Příloha č. 3 – vzor smlouvy

KUPNÍ SMLOUVA

uzavřená dle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,
níže uvedeného dne, měsíce a roku mezi smluvními stranami, kterými jsou:

OTYR s.r.o.
sídlo: Blatnická 4219/4, 628 00 Brno
IČ: 29363799
DIČ: CZ29366799
bankovní spojení: [redacted]
zapsána v obchodním rejstříku vedeném krajský soud v Brně, sp. Zn. C.75505
zastoupená. Bc Robert Janík - jednatel
(dále jen **prodávající**)

a

Uherskohradišťská nemocnice a.s.
sídlo: J. E. Purkyně 365, 686 06 Uherské Hradiště
IČ: 27660915
DIČ: CZ27660915
bankovní spojení: [redacted]
zapsána v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl B, vložka 4420
zastoupená MUDr. Petrem Sládkem, předsedou představenstva
(dále jen **kupující**)

Preambule

Tato smlouva je uzavírána na základě výsledku zadávacího řízení zakázky malého rozsahu „Dodávka licencí antivirové ochrany“, č. 2023/003/MRIII, jehož zadavatelem je kupující.

I.
Předmět smlouvy

1. Předmětem této kupní smlouvy je dodávka licencí antivirové ochrany **SOPHOS podrobně specifikovaných v příloze č. 1**, které jsou majetkem prodávajícího a které splňují požadavky uvedené v příloze č. 2 Technická specifikace (dále jen „Zboží“).
2. Touto smlouvou se prodávající zavazuje, že kupujícímu odevzdá Zboží a umožní mu nabýt vlastnické právo k němu, a kupující se zavazuje, že Zboží převezme do svého výlučného vlastnictví a zaplatí za něj kupní cenu. Součástí plnění je i zaškolení obsluhy tak, jak je uvedeno v příloze č. 2.
3. Prodávající v souvislosti s dodávkou Zboží poskytne kupujícímu kopii prohlášení o shodě, případně CE certifikát, a návod k obsluze v českém jazyce.
4. Prodávající prohlašuje, že Zboží nemá právní vady a jeho kvalitativní a technické vlastnosti odpovídají příslušným obecně závazným právním předpisům a technickým normám. Prodávající prohlašuje, že Zboží je ve stavu způsobilém k jeho řádnému užívání.

II.
Kupní cena

1. Celková kupní cena za Zboží činí **1 570 000,00 Kč bez DPH (1 899 700,00 Kč včetně DPH).** Sazba DPH se řídí příslušným zákonem.

Celkovou kupní cenu (bez DPH) tvoří:	
Cena za 350 ks licencí koncových stanic	1 225 000,00 Kč
Cena za 40 ks licencí pro servery	320 000,00 Kč
Cena za školení	25 000 Kč

2. Kupní cenou se rozumí cena Zboží včetně obalu, dopravy do sídla kupujícího, zaškolení personálu, návodu k použití a veškerých dalších nákladů a výdajů prodávajícího spojených s realizací této kupní smlouvy.
3. Kupní cena je stanovena jako maximální a nepřekročitelná.

III.
Dodací podmínky

1. Místem dodání Zboží je sídlo kupujícího. O předání a převzetí Zboží bude oprávněnými osobami smluvních stran vypracován a podepsán předávací protokol.
2. V případě výskytu vad na Zboží, bránících řádnému užívání Zboží kupujícím k termínu jeho předání a převzetí, není povinen kupující Zboží převzít až do jejich odstranění.
3. Prodávající se zavazuje dodat Zboží kupujícímu do 10 pracovních dní od podpisu smlouvy. Zboží je předáno po podepsání předávacího protokolu oběma stranami, čímž přechází vlastnické právo ke Zboží na kupujícího. S přechodem vlastnického práva přechází na kupujícího současně i nebezpečí škody na Zboží.
4. Kupující je oprávněn od smlouvy odstoupit, pokud Zboží není dodáno řádně, bez vad nebo v dohodnutém termínu a jestliže prodávající nesjedná nápravu ani v kupujícím poskytnuté přiměřené lhůtě.

IV.
Platební podmínky

1. Kupující se zavazuje zaplatit kupní cenu na základě daňového dokladu - faktury (dále jen „faktura“), vystaveného prodávajícím po předání a převzetí Zboží, se splatností 30 dní od jejího doručení kupujícímu.
2. Faktura musí splňovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných právních předpisů. V případě, že faktura nebude mít odpovídající náležitosti, je kupující oprávněn zaslat fakturu ve lhůtě splatnosti zpět prodávajícímu k doplnění, či úpravě, aniž se dostane do prodlení se splatností, lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněného či opraveného dokladu.
3. Za zaplacení kupní ceny se považuje připsání příslušné částky ve prospěch účtu prodávajícího.
4. V případě prodlení kupujícího se zaplacením kupní ceny je prodávající oprávněn účtovat kupujícímu úrok z prodlení dle příslušného nařízení vlády. Za prodlení se zaplacením kupní ceny není kupující povinen kromě úroku z prodlení hradit jakoukoliv smluvní pokutu nebo jinou smluvní sankci.

V.
Záruka, záruční a pozáruční servis

1. Prodávající poskytuje záruku za jakost Zboží v délce 36 měsíců s tím, že práva z odpovědnosti za vady výslovně neupravená tímto článkem se řídí příslušnými ustanoveními občanského zákoníku.
2. Záruční doba začíná běžet ode dne řádného předání a převzetí Zboží.
3. Poskytnutá záruka znamená, že dodané Zboží bude po dobu 36 měsíců ode dne podpisu předávacího protokolu způsobilé k použití pro obvyklý účel a že si zachová obvyklé vlastnosti.
4. Záruční servis zajišťuje prodávající na základě výzvy kupujícího. Kontaktní údaje prodávajícího pro uplatnění záručních vad:
   tel: +420 739 699 e-mail: info@otyr.cz

Závadu je prodávající povinen odstranit do 10 pracovních dní od doručení reklamační výzvy kupujícího, nedohodnou-li se smluvní strany jinak.

VI.
Sankční ujednání

1. V případě prodlení prodávajícího s dodáním Zboží uhradí prodávající kupujícímu smluvní pokutu ve výši 0,2 % z hodnoty Zboží bez DPH za každý započatý den prodlení. Tato smluvní pokuta je zúčtovatelná proti úhradě ceny za Zboží.
2. V případě prodlení prodávajícího s odstraněním reklamované závady (viz V.4 výše) uhradí prodávající kupujícímu smluvní pokutu ve výši 2 000 Kč za každý započatý den prodlení a každý reklamovaný ks PC.
3. V případě, že prodávající poruší jakékoliv jiné smluvní povinnosti dle této smlouvy než výše uvedené (VI.1, VI.2.) uhradí prodávající kupujícímu smluvní pokutu ve výši 5 000 Kč za každý jednotlivý případ porušení smluvní povinnosti.
4. V případě prodlení kupujícího s úhradou kupní ceny uhradí kupující prodávajícímu úroky z prodlení v zákonné výši.
5. Takto sjednané a stranami uplatněné sankce nemají vliv na případnou povinnost náhrady vzniklé škody. Sjednané sankce hradí povinná strana nezávisle na tom, zda a v jaké výši vznikne druhé straně škoda z porušení povinnosti, ke kterému se sankce vztahuje, a jejíž náhradu lze vymáhat samostatně vedle sankcí v celém rozsahu. Částka sankce se tedy do výše náhrady škody nezapočítává. Zaplacením sankce není dotčena povinnost povinné strany splnit závazky vyplývající z této smlouvy.

VII.
Závěrečná ustanovení

1. Tato kupní smlouva se stává platnou dnem podpisu obou smluvních stran a účinnou uveřejněním v registru smluv (viz níže).
2. Veškeré změny a doplňky této kupní smlouvy jsou možné pouze písemnými, jednotlivě číslovanými dodatky podepsanými oprávněnými zástupci obou smluvních stran.
3. Právní vztahy výslovně neupravené touto smlouvou se řídí občanským zákoníkem.
4. Na tuto smlouvu se vztahuje povinnost uveřejnění prostřednictvím registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), v platném znění. Obě smluvní strany souhlasí s tímto uveřejněním a sjednávají, že správci registru smluv zašle tuto smlouvu k uveřejnění prostřednictvím registru smluv kupující. Kupující bude při přípravě dokumentu k uveřejnění vycházet z písemných (e-mail) pokynů prodávajícího, a to zejména ve věci znečitelnění obchodního tajemství, osobních údajů a jiných zákonem chráněných údajů. Pokud k písemnému (e-mail) sdělení prodávajícího o znečitelnění konkrétních údajů ve smlouvě nedojde ještě před uzavřením smlouvy, potvrzuje podpisem smlouvy prodávající, že výslovně souhlasí s uveřejněním smlouvy v plném rozsahu.
5. Pohledávky vyplývající ze smlouvy lze převést na jinou osobu jen s předchozím souhlasem druhé smluvní strany.
6. Podkladem pro uzavření této smlouvy je nabídka prodávajícího, kterou v postavení účastníka zadávacího řízení podal do zadávacího řízení na zakázku malého rozsahu „Dodávka licencí antivirové ochrany“, č. 2023/003/MRIII jehož zadavatelem je kupující. Podkladem pro uzavření této smlouvy je rovněž zadávací dokumentace k uvedené zakázce včetně všech jejích příloh. Jestliže ze zadávací dokumentace k zakázce nebo z nabídky prodávajícího vyplývají prodávajícímu povinnosti vztahující se k realizaci předmětu této smlouvy, avšak tyto povinnosti nejsou výslovně v této smlouvě uvedeny, smluvní strany se pro tento případ dohodly, že i tyto povinnosti prodávajícího jsou součástí závazkového vztahu založeného touto smlouvou a prodávající je povinen je dodržet.

7. Pokud se kterékoliv ustanovení této smlouvy ukáže být po uzavření této Smlouvy neplatným nebo neúčinným, pak tato skutečnost nebude mít za následek neplatnost nebo neúčinnost ostatních ustanovení této smlouvy. Smluvní strany se zavazují bez zbytečného odkladu na žádost druhé smluvní strany nahradit takovéto neplatné nebo neúčinné ustanovení platným a účinným ustanovením, jehož obsah bude co nejblíže odpovídat účelu neplatného nebo neúčinného ustanovení.
8. Smlouva je vyhotovena ve dvou stejnopisech s platností originálu, kdy každá ze stran obdrží po jednom z nich.
9. Smluvní strany shodně prohlašují, že si tuto smlouvu přečetly před jejím podpisem, že byla uzavřena po vzájemném projednání podle jejich pravé a svobodné vůle určitě, vážně a srozumitelně, nikoliv v tísni nebo za nápadně nevýhodných podmínek a její autentičnost stvrzují svými podpisy.

Přílohy: 1. Nabídka prodávajícího
2. Technická specifikace (příloha č. 4 zadávací dokumentace)

V Uherském Hradišti dne .....

V Brně dne .....

……..……
Uherskohradišťská nemocnice a.s.
MUDr. Petr Sládek
předseda představenstva

…….....…..……
OTYR s.r.o.
Bc. Robert Janík
jednatel společnosti

NABÍDKA

„Dodávka licencí antivirové ochrany“

ZADAVATEL:

Uherskohradišťská nemocnice a.s.

sídlo: J. E. Purkyně 365, 686 06 Uherské Hradiště

IČ: 27660915

DIČ: CZ27660915

Brno, 13. 2. 2023

Bc. Robert Janík,

1 Dodavatel

„Nákup licencí antivirové ochrany pro koncové stanice a servery, včetně administrátorského školení.“

Dodavatel

Obchodní firma nebo název:	OTYR s.r.o.
Sídlo / místo podnikání:	Blatnická 4219/4, 628 00 Brno
Právní forma:	společnost s ručením omezeným
Telefon / fax:	
E-mail:	
IČ / DIČ:	29363799 / CZ29363799
Zápis v OR:	Krajský soud v Brně, sp. zn. C.75505
Statutární orgán:	Bc. Robert Janík - jednatel
Osoba oprávněná jednat za dodavatele:	Bc. Robert Janík - jednatel
Telefon / fax:	
Kontaktní osoba:	
Telefon / fax:	
E-mail:	
Bankovní spojení dodavatele:	

Oprávněná osoba k podání nabídky za dodavatele

Titul, jméno, příjmení	Bc. Robert Janík
Funkce:	jednatel
Místo a datum podpisu:	Brno, 13. 2. 2023
Podpis oprávněné osoby:	

2 Technická specifikace a cena

SOPHOS

	Sophos Central Intercept X Advanced with XDR včetně centrální správy	ks	Cena za 1 lic CZK bez DPH	CELKOVÁ CENA bez DPH
1	**Sophos Central Intercept X Advanced with XDR** - Subscription licence s podporou **na 3 roky**	350		
2	**Sophos Central Intercept X Advanced for Server with XDR** - Subscription licence s podporou **na 3 roky**	40		
3	**INSTALACE dle podmínek VŘ (8hod)**	1		
	Cena celkem bez DPH			**1 570 000,00 Kč**
	Cena celkem s DPH			**1 899 700,00 Kč**

Nabízené řešení plní všechny technické parametry a požadavky v rámci technické specifikace VŘ

Technická specifikace - Dodávka licencí antivirové ochrany

Počty licencí a platnost:

- 1x konzole centrální správy
- 350x licence pro stanice
- 40x licence pro servery
- 1x základní zaškolení na XDR pro správce v rozsahu min 8 hodin (lze rozdělit na části)
- Platnost licencí minimálně 36 měsíců od data instalace

Specifikace centrální správy

Popis vlastností
Správa všech poptávaných produktů (ochrana endpointů a serverů) z jednoho administračního rozhraní
Přístup do administračního rozhraní pomocí protokolu HTTPS
Centrální administrační rozhraní musí mít dokumentované API
Vícefaktorová autentifikace pro administrátory
Centrální administrace podporuje automatické odhlášení uživatele při nečinnosti
Centrální správa je poskytována online výrobcem v zabezpečeném datacentru (cloud)
Synchronizace uživatelů a skupin je zajištěna pomocí služby, jež vyčítá informace z Active Directory a šifrovaným tunelem je synchronizuje do centrální správy.
Synchronizační služba synchronizuje minimálně tyto parametry: Username, Login, Email address, skupiny a členy každé skupiny
Synchronizační služba musí podporovat LDAP filtry pro užší výběr synchronizovaných položek
Synchronizační služba musí podporovat manuální a intervalovou synchronizaci v definovaných časových intervalech
Mimo synchronizaci uživatelů a skupin z Active Directory musí řešení nabízet vytváření lokálních uživatelů a skupin
Centrální administrační rozhraní musí umožnit vytvoření min. dvoustupňové hierarchické struktury (celá organizace - podřízené organizace)
Administrátor celé organizace musí mít právo vytvářet podřízené organizace/entity a přidělovat jim potřebné licence z rozsahu přiděleného celé organizaci
Administrátoři podřízených organizací mohou administrovat pouze svoji organizaci/entitu a její uživatele
Centrální administrace podporuje řízení uživatelů dle rolí a to minimálně v rozsahu: • Administrátor celé organizace - Může vytvářet nové podřízené entity a přidělovat jim administrátory • Administrátor podřízené entity - Má plná práva pro správu a může přidělovat role dalším uživatelům • Pracovník technické podpory - Má práva pro čtení pro správu, může číst logy, může vyvolat sken a update uživatelského zařízení, spravuje výstrahy • Uživatel s přístupem pro čtení - Má práva pro čtení pro správu, logy a výstrahy
Centrální administrace podporuje napojení na systémy SIEM a zasílání událostí typu Události a Výstrahy
Centrální administrace poskytuje vestavěné logování a reportování

Centrální administrace podporuje zasílání alertů emailem na definované adresy
Centrální administrace disponuje souhrnným dashboardem, tedy místem, na kterém se zobrazují klíčové informace o celém prostředí

Specifikace endpoint protection

Popis vlastností
Licence na počet použitých zařízení
Podpora OS Windows 8 a vyšší, MAC OS X 10.10 a vyšší
Blokování škodlivých webových stránek
Kontrola souborů dle reputace
Webová kontrola / Blokování URL na základě kategorie (nejméně 40 předdefinovaných kategorií)
Kontrola a blokování HW zařízení - USB disky, externí HDD, CD/DVD, Wi-Fi, Bluetooth, IR, Modemy
Kontrola a blokování aplikací, nejméně 40 předdefinovaných kategorií
Detekce malware pomocí strojového učení Deep Learning
Skenování souborů proti malware (lokální i vzdálené soubory)
Skenování archivů
Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze
Analýza chování před spuštěním souboru (HIPS)
Blokování potenciálně nechtěných aplikací (PUA)
DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení
Detekce a prevence známých i neznámých exploitů, nezávislá na signaturách
Ochrana před následujícími exploitními technikami: - Enforce Data Execution Prevention (DEP) - Mandatory Address Space Layout Randomization (ASLR) - Bottom Up ASLR - Null Page (Null Dereference Protection) - Heap Spray Allocation - Dynamic Heap Spray - Stack Pivot - Stack Exec (MemProt) - Stack-based ROP Mitigations (Caller) - Branch-based ROP Mitigations - Structured Exception Handler Overwrite Protection (SEHOP) - Import Address Table Filtering (IAF) - Load Library - Reflective DLL Injection - VBScript God Mode - WoW64 - Syscall - Hollow Process - DLL Hijacking - Shellcode a Dynamic Shellcode - APC Protection (Double Pulsar / AtomBombing) - Squiblydoo AppLocker Bypass - Process Privilege Escalation
Detekce a odstranění rootkitů
Detekce škodlivého provozu typu Command and Control (botnet)
Analýza chování při běhu procesů

Aktivní zamezení negativních dopadů zneužití zranitelností
Blokování neautorizovaného šifrování (kryprovirus) dat
Automatická obnova souborů do původního stavu před zašifrováním
Ochrana Master Boot Record před zašifrováním
Ochrana prohlížeče před injektáží kódu
Automatické odstranění malware
Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware
Určení zdroje a příčiny útoku, grafická reprezentace děje útoku
Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta
Detekce pomocí strojového učení bez nutnosti připojení k internetu
Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres
Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce).
Vytvoření „hash“ pro soubor na úrovni lokálního agenta
Vyhledání infikovaných počítačů na základě „hash“ malware
Automatické vyhodnocení incidentů
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby) minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.
Možnost dešifrace a kontroly HTTPS provozu
Application lockdown (Web Browser, Java, Media, Office)
Součástí řešení je lehký klient na koncové stanice
Řešení poskytuje zázemí pro threat hunting
Možnost terminálového připojení na endpoint z centální správy na úrovni systému
Možnost spouštění SQL dotazů vůči endpointům pro aktivní vyhledávaní hrozeb (minimálně 200 před definovaných dotazů)
Automatická nebo manuální izolace koncového zařízení (např. při napadení malwarem)
Správa Windows Firewall

Specifikace server protection

Popis vlastností
Licence na chráněný serverový OS
Podpora OS Windows Server 2012 a vyšší, Amazon Linux 2, CentOS 7/Minimal/Stream, Red Hat Enterprise Linux 7/8, Ubuntu 18.04/20.04/Minimal
Podpora Windows Remote Desktop Services
Blokování škodlivých webových stránek
Kontrola souborů dle reputace
Webová kontrola / Blokování URL na základě kategorie (nejméně 10 předdefinovaných kategorií)
Kontrola a blokování HW zařízení - USB disky, externí HDD/SSD, CD/DVD, Wi-Fi, Bluetooth, IR, Modemy
Kontrola a blokování aplikací, nejméně 40 předdefinovaných kategorií
Whitelisting aplikací
Správa Windows Firewall
Možnost bezagentového skenování virtuálních prostředí VMware a Hyper-V

Detekce malware pomocí strojového učení Deep Learning
Automatické výjimky ze skenování
Skenování souborů proti malware
Skenování archivů
Signatury AV dostupné v reálném čase v Cloudu, nezávislost na četnosti aktualizace databáze
Analýza chování před spuštěním souboru (HIPS)
Blokování potenciálně nechtěných aplikací (PUA)
DLP - blokování přenosu dat na základě pravidel, možnost úplné blokace nebo upozornění uživatele a vyžádání potvrzení
Detekce a prevence známých i neznámých exploitů, nezávislá na signaturách
Ochrana před následujícími exploitními technikami: - Enforce Data Execution Prevention (DEP) - Mandatory Address Space Layout Randomization (ASLR) - Bottom Up ASLR - Null Page (Null Dereference Protection) - Heap Spray Allocation - Dynamic Heap Spray - Stack Pivot - Stack Exec (MemProt) - Stack-based ROP Mitigations (Caller) - Branch-based ROP Mitigations - Structured Exception Handler Overwrite Protection (SEHOP) - Import Address Table Filtering (IAF) - Load Library - Reflective DLL Injection - VBScript God Mode - WoW64 - Syscall - Hollow Process - DLL Hijacking - Shellcode a Dynamic Shellcode - APC Protection (Double Pulsar / AtomBombing) - Squiblydoo AppLocker Bypass - Process Privilege Escalation
Detekce a odstranění rootkitů
Detekce škodlivého provozu typu Command and Control (botnet)
Analýza chování při běhu procesů
Aktivní zamezení negativních dopadů zneužití zranitelností
Blokování neautorizovaného šifrování (kryprovirus) dat
Automatická obnova souborů do původního stavu před zašifrováním
Ochrana Master Boot Record před zašifrováním
Ochrana prohlížeče před injektáží kódu
Automatické odstranění malware
Automatické odstranění zbytkových souborů (čištění registrů) po zablokování malware
Určení zdroje a příčiny útoku, grafická reprezentace děje útoku
Ochrana proti zásahu uživatele s lokálními admin. právy do nastavení klienta
Uzamčení stavu serveru z pohledu aplikací a služeb

Zjednodušený náhled na nákazu minimálně v rozsahu, vstupní bod malware do systému (aplikace), malware, přijaté opatření Grafické znázornění průběhu nákazy minimálně v rozsahu, vstupní bod malware do systému (aplikace), zápisy do systému a do registrů OS, komunikace na internet včetně zobrazí IP a URL adres
Možnost globálního vyčištění a blokování nalezeného malware na všech systémech najednou (pomocí jedné akce).
Vytvoření „hash“ pro soubor na úrovni lokálního agenta
Vyhledání infikovaných počítačů na základě „hash“ malware
Automatické vyhodnocení incidentů
Zobrazení obecných informací o proběhnutých útocích (alespoň z poslední doby) minimálně v rozsahu jméno malware, počet postižených systémů a hodnocení nebezpečnosti malware výrobcem.
Možnost tzv. Lockdownu zařízení, následně není možná instalace aplikací
Aktivní rozeznávání běžících aplikací
Možnost spouštění SQL dotazů vůči serverům pro aktivní vyhledávaní hrozeb (minimálně 200 před definovaných dotazů)
Řešení poskytuje zázemí pro threat hunting
Řešení disponuje před-definovanými politikami dle best practices
Anti-Virus pro Linux servery (Amazon Linux/Amazon Linux 2, CentOS 7/8, Debian 9/10, Oracle Linux 7/8, RHEL 7/8, SUSE Linux Enterprise Server 12/15, Ubuntu 18LTS/20.04 LTS)