Smlouva o dodání a implementaci antivirového řešení vč. maintenance

číslo smlouvy objednatele: DS202502097
číslo smlouvy dodavatele: OP-25-099

1. Smluvní strany

STATUTÁRNÍ MĚSTO LIBEREC

se sídlem:	nám. Dr. E. Beneše 1/1, Liberec 1, 460 59
zastoupené:	Ing. Jaroslavem Zámečníkem, CSc., primátorem
ve věci smlouvy:	Ing. Jaroslavem Zámečníkem, CSc., primátorem
ve věci plnění smlouvy:	Ing. Zbyňkem Vavřinou, vedoucím odboru vnitřních věcí
IČ:	00262978
DIČ:	CZ00262978
Bankovní spojení:	4096142/0800

(dále jen **Objednatel**)

a

PCS spol. s r.o.

se sídlem:	Na Dvorcích 122/18, Krč, 14000 Praha 4
zastoupená:	Ing. Petrem Vašákem, jednatelem
IČ:	00571024
DIČ:	CZ00571024
Bankovní spojení:	9252802 / 0800
zapsaná v OR vedeným	Městským soudem v Praze, oddíl C, vložka 527

(dále jen **Dodavatel**)

Společně též jako **Smluvní strany**

2. Předmět plnění

2.1 Předmětem této smlouvy je dodávka a implementace antivirového řešení pro ochranu koncových stanic. Jedná se o dodání a implementace 550 licencí antivirového řešení splňujícího požadavky v minimální konfiguraci dle přílohy č. 1 – Technické specifikace. Platnost licencí jsou 4 roky.

2.2 Antivirové řešení bude dodáno v ujednaném množství, druzích, jakosti a termínech uvedených v této smlouvě a její příloze č. 1.

2.3 Veškeré dodané antivirové řešení musí být schválené pro použití v ČR a splňující související normy.

2.4 Předmětem této smlouvy je také zajištění údržby a technické podpory (maintenance) pro 550 licencí dodaného antivirového řešení po dobu 4 let, počínaje dnem oboustranného podpisu předávacího protokolu potvrzujícího dodání a implementaci antivirového řešení dle čl. 1. odst. 2.1 této smlouvy. Maintenance zahrnuje pravidelné aktualizace, řešení technických problémů, poskytování bezpečnostních záplat a konzultace dle potřeby Objednatele.

2.5 Předmět plnění je dále upřesněn v příloze č. 1 této smlouvy – Technické specifikace.

3. Cena

3.1 Celkovou cenou se rozumí cena za dodání a implementaci antivirového řešení dle čl. 1. odst. 2.1 této smlouvy a cena za zajištění maintenance dle čl. 1. odst. 2.4 této smlouvy.

3.2 Cena za jednotlivé části předmětu plnění, jakož i celková cena, byla sjednána na základě nabídky Dodavatele ze dne 16.4.2025, podané v rámci veřejné zakázky „Dodání a implementace ochrany koncových stanic a serverů před bezpečnostními hrozbami".

3.3 Cena za jednotlivé části předmětu plnění, jakož i celková cena, činí:

Název	Počet jednotek	Cena bez DPH	Cena s DPH
Licence a implementace antivirového řešení dle čl. 1. odst. 2.1	550 ks	[redacted]	
Zajištění maintenance dle čl. 1. odst. 2.4	4 roky		
Celková cena za předmět plnění	**celkem**	**638.000,- Kč**	**771.980,- Kč**

3.4 Celková cena za předmět plnění (i cena za jeho části) je sjednána jako konečná a nepřekročitelná a zahrnuje veškeré náklady Dodavatele nezbytné k řádnému, úplnému a kvalitnímu provedení a zajištění předmětu plnění (jeho částí) této smlouvy, včetně nákladů na dopravu.

4. Platební podmínky

4.1 Objednatel zaplatí cenu za jednotlivé části předmětu plnění na základě faktur, a to nejpozději do posledního dne její splatnosti, a to pouze v případě, že dodávka bude ze strany Objednatele bez výhrad převzata formou oboustranného podpisu předávacího protokolu.

4.2 Cena za licenci a implementaci antivirového řešení dle čl. 1. odst. 2.1 této smlouvy bude hrazena jednorázově. Dodavatel je oprávněn vystavit fakturu na částku ve výši ceny za licenci a implementaci antivirového řešení dle čl. 1. odst. 2.1 této smlouvy po předání a převzetí příslušné části předmětu plnění. K předání a převzetí dojde okamžikem oboustranného podpisu předávacího protokolu.

4.3 Cena za zajištění maintenance dle čl. 1. odst. 2.4 této smlouvy (či její poměrná část) bude hrazena jednou ročně, a to na základě faktury vystavené Dodavatelem po zajištění (provedení) maintenance v předchozím kalendářním roce, kdy řádnost tohoto zajištění (provedení) bude potvrzena okamžikem oboustranného podpisu předávacího protokolu. V případě ukončení smlouvy před koncem kalendářního roku platí, že k předání poslední části předmětu plnění dojde do 30 dní od jejího ukončení.

4.4 Za zaplacení ceny (její části) se považuje připsání příslušné částky ve prospěch účtu Dodavatele.

4.5 Každá faktura bude vystavena v měně CZK. Na faktuře bude vždy uvedeno číslo smlouvy Objednatele i Dodavatele. Datum oboustranného podepsání předávacího protokolu je datem příslušného zdanitelného plnění.

4.6 Dodavatel je oprávněn vystavit fakturu po oboustranném podpisu předávacího protokolu.

4.7 Splatnost vystavené faktury obsahující veškeré náležitosti je stanovena na 30 (slovy třicet) dní ode dne jejího doručení Objednateli. Faktura bude zaslána na adresu Objednatele.

4.8 Přílohou faktury – daňového dokladu bude předávací protokol podepsaný pověřeným zástupcem Objednatele.

5. Užívání

5.1 Licence implementovaného antivirového řešení dle čl. 1. odst. 2.1 této smlouvy přechází do užívání Objednatele okamžikem oboustranného podpisu předávacího protokolu.

6. Dodací podmínky

6.1 Dodavatel dodá a zaimplementuje Objednateli antivirového řešení dle čl. 1. odst. 2.1 této smlouvy do místa plnění po nabytí účinnosti této smlouvy.

6.2 Dodavatel zajistí Objednateli maintenance po dobu 4 let, počínaje dnem oboustranného podpisu předávacího protokolu potvrzujícího dodání a implementaci antivirového řešení dle čl. 1. odst. 2.1 této smlouvy.

6.3 Zajištění maintenance za předchozí rok bude potvrzeno oboustranným podpisem předávacího protokolu.

6.4 Místem plnění zakázky jsou budovy Magistrátu města Liberec.

6.5 Dodávka a implementace antivirového řešení dle čl. 1. odst. 2.1 této smlouvy se uskuteční nejpozději do 1 měsíce ode dne nabytí účinnosti této smlouvy.

6.6 Dodávka bude potvrzena oboustranným podpisem předávacího protokolu.

6.7 Za doklad nutný k převzetí a užívání implementovaného antivirového řešení se považuje předávací protokol.

7. Záruky

7.1 Záruka na antivirové řešení dodané a implementované dle této smlouvy bude poskytnuta v délce trvání minimálně 4 let, počínaje dnem oboustranného podpisu předávacího protokolu části předmětu plnění dle čl. 1. odst. 2.1 této smlouvy.

7.2 Dodavatel je povinen odstranit vady nejpozději do 7 dnů ode dne jejich oznámení, pokud nebude s ohledem na charakter vady s Objednatelem dohodnuta lhůta delší.

7.3 Oznámení o vadách musí obsahovat:

a. číslo smlouvy nebo faktury,

b. popis vady nebo určení, jak se vada projevuje.

8. Smluvní pokuty

8.1 V případě, že Dodavatel nedodrží termín dodávky, sjednaný v této smlouvě, je Objednatel oprávněn požadovat smluvní pokutu ve výši 0,2 % z celkové kupní ceny včetně DPH za každý den prodlení.

8.2 V případě prodlení Dodavatele s odstraněním vad ve lhůtě stanovené touto smlouvou se Dodavatel zavazuje Objednateli uhradit smluvní pokutu ve výši 0,2 % z celkové kupní ceny včetně DPH za každý den prodlení a jednotlivou vadu.

8.3 V případě prodlení Objednatele s placením faktury za dodané a implementované antivirové řešení nebo za maintenance je Dodavatel oprávněn požadovat smluvní úrok z prodlení ve výši 0,2 % z celkové nezaplacené částky za každý den prodlení. Objednatel není v prodlení s plněním své povinnosti zaplatit kupní cenu, pokud je Dodavatel v prodlení s plněním kterékoliv své povinnosti vyplívající z této smlouvy.

8.4 Objednatel si vyhrazuje právo na úhradu smluvní pokuty formou zápočtu ke kterékoliv splatné pohledávce Dodavatele vůči Objednateli. Kterákoliv smluvní pokuta dle této smlouvy nevylučuje nárok na náhradu škody.

9. Všeobecná ujednání

9.1 Tato smlouva je uzavřena dle zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

9.2 Smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami.

9.3 Jakékoli změny této smlouvy mohou být učiněny pouze písemnými dodatky, schválenými podpisem obou stran. Tyto dodatky se stanou integrální součástí této smlouvy. Dodatky budou číslovány vzestupně.

9.4 Veškeré informace, jež si smluvní strany navzájem poskytnou, jsou označeny jako důvěrné a žádná ze smluvních stran není oprávněna je poskytnout třetí osobě ani použít v rozporu s jejich účelem pro své potřeby.

9.5 Smluvní strany jsou oprávněny zveřejnit veškerý obsah této smlouvy, budou-li o to požádány dle zákona č. 106/1999 Sb.

9.6 Smluvní strany berou na vědomí, že tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb. o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

9.7 Smluvní strany berou na vědomí, že jsou povinny označit údaje ve smlouvě, které jsou chráněny zvláštními zákony (obchodní, bankovní tajemství, osobní údaje, …) a nemohou

být poskytnuty, a to šedou barvou zvýraznění textu. Neoznačení údajů je považováno za souhlas s jejich uveřejněním a za souhlas subjektu údajů.

9.8 Smlouva nabývá účinnosti nejdříve dnem uveřejnění v registru smluv podle § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

9.9 Smluvní strany berou na vědomí, že plnění podle této smlouvy poskytnutá před její účinností jsou plnění bez právního důvodu a strana, která by plnila před účinností této smlouvy, nese veškerou odpovědnost za případné škody takového plnění bez právního důvodu, a to i v případě, že druhá strana takové plnění přijme a potvrdí jeho přijetí.

9.10 Smlouva se vypracovává ve 2 vyhotoveních s platností originálu, z nichž po jednom obdrží každá ze smluvních stran nebo elektronicky a podepsána oběma smluvními stranami kvalifikovaným elektronickým podpisem.

9.11 Smluvní strany si smlouvu přečetly, s jejím obsahem souhlasí, což stvrzují svým vlastnoručním podpisem.

9.12 Přílohy smlouvy:

Příloha č. 1 – Technické specifikace

.....	.....
statutární město Liberec	PCS, spol. s r.o.
Ing. Jaroslav Zámečník	Ing. Petr Vašák
primátor	jednatel

Příloha č. 4

DODÁNÍ A IMPLEMENTACE OCHRANY KONCOVÝCH STANIC A SERVERŮ PŘED BEZPEČNOSTNÍMI HROZBAMI

ochrana koncových stanic a serverů:

1. Detekce a prevence malware: Dodaný systém musí být schopen detekovat a zabránit různým typům malware, včetně virů, trojských koní, ransomwaru, spywaru a dalších hrozeb. Musí umět používat pokročilé algoritmy analýzy chování a heuristiky pro odhalování nových a neznámých hrozeb (tzn. nerozhodovat pouze na základě antivirové databáze).

2. Behaviorální analýza: Dodaný systém musí sledovat chování souborů a procesů v reálném čase a detekovat podezřelé aktivity, které naznačují přítomnost malware, případně jiných hrozeb. Musí používat strojové učení a umělou inteligenci pro identifikaci nových vzorů chování malware.

3. Ochrana před ransomwarem: Dodaný systém musí obsahovat funkce pro ochranu proti ransomwaru, jako je monitorování podezřelých souborových operací.

4. Síťová ochrana: Dodaný systém musí poskytovat funkce ochrany síťové komunikace před neoprávněným přístupem ze sítě třetích stran. (mimo interní prostředí zadavatele, například práce z domova apod.).

5. Kompatibilita a výkon: Dodaný systém musí být kompatibilní s aktuálně podporovanými verzemi MS Windows – desktop i server a aktuálně podporovaných verzí OS Linux. Musí nabízet efektivní skenování zařízení a nesmí zásadním způsobem ovlivnit výkon zařízení. Minimální konfigurace: 2 jádrový CPU, 8GB RAM a SSD disk.

6. Automatické aktualizace: Dodaný systém musí automaticky stahovat a instalovat aktualizace s definicí škodlivého software (virová databáze).

7. Dodaný systém musí umět sám všechny hrozby vyhodnotit a bez nutnosti administrátora sám zakročit a případný útok zastavit dle nastavených pravidel v centrální správě dodaného systému.

8. Dodaný systém musí umožnit automatické skenování všech nově připojených datových zdrojů k zařízení (například USB disk, FlashDisk, paměťové karty apod.).

9. Dodaný systém musí umožnit aktivní správu všech vstupně výstupních portů určených k přenosu dat.

10. Centrální správa a monitorování: Dodaný systém musí mít možnost centrální správy a monitorování, která umožňuje správcům IT prostředí sledovat stav a výkonnost antivirového programu a provádět vzdálené aktualizace antivirových databází a konfigurace z jednoho místa.

Centrální správa:

1. Centrální správa: Dodaný systém musí poskytovat nástroj, který umožňuje správcům IT sledovat a spravovat všechny stanice a servery z jednoho místa (centrální správa). Dodaný systém musí nabízet uživatelsky přívětivé rozhraní pro snadnou správu (GUI).

2. Instalace klientů pomocí doménové politiky: Dodaný systém musí umožňovat automatizovanou instalaci klientů na koncová zařízení pomocí doménové politiky. Tímto způsobem bude zajištěna automatická instalace a konfigurace na všech koncových zařízeních bez nutnosti manuální intervence na každém koncovém zařízení.

3. Základní přehled stanic: Dodaný systém musí poskytovat přehled o aktuálním stavu všech koncových zařízeních (například: poslední aktualizace databáze a její verze, verze programu, posledním skenování a výsledcích, zda je zařízení aktivní, zda je zařízení v ohrožení apod.).

4. Upozornění na hrozby: Dodaný systém musí disponovat funkcí upozornění a notifikací (minimálně notifikace emailem) v případě detekce hrozeb nebo jiných událostí dle konfigurace.

5. Dashboard: Dodaný systém musí disponovat nástrojem pro centrální sledování stavu všech koncových zařízení (dashboard). Tento dashboard musí být interaktivní a musí reagovat v reálném čase.

6. Analýza hrozeb: Dodaný systém musí poskytovat nástroje pro analýzu hrozeb, včetně detailních informací o detekovaných hrozbách, jejich původu, chování a dopadu na postižené koncové

zařízení. Součástí nabízeného řešení je možnost vyhledávání a filtrování hrozeb pro podrobnější analýzu.

7. Vzdálená správa bezpečnostních incidentů: Nabízené řešení musí umožňovat vzdálenou správu bezpečnostních incidentů a jejich řešení (a to i v případě, kdy agent nabízeného řešení instalovaný na koncovém zařízení zablokuje síťovou komunikaci).

8. Přihlášení správce do aplikace musí být zabezpečeno min. dvou-faktorovou autentizací.

Prostředí:

1. Agent nabízeného řešení musí umět chránit koncové zařízení v každém okamžiku (v prostředí zadavatele i v externím prostředí, i bez aktivního připojení k internetu).

2. Agenta nabízeného řešení musí jít vypnout, pozastavit, nebo zapnout pouze z centrální správy, nebo pověřeným účtem.

3. Agent nabízeného řešení musí umět komunikovat s centrální správou i v případě, kdy je v externím prostředí, ale je připojený k veřejné síti internet.

4. Nabízené řešení musí být provozováno dodavatelem v bezpečném datovém centru, splňující aktuálně platnou legislativu ČR (zvláště pak musí být v souladu s požadavky NUKIB, NIS2, GDPR apod.).

Maintenance:

1. Po dobu životnosti licence musí být poskytnuty aktualizace software.

2. Po dobu životnosti licence musí být poskytnuty bezpečnostní záplaty.

3. Pro antivirové řešení musí být poskytnuta technická podpora.

4. Pro antivirové řešení musí být poskytnuta konzultace a školení pro zavedení antivirového řešení.