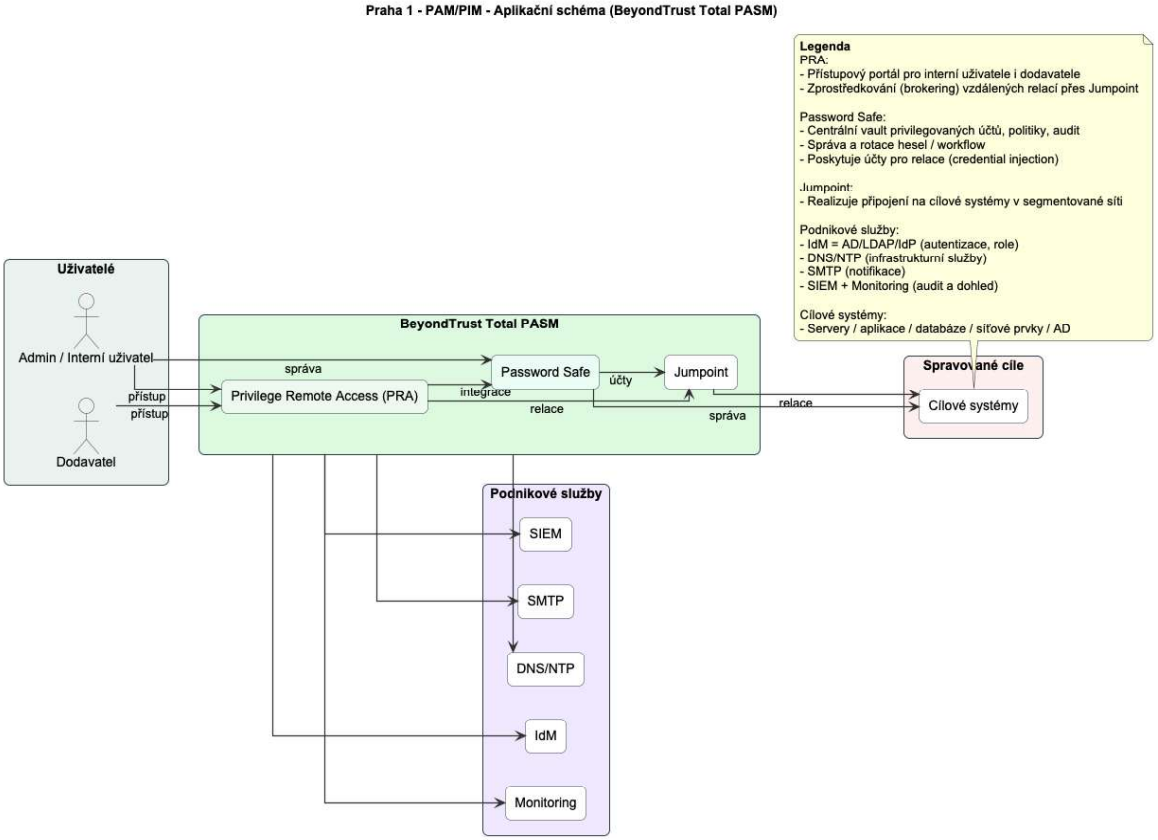
Pozn.: Uvedené hodnoty představují minimální dimenzování pro standardní produkční nasazení; skutečná dostupnost a výkon jsou závislé na parametrech a dostupnosti podkladové virtualizační infrastruktury Zadavatele. Přesné zdroje budou potvrzeny se Zadavatelem v rámci před-implementační analýzy.

Diagram navrhované architektury celého nabízeného řešení

Aplikační architektura

Schéma níže znázorňuje logické vazby komponent řešení BeyondTrust Total PASM a hlavní toky komunikace z pohledu funkcí PAM.

- Uživatelé (interní administrátoři a externí dodavatelé) přistupují do řešení přes komponentu Privilege Remote Access (PRA) prostřednictvím zabezpečeného webového rozhraní.
- Komponenta Password Safe zajišťuje centrální vault pro privilegované účty, politiky a workflow, včetně správy a rotace hesel.
- PRA využívá účty z Password Safe trezoru a ve spolupráci s komponentou Jumpoint zprostředkovává řízené relace na spravované cíle.
- Password Safe komunikuje se spravovanými cíli pro účely správy účtů a rotace hesel.
- Řešení je integrováno s podnikovými službami Zadavatele (AD/LDAP/IdP, DNS/NTP, SMTP) a se systémy SIEM/monitoring pro auditní záznamy a dohled.



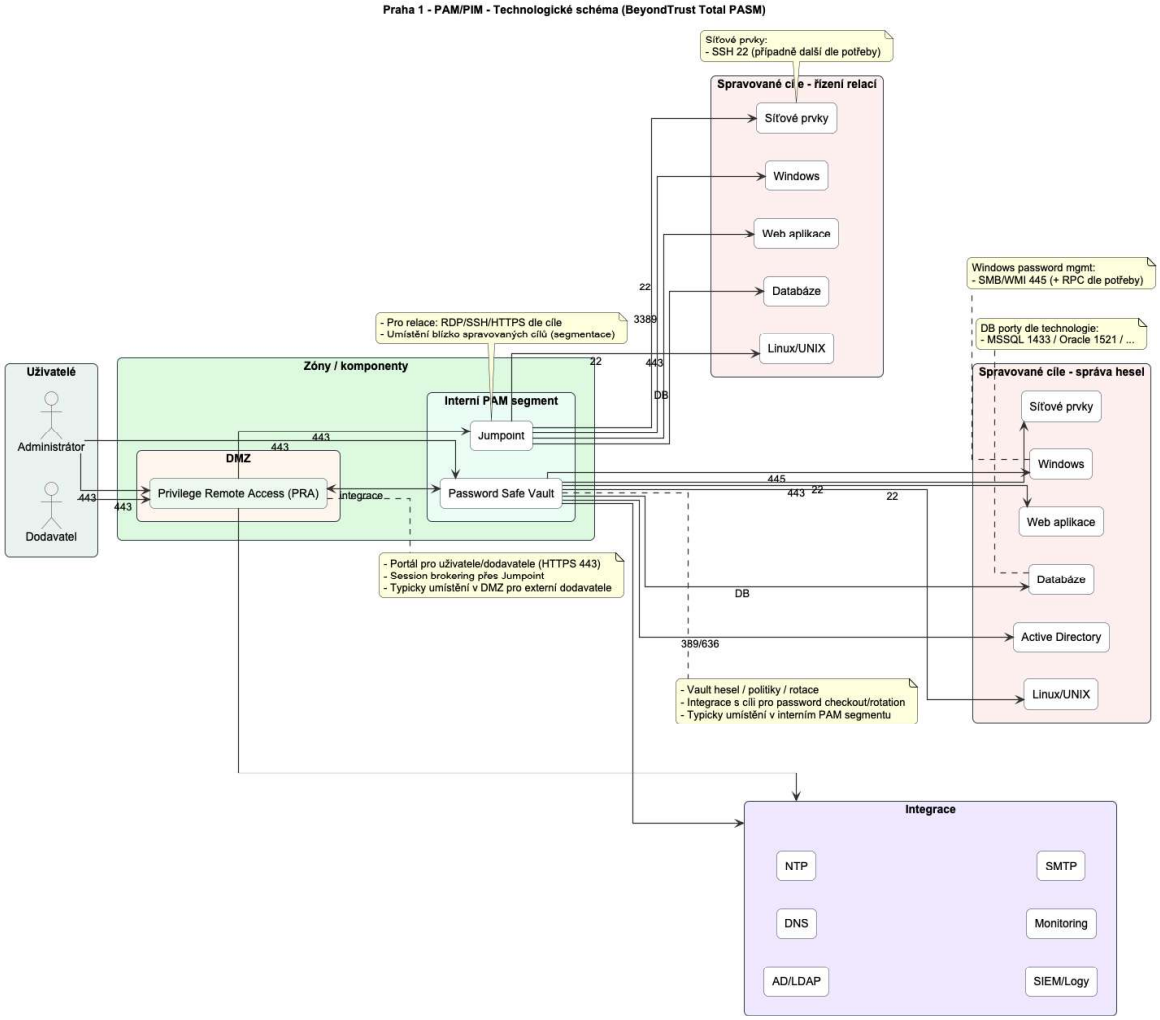
Technologická architektura

Navržené řešení je tvořeno komponentami BeyondTrust Total PASM provozovanými v infrastruktuře Zadavatele, s oddělením do bezpečnostních zón DMZ a interního PAM segmentu. Schéma níže znázorňuje umístění jednotlivých komponent, jejich vzájemné vazby a vazby na podnikové služby a spravované cíle.

Komponenty řešení a jejich role:

- Privilege Remote Access (PRA) – DMZ: přístupový portál pro uživatele a dodavatele, zprostředkování vzdálených relací.
- Password Safe Vault – interní PAM segment: centrální úložiště (vault) privilegovaných účtů, politiky, audit, správa a rotace hesel.

- Jumpoint – interní segment / blízko spravovaných cílů: softwarová komponenta realizující připojení (relace) na spravované cíle v segmentované síti.



Příloha č. 2 – Popis požadovaných vlastností Díla

Povinné funkční vlastnosti - Správa privilegovaných účtů
Obecné vlastnosti
Systém musí umožňovat centrální správu účtů a jejich hesel v rámci zabezpečeného úložiště se správou přístupu k těmto účtům (Password Management).
Systém umožňuje zaznamenávání aktivit privilegovaných účtů v rámci relací navázaných přes tento systém formou nahrávky obrazovky a formou kompletního výpisu činností (logu) ohledně dění v jednotlivé instanci.
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.
Systém plně podporuje multi-tenant prostředí. Uživatelé/skupiny uživatelů mají přístup pouze k vybraným účtům, systémům, auditním záznamům, konfiguraci daného prvku. I správce/administrátor řešení má povolen přístup pouze k vybraným složkám a konfiguraci.
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.
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 dodatečné autorizace (dle nastaveného procesu).
Správa řešení je umožněna pomocí jednotné centrální správy - konzole.
Řešení nabízí plnou integraci s Microsoft Active Directory/ Entra ID. Přístup k uživatelskému rozhraní je požadovaný přes webový portál s možností ověření přes LDAP/MS AD a druhým faktorem.
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, či podobné).
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.
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.

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.
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.
Řešení poskytuje možnost připojení na vzdálené relace pouze pomocí prohlížeče a protokolu HTTPS, není tedy nutné otevírat z klientské stanice např. RDP/SSH sessions.
Systém musí umožňovat audit jednotlivých akcí uživatelů s privilegovanými účty - zobrazení hesla, změny uložených údajů, vytvoření relace.
Řešení musí umožňovat vygenerování reportu veškerých aktivit administrátora řešení.
Řešení umožňuje nastavení přístupu k reportům pouze pro vybrané uživatele.
Systém musí umožňovat integraci s nástroji SIEM - přenos logovaných auditních záznamů v reálném čase pomocí Syslog.
Systém musí podporovat HA.
Reporty
Systém umožňuje generování reportů - přehled realizovaných spojení za dané období, včetně doplňujících dat (uživatel, koncový sysstém, datum, čas)
Možnost vytvoření vlastních reportů podle potřeb.
Dashboardy - přehledné vizualizace právě probíhajících anebo historických událostí.

Příloha č. 3 – Nabídková cena

Cenová tabulka					
Položka	**Počet jednotek**	**Cena v Kč za jednotku bez DPH**	**Cena celkem v Kč bez DPH**	**DPH celkem**	**Cena celkem v Kč vč. DPH**
Nabídková cena (cena Díla)	1	2 342 789,00 Kč	2 342 789,00 Kč	491 985,69 Kč	2 834 774,69 Kč
Cena Služeb servisní podpory (kalendářní měsíc)	12	3 600,00 Kč	43 200,00 Kč	9 072,00 Kč	52 272,00 Kč
Cena Služeb servisního rozvoje (manday)	12	8 400,00 Kč	100 800,00 Kč	21 168,00 Kč	121 968,00 Kč
		Celková nabídková cena	**2 486 789,00 Kč**	**522 225,69 Kč**	**3 009 014,69 Kč**

Příloha č. 4 – Čestné prohlášení – potvrzení výrobce

ČESTNÉ PROHLÁŠENÍ

Společnost **Avenet Distribution s.r.o**, IČO: 05327814 tímto čestně prohlašuje, že dodávaná licence a maintenance (softwarová podpora):

1. je poskytována pod oficiální a garantovanou podporou lokálního zastoupení výrobce,
2. pochází z oficiálního distribučního kanálu výrobce, a
3. je řádně evidována / uvedena v systémech výrobce (tj. je dohledatelná a registrovatelná u výrobce).

Toto čestné prohlášení je vydáno pro účely účasti dodavatele ve veřejné zakázce s názvem „Zvýšení kybernetické bezpečnosti – systém pro řízení přístupu", zadavatele: Městská část Praha 1, IČO 000 63 410, se sídlem Vodičkova 681/18, 110 00 Praha 1

V Praze dne: dle el. podpisu

Za Avenet Distribution s.r.o.

Ing. Dan Kocour

Digitally signed by Ing. Dan Kocour
Date: 2026.01.13 20:24:29 +01'00'

.....

Ing. Dan Kocour
Jednatel

BeyondTrust

August 25, 2025

RE: Authorization to Distribute BeyondTrust products

To Whom It May Concern:

This letter is to confirm that Avenet Distribution s.r.o. ("Avenet") is a fully authorized Value-Added Distributor partner of BeyondTrust Corporation ("BeyondTrust"). Avenet is authorized to resell BeyondTrust's software and services pursuant to the Value- Added Distributor Agreement entered into between BeyondTrust and Avenet dated May 17, 2021.

Avenet is authorized to resell to the country(ies) identified in the Partner Portal ("Partner Portal" means the website for BeyondTrust partners at, https://privilegepartners.beyondtrust.com/prm/api/objects/v1/asset/44i0f55ok3lx/_download) where the partner is authorized, solely by BeyondTrust, to market and sell the offerings. Under no circumstances shall the territory include any region or country where the United States government prohibits sales by US based companies, and any region or country designated as such by BeyondTrust or the United States government, after the Territory is determined shall automatically be removed without further action by the parties.

BeyondTrust regularly reviews its product portfolio to ensure we are providing the best Privileged Access Management products to our customers. Where feasible, BeyondTrust will provide notification to customers about the end of sale of a product or service. All customers with active maintenance contracts for the affected product or service will be notified via email communication. Additional information on BeyondTrust's End of Life Policy can be found at https://www.beyondtrust.com/docs/eol/index.htm.

For further verification, please feel free to contact Ysabelle Marie, Partner Ops Analyst, at ymarie@beyondtrust.com.

Best regards,

Melissa Thibodeau
Contracts Manager

beyondtrust.com
11695 Johns Creek Parkway | Suite 200 |Johns Creek | GA 30097

Příloha č. 5 – Etalon minimální bezpečnosti informací

1 Účel a cíle

Etalon minimální bezpečnosti informací pro poskytovatele MČ Praha 1 tvoří soubor pravidel a postupů, které stanovují požadovanou minimální úroveň bezpečnosti informací.

Dodržování pravidel uvedených v dokumentu je povinné pro všechny partnery spolupracující na smluvní bázi s MČ Praha 1, pro všechny jejich zaměstnance či osoby spolupracující se smluvními partnery.

Etalon minimální bezpečnosti informací pro poskytovatele MČ Praha 1 se na některých místech odkazuje na platné dokumenty o ICT a o bezpečnosti informací na MČ.

Používané i nově zaváděné informační systémy v rámci MČ Praha 1 musí být upraveny, vyvíjeny nebo vybírány tak, aby splňovaly zásady bezpečnosti informací v souladu s tímto dokumentem a se základním dokumentem pro bezpečnost informací MČ Praha 1, tj. Politikou bezpečnosti informací MČ Praha 1 ze dne 6. 11. 2018.

Cílem etalonu minimální bezpečnosti pro smluvní partnery obecně je:

a) Specifikovat základní pravidla a požadavky bezpečnosti informací MČ Praha 1 pro smluvní partnery;
b) Předcházet porušování platných právních předpisů ČR;
c) Zamezit, příp. minimalizovat možnost finanční, majetkové a nemajetkové újmy MČ Praha 1;
d) Zabránit neautorizovanému přístupu k informacím MČ Praha 1;
e) Umožnit řízení bezpečnosti informací MČ Praha 1 ve vztahu s poskytovateli;
f) Zajistit dostupnost informací pro oprávněné uživatele a procesy;
g) Zabránit neautorizované modifikaci nebo zneužití dat a informací;
h) Definovat základní pravidla bezpečnosti v oblasti vývoje a dodávek prostředí IT;
i) Umožnit monitorování a vyhodnocování stavu bezpečnosti.

Výklad použitých zkratek:

BP	bezpečnostní politika informačního systému veřejné správy
ICT	informační a komunikační technologie (Information and Communication Technology)
IS	informační systém (obecně)
ISVS	informační systém veřejné správy (viz § 3 odst. 1 zák. č. 365/2000 Sb.)
MČ Praha1	Městská část Praha 1
ÚMČ Praha 1	Úřad městské části Praha 1
SŘBI / ISMS	systém řízení bezpečnosti informací, ustanovený na základě požadavků IEC 27001
MBI	Manažer bezpečnosti informací ÚMČ Praha 1
Zákon o ISVS	Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění
HelpDesk	primární, centrální bod pro kontakt se všemi uživateli IS/ICT a informačních služeb za účelem hlášení chyb, nedostatků i námětů pro rozvoj řešení
NTB	notebook

2 Bezpečnost informací

Bezpečností informací se rozumí zajištění třech hlavních aspektů – důvěrnosti, dostupnosti a integrity informací v duchu požadavků a doporučení norem řady ISO/IEC 27000.
K zajištění výše uvedených aspektů bezpečnosti informací musí poskytovatel použít a řídit vhodná bezpečnostní opatření, zahrnující jak technické, tak organizační opatření, zohledňující rozsah hrozeb souvisejících s předmětem dodávky.

3 Obecné povinnosti

Mezi odpovědnosti smluvních partnerů patří zejména:

a) Dodržování platných právních předpisů ČR k zajištění bezpečnosti informací;
b) Využívání informačních systémů MČ Praha 1 a jejich komponent v souladu s provozní a bezpečnostní dokumentací MČ Praha 1;
c) Používání informačních aktiv a ostatních aktiv MČ Praha 1 pouze v souladu s určeným rozsahem přístupových oprávnění a pouze ke schváleným účelům;
d) Zajištění ochrany autentizačních údajů (login, heslo, identifikační předmět) k informačním systémům a zařízením MČ Praha 1, které byly smluvnímu partnerovi svěřené, příp. těch, ke kterým má přístup při naplňování smluvního vztahu;
e) Odpovědnost za každý přístup k informačním aktivům a dalším aktivům, provedený prostřednictvím jejich autentizačních údajů;
f) Respektování a dodržování všech bezpečnostních opatření, pravidel a procedur, stanovených vlastníkem informací, tj. MČ Praha 1, se kterými partnera vlastník informací prokazatelně seznámí;
g) Odpovědnost za dostatečné proškolení svých zaměstnanců a pracovníků svých subposkytovatelů v oblasti zajištění bezpečnosti informací MČ Praha 1;
h) Odstraňovat zranitelnosti všech aplikací/komponent, které jsou nezbytné pro funkčnost daného SW/HW.
i) V případě vzniku bezpečnostního incidentu přijmutí nezbytných opatření k eliminaci dopadů tohoto incidentu a neprodlené informování MČ Praha 1.

3.1 Poskytování informací třetím stranám

a) Smluvní partneři jsou povinni dodržovat mlčenlivost o skutečnostech, které se dozvěděli při výkonu své činnosti na základě uzavřené smlouvy s MČ Praha 1.
b) Každé případné veřejné použití neveřejných informací MČ Praha 1 musí být schváleno vedoucím Odboru informatiky MČ Praha 1.

4 Bezpečnost HW, SW a komunikací

Smluvní partneři MČ Praha 1 musí chránit aktiva MČ Praha 1, která používají při své práci nebo naplňování smluvního vztahu a zabránit podle svých nejlepších možností a schopností jejich poškození, zneužití a/nebo odcizení.

4.1 Koncové pracovní stanice

Při práci na koncových stanicích nebo zařízeních smluvních partnerů, ze kterých se přistupuje do vnitřní sítě MČ Praha 1, musí být splněna nejméně následující bezpečnostní pravidla:

a) Použití koncového zařízení (počítače) musí být umožněno pouze oprávněné osobě; (Osoba oprávněná k použití koncového zařízení musí být vybavena přístupovými oprávněními.)
b) Je zakázáno připojovat soukromé počítače do vnitřní sítě MČ Praha 1 bez vědomí oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;
c) Koncová zařízení (pracovní stanice, NTB) nesmí být ponechána bez dozoru zapnutá a s přihlášeným uživatelem (k aplikaci, k IS); za minimální opatření se považuje „uzamčení" pracovní stanice (v každém případě je třeba minimalizovat možnost fyzického přístupu neoprávněným osobám);
d) Počítače smluvního partnera, které mají být připojeny do vnitřní sítě ÚMČ Praha 1, musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází virových definic (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále je smluvní partner též zodpovědný za pravidelnou bezpečnostní aktualizaci operačních systémů a všech dalších komponent, která se na daném zařízení vyskytují a mohli by být potencionálně zneužity pro kybernetický útok na těchto svých počítačích;
e) V případě ukončení práce se zařízením je smluvní partner povinen provést odhlášení od systému.

V případě, že smluvní partner vykonává svoji činnost též na ICT prostředcích nacházejících se na ÚMČ Praha 1, je povinen chránit vybavení ÚMČ Praha 1 a udržovat bezpečné pracovní prostředí. V blízkosti prostředků informačních technologií je zakázáno jíst, pít a kouřit.

4.2 Využívání prostředků a internetu

Systémy MČ Praha 1, vztahující se k počítačové síti, internetu, intranetu, počítačovému vybavení, k operačním systémům a médiím pro ukládání dat apod., jsou ve vlastnictví MČ Praha 1. Tyto systémy mohou být používány pouze pro pracovní účely tak, aby to sloužilo zájmům MČ Praha 1.

Smluvní partneři mají povoleno používání internetového připojení do a z vnitřní sítě MČ Praha 1 pouze za účelem plnění pracovních záležitostí v rozsahu smluvního vztahu. Způsob připojení a autentizace musí být předem dohodnuty s Odborem informatiky ÚMČ Praha 1.

Obecně platí povinnost, že smluvní partner předem oznamuje datum a čas přihlášení k vnitřnímu prostředí a následné ukončení práce ve vnitřním prostředí systémů MČ Praha 1, ledaže se smluvní strany dohodnou jinak.

5 Bezpečnost IS / IT systémů

U vyvíjených nebo dodávaných informačních systémů, jejich HW/SW komponent, musí být zajištěna níže uvedená pravidla:

5.1 Řízení přístupu k informačním systémům a aplikacím

a) Informační systémy a aplikace by měly být vytvářeny tak, aby byl vždy vyžadován autorizovaný přístup uživatelů (identifikační a autentizační údaje) a měla by být zaznamenávána činnost uživatele v aplikaci/systému;
b) Pokud to systém umožňuje, použít více faktorovou autentizaci na základě požadavku MČ Prahy 1
c) Uživatel informačního systému případně aplikace by měl být nucen si své přístupové heslo pravidelně měnit;
d) Informační systémy a aplikace, které nepřebírají přihlašovací údaje z Active Directory MČ Praha 1, by měly být vytvořeny tak, aby byl počet neúspěšných pokusů o přihlášení omezen. Po třech

neúspěšných pokusech o přihlášení musí být další zadávání hesla dočasně omezeno nebo činnost ukončena.

e) Pokud je při přihlašování do aplikace či informačního systému některá část přihlašovacích údajů chybná, nesmí být přihlašovateli poskytnuta informace, kde je chyba v přihlašovacích údajích;

f) V případě, že je povolen přístup do aplikace či informačního systému, který nepřebírá přihlašovací údaje z Active Directory MČ Praha 1, a v němž iniciační (vstupní) heslo určuje administrátor, měl by informační systém či aplikace vynutit změnu tohoto iniciačního hesla při prvním přihlášení uživatele;

g) Všichni uživatelé by měli při své činnosti používat jedinečný identifikátor tak, aby bylo možné vysledovat odpovědnost jednotlivců za prováděné činnosti;

h) Každý pracovník na straně smluvního partnera, který pracuje s informačním systémem či aplikací, musí používat svůj vlastní přihlašovací identifikátor. (Smluvní partner tedy nemůže používat jeden přihlašovací identifikátor pro několik svých zaměstnanců.) Dále smluvní partner odpovídá za veškeré úkony provedené v aplikaci či informačním systému pracovníkem přihlášeným pod tímto identifikátorem;

i) Systém správy hesel by měl být podpořen efektivním a interaktivním vybavením, které prosazuje a vynucuje požadovanou kvalitu hesel;

j) U každého uživatele systému musí být možné identifikovat, jaká přístupová práva má přidělena;

k) Pro každý prostředek systému musí být možné vytvořit seznam uživatelů, kteří mají přístupová práva k tomuto prostředku, s rozlišením druhu přístupových práv (čtení, zápis, editace, ...);

l) Informační systém musí mít mechanismus pro odejmutí všech přístupových práv konkrétnímu uživateli nebo celé skupině uživatelů.

5.2 Monitorování používání systému a přístupu k systému

Přístup poskytovatele do prostředí MČP1 je povolen pouze za podmínek stanovených Odborem informatiky ÚMČ Praha 1 a je monitorován. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, případně bezpečnostním správcem systému.

V informačním systému (případně v jeho jednotlivých součástech) musí být pořizovány auditní záznamy. Tyto záznamy by měly obsahovat údaje a informace, které jsou nezbytné k identifikaci aktivit sledovaného uživatele (jeho identifikační údaje, datum a čas přihlášení a odhlášení apod.)

6 Bezpečnost informací a dat

6.1 Kontrola správnosti dat

Data vstupující do systémů musí být kontrolována tak, aby byla zajištěna jejich maximální správnost. V aplikaci by se měl evidovat identifikátor uživatele nebo procesu, který pořízení nebo změnu dat provedl.

Pokud bude usouzeno, že vytvářený informační systém nebo aplikace by měla podporovat (využívat) kryptografické prostředky pro zajištění integrity dat, je nezbytné, aby aplikované prostředky byly podporovány mezinárodně uznávanými standardy a byly dodrženy právní předpisy České republiky.

6.2 Data / informace předávané smluvním partnerům

Jedná se o informace předávané MČ Praha 1 smluvnímu partnerovi na jakémkoliv nosiči a v jakékoliv formě, zejména listiny a dokumenty, CD ROM, Flash disky, pevné disky, nebo informace zaslané emailem.

Dále se jedná o jakékoliv informace a data MČ Praha 1, se kterými se smluvní partner seznámí nebo k nim má přístup na základě realizace činností prováděných v rámci smluvního vztahu.

Smluvní partner musí s informacemi nakládat v souladu s následujícími ustanoveními tohoto dokumentu, pokud není smlouvou stanoveno jinak:

a) Předání, resp. poskytnutí nebo přístup k informacím (datům) musí být vymezeno ve smlouvě (struktura dat, způsob předání/ poskytování, způsoby ochrany, ...) a musí probíhat řízeným a bezpečným způsobem;
b) Uchovávání a případné zpracovávání dat u smluvního partnera musí být prováděno tak, aby byla zajištěna jejich ochrana dle pravidel stanovených v bezpečnostní dokumentaci MČ Praha 1 (se kterými byl smluvní partner prokazatelně seznámen). Uchovávání a zpracování dat musí být ochráněno před neoprávněným přístupem a možným zneužitím – v souladu s bezpečnostními požadavky MČ Praha 1;
c) Zodpovědnost za ochranu informací (dat) má smluvní partner;
d) Informace (data), která již nejsou potřeba pro účely vymezené smluvním vztahem, musí být smluvním partnerem bezpečně zlikvidována, včetně jejich nosičů. Pro likvidaci nosičů obsahující neveřejné informace MČ Praha 1 musí být zvolena metoda, zaručující, že takto zlikvidované informace (data) nelze běžně dostupnými prostředky obnovit (např. skartovače, SW skartovače dat, ...); provedení likvidace doloží partner protokolem o jejich zlikvidování;
e) Každé nové předání informací (dat) nebo zřízení dálkového přístupu k informačnímu systému nebo databázi na smluvním základě musí být konzultováno s manažerem bezpečnosti informací MČ Praha 1, případně s bezpečnostním správcem systému MČ Praha 1;
f) Smluvní partner si nesmí bez písemného souhlasu MČ Praha 1 sám „stahovat“ (získávat) žádná data z informačních systémů MČ Praha 1. Data může uchovat pouze po nezbytně nutnou dobu.
g) Informace (data), která jsou součástí řešení, vytvářeného smluvním partnerem, nebo jsou předávána na základě realizace činností prováděných partnerem v rámci smluvního vztahu, se budou předávat pouze na vyžádání oprávněného pracovníka MČ Praha 1.

7 Pravidla pro vzdálený přístup do informačního systému

Vzdálený přístup do informačního systému je poskytován výhradně smluvnímu partnerovi, resp. pracovníkům smluvního partnera a nelze ho dále převádět na jiné osoby, a to ani z části. Porušení této povinnosti je považováno za závažné porušení smlouvy.

Smluvní partner se zavazuje, že vzdálený přístup do informačního systému bude používat výhradně za účelem konání prací specifikovaných ve smlouvě. Porušení této povinnosti je považováno za závažné porušení smlouvy.

Smluvní partner, resp. pracovníci smluvního partnera, jsou povinni dodržovat pravidla pro vzdálený přístup do informačního systému (bod 7.1). Porušení jakékoli povinnosti uvedené v těchto pravidlech se považuje za závažné porušení smlouvy.

7.1 Přístup smluvního partnera (poskytovatele) do informačních systémů – podmínky:

a) Pracovník poskytovatele, za účelem zřízení vzdáleného přístupu do informačního systému a možnosti se do tohoto systému přihlásit a pohybovat se v něm, obdrží e-mailem od pracovníka informatiky MČ Prahy 1 přihlašovací jméno, certifikát a prostřednictvím SMS zprávy heslo, které je z důvodu bezpečnosti generované a pracovník poskytovatele ho musí změnit za bezpečné heslo.

Pracovník poskytovatele musí heslo udržovat v tajnosti a nesmí jej zpřístupnit třetí osobě nebo jej využít pro soukromé účely.

b) Vzdálený přístup k informačnímu systému MČ Praha 1 musí být chráněn kryptografickými prostředky, v současné době je přístup realizován pomocí klienta SSL VPN.

c) Po ukončení konání prací ve vzdáleném přístupu do informačního systému za účelem plnění smlouvy je pracovník poskytovatele vždy povinen se odhlásit.

d) Pracovník poskytovatele musí dodržovat pravidla bezpečnosti práce na svém počítači (stolní PC, notebook), ze kterého realizuje vzdálený přístup do informačního systému. Tento počítač musí mít aktivní ochranu před škodlivými kódy (antivirový program) v aktuální verzi databází (tento antivirový program by měl být v maximální míře aktualizován vůči všem známým virům). Dále musí tento počítač mít aktualizovaný operační systém a další obslužný SW.

e) Pracovník poskytovatele se nesmí pokoušet přistupovat na jiné servery než ty, které mu byly přiděleny v rámci vykonávaných smluvních prací, aktivita na účtě může být monitorována.

f) Ukončení pracovního poměru pracovníka poskytovatele s poskytovatelem je poskytovatel povinen písemně oznámit odpovědným pracovníkům Odboru informatiky ÚMČ Praha 1 nejpozději 5 pracovních dnů po ukončení tohoto pracovního poměru, přičemž Odbor informatiky ÚMČ Praha 1 je oprávněn vzdálený přístup do informačního systému pracovníkovi poskytovatele bez dalšího prodlení s okamžitou platností zrušit, při neoznámení této skutečnosti nese poskytovatel plnou zodpovědnost za činnost tohoto bývalého pracovníka.

g) V případě, že pracovník poskytovatele poruší kterékoli ujednání těchto pravidel, je Odbor informatiky UMČ Praha 1 oprávněn okamžitě po zjištění porušení těchto pravidel zrušit tomuto pracovníkovi poskytovatele vzdálený přístup do informačního systému bez dalšího prodlení. Poskytovatel se zavazuje nejpozději do 5 kalendářních dnů ode dne, kdy mu Odbor informatiky ÚMČ Praha 1 oznámil toto zrušení, zajistit plnění smlouvy, potažmo této dohody, jiným zaměstnancem poskytovatele, a o této výměně neprodleně písemně informovat Odbor informatiky ÚMČ Praha 1, přičemž tato výměna podléhá schválení Odborem informatiky ÚMČ Praha 1.

Vzdálený přístup poskytovatele může být povolen pouze do prostředí MČ Praha 1 za podmínek stanovených Odborem informatiky ÚMČ Praha 1. Případné výjimky musí být projednány a schváleny manažerem bezpečnosti informací MČ Praha 1, případně bezpečnostním správcem systému.

Lokální (přímý) přístup poskytovatele do prostředí MČ Praha 1 (případně k aktivům MČ Praha 1) musí být v odůvodněných případech povolen manažerem bezpečnosti informací MČ Praha 1 a musí probíhat v režimu dohledu ze strany Odboru informatiky ÚMČ Praha 1 nebo oprávněného (stanoveného) pracovníka ÚMČ Praha 1, ale vždy na základě žádosti poskytovatele a po schválení Odborem informatiky UMČ Praha 1.

8 Bezpečnost dodávek a služeb

8.1 Vývoj software, informačních systémů a jejich modulů

Vývoj SW a informačních systémů musí probíhat:

a) s využitím legálního software;

b) na testovacím prostředí odděleném od prostředí produkčního. Za vytvoření softwarové složky testovacího prostředí v rozsahu své dodávky odpovídá smluvní partner, za vytvoření ostatních částí testovacího prostředí a jeho bezpečnost odpovídá MČ Praha 1;

c) na testovacích datech, která nejsou převzata z provozní databáze; za testovací data je odpovědný smluvní partner. Pokud je nutné použít data z provozní databáze, je nutné je předem anonymizovat, přičemž za anonymizaci těchto dat odpovídá MČ Praha 1. Za bezpečnost testovacích dat v rozsahu smluvně dohodnutých pravidel odpovídá smluvní partner;

d) tak, že migrace do provozního prostředí může být provedena až po akceptaci výsledků testů v testovacím prostředí a formalizovaném a doložitelném odsouhlasení těchto testů.

Před zahájením vývoje je smluvní partner povinen projednat se zástupci Odboru informatiky ÚMČ Praha 1 své navrhované řešení. Odbor informatiky musí předem odsouhlasit veškeré hardwarové, softwarové a síťové požadavky vytvářeného řešení a musí se předem ubezpečit, zda toto řešení bude respektovat veškeré bezpečnostní standardy MČ Praha 1.

8.2 Dodávky software a hardware

a) Dodávka software (SW) a hardware (HW) musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována;

b) U veškerého dodávaného programového vybavení musí být zřejmé, zda se jedná o volně šířený SW, nebo SW podléhající licenční nebo registrační politice;

c) Dodávka licenčního SW musí zahrnovat jasná pravidla pro vydávání a používání licencí, včetně jejich evidence;

d) O každé dodávce musí existovat kromě účetních dokladů také předávací protokol o řádném dodání a instalaci; podepsaný poskytovatelem a za odběratele oprávněným pracovníkem Odboru informatiky ÚMČ Praha 1;

e) Každý nový SW/nové HW zařízení musí být otestováno, než bude akceptováno a zařazeno do produkčního prostředí daného systému MČ Praha 1; za provedení testů je odpovědný poskytovatel daného SW/HW, přičemž MČ Praha 1 je při provádění předmětných testů povinna poskytnout přiměřenou součinnost.

f) Správce HW (případně MČP1) je povinen na příslušném fyzickém či virtuálním serveru, na kterém je SW/aplikace Poskytovatele (pro niž je správcem) provozována, zajišťovat pravidelné aktualizace příslušného operačního systému a komponent běžících na tomto serveru. V případě, že po aktualizaci je SW/aplikace nefunkční nebo vykazuje chyby, je Poskytovatel SW/aplikace povinen zajistit odstranění chyb a plnou funkčnost SW/aplikace.

8.3 Dodávky služeb a ostatní služby

a) Dodávka služeb musí být řádně smluvně zajištěna, průběžně kontrolována a dokumentována ze strany poskytovatele i zákazníka;

b) Způsob předání výstupů služby závisí na konkrétní službě a na smluvních podmínkách dohodnutých ve smlouvě; vždy musí existovat předávací a akceptační protokol o řádném poskytnutí služby;

c) Pracovníci smluvních partnerů, zajišťující servis IT technologií (HW / SW / IS), jsou na základě smlouvy oprávněni se pohybovat i na neveřejných místech ÚMČ Praha 1; a to vždy a pouze s vědomím oprávněného pracovníka Odboru informatiky ÚMČ Praha 1;

d) Pracovníci smluvních partnerů, zajišťující ostatní služby (např. úklid, ostrahu, ...) jsou na základě smlouvy oprávněni pohybovat se na neveřejných místech ÚMČ Praha 1. Při svém pohybu musí dbát příslušných bezpečnostních pravidel, nemají zpravidla přístup k informačním aktivům MČ Praha 1.

8.4 Dokumentace dodávky SW, HW a služeb

a) Nedílnou součástí každé dodávky SW, HW nebo služeb je příslušná projektová, provozní a bezpečnostní dokumentace vztahující se k předmětu dodávky, včetně její aktualizace;

b) Dokumentace musí být předána formálním způsobem a podrobena akceptačnímu řízení ze strany zákazníka, tj. MČ Praha 1;

c) Poskytovatel je povinen všechny změny v konfiguraci IS/IT v průběhu dodávky zadokumentovat a v případě již zpracované dokumentace musí provést její aktualizaci v potřebném rozsahu.

8.5 Akceptace dodávky

a) Každý dodaný SW, HW a služba musí být plně a v potřebné míře otestovány, zda splňují očekávané a smluvně definované parametry; a zda jejich používání nepředstavuje neočekávaná bezpečnostní nebo provozní rizika;

b) V případě informačního systému, před jeho uvedením do rutinního provozu, musí být tento z hlediska provozního formálně akceptován příslušným pracovníkem Odboru informatiky a z hlediska bezpečnosti informací manažerem bezpečnosti informací ÚMČ Praha 1.

9 Fyzická bezpečnost

Cílem fyzické bezpečnosti v oblasti IT je chránit prostředí, ve kterém se nacházejí aktiva MČ Praha 1, zabránit náhodnému nebo cílenému neautorizovanému přístupu, poškození nebo narušení aktiv MČ Praha 1.

Prostory ÚMČ Praha 1 jsou rozčleněny na oblasti veřejnosti přístupné a oblasti neveřejné (např. serverovny, prostory s HW aktivy, ...).

a) V neveřejných prostorech není dovolen pohyb cizích osob, tzn. včetně pracovníků smluvních partnerů (= neautorizovaných osob) bez doprovodu oprávněného pracovníka ÚMČ Praha 1;

b) Cizí osoby (= neautorizované osoby) nesmějí být ponechány v neveřejných prostorech ÚMČ Praha 1 bez dozoru, pokud tato skutečnost není ošetřena smlouvou.

10 Personální bezpečnost

Cílem personální bezpečnosti v oblasti IT je vytvoření potřebného bezpečnostního povědomí zaměstnanců poskytovatele, příp. subposkytovatelů, smluvních partnerů MČ Praha 1 v oblasti zajištění ochrany a bezpečnosti aktiv MČ Praha 1 s cílem předcházet, příp. zabránit neautorizovanému přístupu, narušení důvěrnosti a integrity aktiv MČ Praha 1.

Smluvní partner je odpovědný za veškeré aktivity svých pracovníků a pracovníků svých subposkytovatelů provádějících činnosti na základě uzavřeného smluvního mezi smluvním partnerem a MČ Praha 1;

Smluvní partner zajistí, že veškeré činnosti dle smluvního vztahu budou prováděny jeho zaměstnanci nebo subposkytovateli, budou prováděny kompetentními osobami, s příslušnou odbornou kvalifikací a bezpečnostními zárukami;

Smluvní partner provede a doložitelně zdokumentuje rozsah a obsah proškolení osob podílejících se na realizaci smluvního vztahu v oblasti zajištění bezpečnosti informací MČ Praha 1;

Rozsah a obsah proškolení vychází jednak z požadavků tohoto dokumentu, dále z platné Politiky bezpečnosti informací MČ Praha 1 a dalších upřesnění manažera bezpečnosti informací k danému

smluvnímu vztahu. Obsah proškolení bude též vycházet z bezpečnostní dokumentace MČ Praha 1, kterou bude mít smluvní partner k dispozici.

Příloha č. 6 – Seznam členů Realizačního týmu

SEZNAM ČLENŮ REALIZAČNÍHO TÝMU

Pro účely plnění veřejné zakázky s názvem *„Zvýšení kybernetické bezpečnosti - systém pro řízení přístupu“*, ev. č. ve Věstníku veřejných zakázek Z2025-062751, vyhlášenou zadavatelem **Městská část Praha 1**, IČO: 000 63 410, se sídlem Vodičkova 681/18, 110 00 Praha 1.

obchodní firma / jméno a příjmení[1] O2 IT Services s.r.o.
se sídlem / trvale bytem Za Brumlovkou 266/2, Michle, 140 00 Praha 4
IČO: 02819678
společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze,
sp. zn. C 223566
zastoupená: Ing. Josefem Appelem, na základě pověření

prohlašuje, že níže uvedenými osobami hodlá plnit předmět uvedené veřejné zakázky.

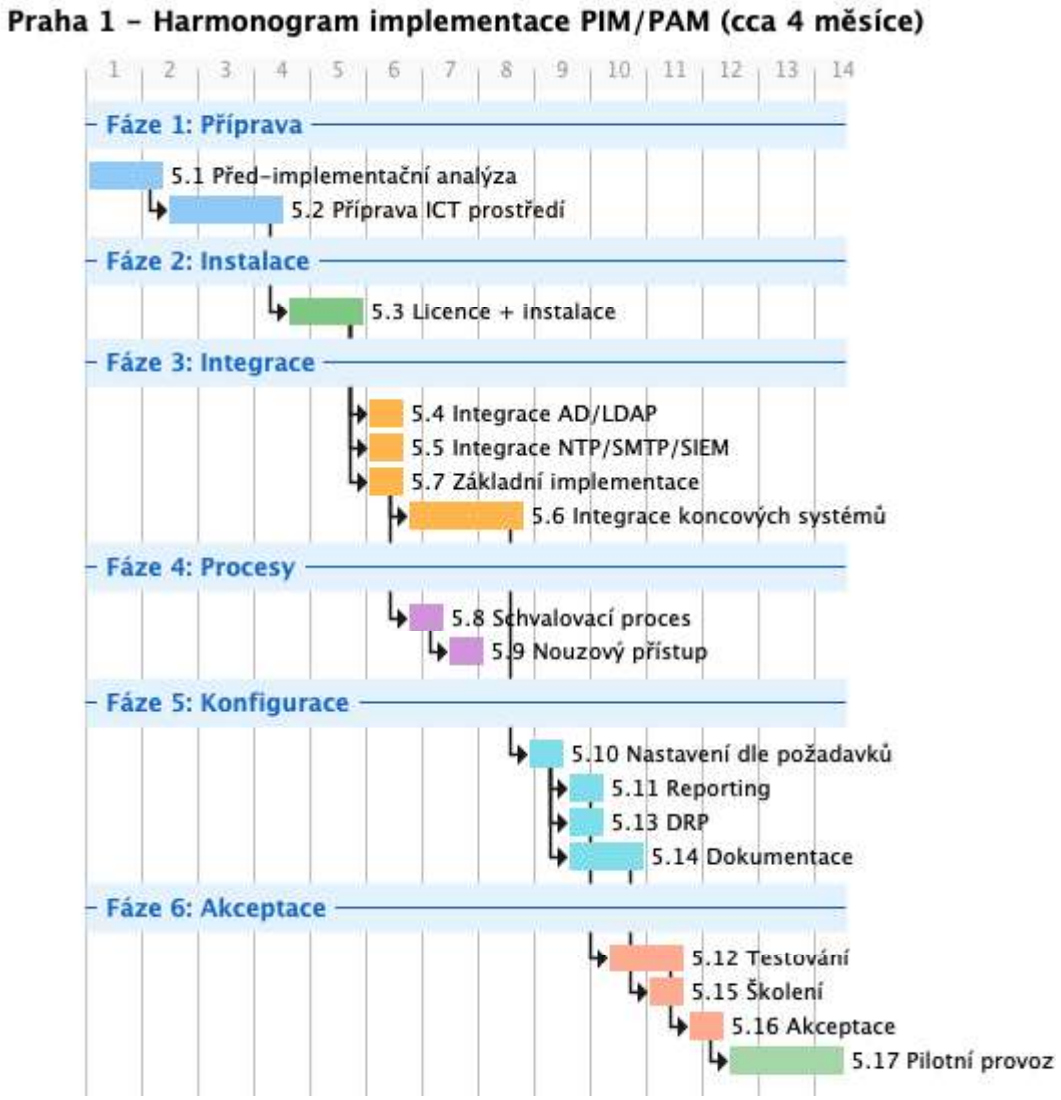
Odst. zadávací dokumentace, z něhož požadavek vyplývá	**Jméno, příjmení, titul**	**Pozice v realizačním týmu**	**Nejvyšší dosažené vzdělání**	**Druh praxe a její délka** (v doporučeném formátu mm/rrrr – mm/rrrr)	**Osvědčení o odborné kvalifikaci**	**Zkušenosti prokazující kvalifikaci dle požadavků zadavatele**
18.3.4 písm. A)	[redacted]	Projektový manažer	Vysokoškolské	08/2008 - současnost	Prince 2 – Practitioner certificate in Project management	AVENET Distribution s.r.o. (Koncoví zákazníci: Partners Banka, a.s. a Notino, s.r.o.)

[1] Identifikační údaje doplní účastník dle skutečnosti, zda se jedná o účastníka – fyzickou či právnickou osobu.

					ITIL v3 Foundation	
18.3.4 písm. B)	[redacted]	Architekt řešení	Středoškolské	02/2005 – současnost	BeyondTrust Certified Administrator TOGAF 9 Certified level	AVENET Distribution s.r.o. (Koncoví zákazníci: Partners Banka, a.s. a Notino, s.r.o.)
18.3.4 písm. C)	[redacted]	Specialista systému řízení bezpečnosti informací	Vysokoškolské	03/2018 - současnost	Lead auditor Systému řízení bezpečnosti informací	AVENET Distribution s.r.o. (Koncoví zákazníci: Partners Banka, a.s. a Notino, s.r.o.)
27.9.1	[redacted]	IT specialista OS Linux	Vysokoškolské	02/2015 – současnost	Red Hat Certified Engineer (RHCE)	není požadováno
27.9.2	[redacted]	IT specialista OS Windows	Vysokoškolské	04/2006 - současnost	Microsoft® Certified Solutions Associate: Windows Server 2016	není požadováno
27.9.3	[redacted]	Specialista kybernetické bezpečnosti	Středoškolské	01/2018 - současnost	Certified Ethical Hacker	není požadováno

Příloha č. 7 – Harmonogram projektu implementace

Implementace řešení PIM/PAM je plánována v délce přibližně 4 měsíců (včetně testování, akceptace a pilotního provozu). Skutečný průběh a celkový termín realizace je závislý na součinnosti Zadavatele, zejména na včasné přípravě ICT prostředí (zajištění virtuálních serverů, konektivity, síťových prostupů a souvisejících infrastrukturních předpokladů) a na dostupnosti odpovědných osob pro integrační a akceptační činnosti.



Činnost	Výstup / Akceptační kritérium
Návrh architektury řešení PIM/PAM a zpracování před-implementační analýzy	Je dokončený a Zadavatelem akceptovaný dokument.
Příprava ICT prostředí na straně Zadavatele	Připravené virtuální servery, konektivita, prostupy a další zdroje pro zprovoznění řešení PIM/PAM

Poskytnutí licencí a instalace PIM/PAM řešení	Zadavatel má k dispozici počet účtů požadovaných v rámci specifikace.
Integrace s AD/LDAP, prostupy	Nástroj PIM/PAM je integrovaný s AD/LDAP a rozděleny přístupy a role
Integrace s dalšími infrastrukturními systémy	Systém je integrován se systémy: NTP SMTP Log Management/SIEM
Integrace s koncovými systémy	Systém je integrován na uvedené systémy.
Základní implementace	Nástroj PIM/PAM řídí všechny privilegované účty, přístupy a oprávnění.
Vytvoření schvalovacího procesu pro žádost o privilegovaný přístup	Dokument s navrženým procesem.
Vytvoření procesu pro nouzový přístup ke koncovému systému v případě celkového nebo částečného výpadku PIM/PAM řešení	Dokument s navrženým procesem.
Nastavení dodaného PIM/PAM řešení dle technických požadavků	Nástroj PIM/PAM nastavený dle schválené před-implementační analýzy.
Nastavení reportingu	Jsou funkční reporty v souladu s technickou specifikací.
Testování řešení PIM/PAM	Nástroj PIM/PAM je otestovaný a plně funkční dle předem schválených akceptačních scénářů. Testy neodhalily žádné incidenty kategorie A a B. Penetrační testy a testy zranitelností neodhalily žádné zranitelnosti/chyby kategorie „kritická“.
Plán obnovy po havárii (DRP)	Je dokončený a Zadavatelem akceptovaný dokument.
Dokumentace	Aktuální řídící dokumentace v elektronické podobě (DOCX, XLSX), včetně dokumentace skutečného provedení a příruček jsou dokončené a Zadavatelem akceptované.
Školení pracovníků Zadavatele	Realizace on-site školení pro interní a externí pracovníky

Akceptace základní implementace	Plně funkční Nástroj PIM/PAM v rozsahu základní implementace.
Pilotní provoz a předání do produkčního užívání	Po dobu 15 dnů zpětně k datu vyhodnocení nenastalo více než 3 incidenty kategorie A a ty byly uzavřeny v souladu s SLA parametry dle smlouvy.