

Licenční smlouva

Smluvní strany

ESET software spol. s r.o.

se sídlem: Jankovcova 1037/49, 170 00 Praha 7,
zastoupená: Jurajem Ferencem, ředitelem na základě plné moci ze dne 12.9.2016,
IČO: 26467593,
DIČ: CZ26467593,
bankovní spojení: [REDAKCE]
č. ú.: [REDAKCE]
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 84196,
(dále jen „poskytovatel“)

a

město Sokolov

se sídlem: Rokycanova 1929, 356 01 Sokolov,
zastoupené: Bc. Janem Pickou, starostou,
IČO: 00259586,
bankovní spojení: [REDAKCE]
č. ú.: [REDAKCE]
(dále jen „nabyvatel“)

uzavírají níže uvedeného dne v souladu s příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, (dále jen „občanský zákoník“) tuto smlouvu:

Čl. 1

Úvodní ustanovení

Tato smlouva se uzavírá na základě výsledů zadávacího řízení na zadání veřejné zakázky malého rozsahu s názvem „Dodávka antivirového SW“ v souladu s výzvou nabyvatele ze dne 14.08.2018 a nabídkou poskytovatele ze dne 21.8.2018 na plnění uvedené veřejné zakázky (dále jen „Nabídka“).

Čl. 2

Předmět smlouvy

- 2.1 Poskytovatel touto smlouvou a za podmínek v ní uvedených poskytuje nabyvateli právo užívat antivirový software ESET Secure Office Plus na 300 zařízení a ESET Mail Security na 300 mailboxů, jehož přesná specifikace je uvedena v Požadovaných technických parametrech produktu, jež jsou přílohou č. 1 k této smlouvě, a v Nabídce, jež je přílohou č. 2 k této smlouvě, (dále jen „antivirový SW“).
- 2.2 Součástí licenčního práva podle odst. 2.1 a odměny za něj jsou rovněž:
- právo na aktualizace virové databáze antivirového SW, programových komponent antivirového SW, právo upgradu na nové verze antivirového SW,
 - poskytování servisní podpory antivirového SW,
 - poskytování technické podpory antivirového SW v češtině v rozsahu 12/5 po telefonu, elektronickou poštou nebo vzdáleně, a to podle volby nabyvatele,
 - instalace antivirového SW nebo provedení jeho aktualizace či upgrade v případě požadavku nabyvatele na jejich provedení, popř. pomoc s touto instalací či aktualizací,
 - školení určených zaměstnanců nabyvatele stran užívání antivirového SW, konzultace, pomoc s instalací / nasazením / aktualizací / ověřením bezpečnostních politik v ceně.
 - 4 hodiny práce poskytovatele související s předmětem smlouvy, provedené na vyžádání nabyvatele buď na místě (v sídle nabyvatele) nebo vzdáleně.
- 2.3 Práva podle odst. 2.1 a 2.2 se udělují jako nevýhradní na dobu uvedenou v čl. 4.
- 2.4 Právo podle odst. 2.1 se poskytuje v počtu 300 instalací na koncová zařízení, zahrnující stanice, servery, mobilní zařízení a terminálové relace a 1 ks Microsoft Exchange 2010 server (pro 300 ks poštovních schránek). Nabyvatel je oprávněn užívat antivirový SW na jakémkoliv zařízení v jeho vlastnictví, avšak v maximálním počtu licencí podle věty první, s tím, že licencí podle této

smlouvy není povinen využít.

- 2.5 Poskytovatel je oprávněn k výkonu práva, ke kterému udělil nevýhradní licenci podle této smlouvy, jakož i poskytnout licenci podle této smlouvy nabyvateli.
- 2.6 Poskytovatel garantuje, že antivirový SW má vlastností uvedené v Nabídce a v příloze č. 1 - Požadované technické parametry produktu.

Čl. 3

Odměna

- 3.1 Odměna za užívání licence za celou dobu trvání smlouvy podle čl. 4 se sjednává ve výši 485 280,- Kč (slovy čtyřistaosmdesátpěttisícdvěstěosmdesát korun českých) bez DPH. K odměně se připočte DPH v příslušné zákonné sazbě.
- 3.2 Odměna podle předchozího odstavce zahrnuje odměnu za právo k užívání antivirového SW v rozsahu podle této smlouvy včetně jeho aktualizace, upgrade a poskytování servisní a technické podpory.
- 3.3 Odměna podle odst. 3.1 je konečná, nejvýše přípustná a pevná a zahrnuje veškeré náklady poskytovatele spojené s poskytováním plnění podle této smlouvy včetně odměny za poskytnutí licence k užívání dodaného softwaru. Jediným důvodem změny výše odměny je změna zákonné sazby DPH.
- 3.4 Odměna podle odst. 3.1 je splatná ve čtyřech rovnoměrných částech za každý rok trvání smlouvy, a to na základě daňového dokladu (faktury) vystaveného poskytovatelem. Fakturu na úhradu části odměny za první rok trvání smlouvy vystaví poskytovatel do 14 dnů od předání antivirového SW podle čl. 4 odst. 4.2. Faktury na úhradu části odměny za druhý a následující roky trvání smlouvy vystaví poskytovatel vždy do 14 dnů od počátku příslušného roku, za který se má odměna hradit.
- 3.5 Faktura musí obsahovat veškeré náležitosti daňového dokladu stanovené příslušnými právními předpisy, zejména zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Nebude-li faktura splňovat veškeré náležitosti řádného daňového dokladu nebo bude-li mít jiné závady v obsahu, je nabyvatel oprávněn ji ve lhůtě její splatnosti poskytovateli vrátit a ten je povinen vystavit fakturu opravenou či doplněnou. V případě vrácení faktury poskytovateli se lhůta splatnosti přerušuje a nová lhůta splatnosti počíná běžet od počátku dnem následujícím po dni, kdy byla opravená či doplněná faktura splňující všechny náležitosti doručena nabyvateli.
- 3.6 Odměna je splatná do 30 dnů od ode dne doručení faktury nabyvateli, a to bezhotovostním převodem na bankovní účet poskytovatele uvedený v záhlaví této smlouvy.
- 3.7 Za den úhrady odměny se považuje den odepsání fakturované částky z účtu nabyvatele ve prospěch účtu poskytovatele.
- 3.8 Poskytovatel nemá nárok na zaplacení části odměny za dobu, po kterou nebyl antivirový SW dostupný či poskytován.

Čl. 4

Doba trvání licence a dodací podmínky

- 4.1 Závazek zřízený touto smlouvou se sjednává na dobu určitou v trvání 4 let počínaje dnem účinnosti této smlouvy.
- 4.2 Poskytovatel předá nabyvateli antivirový SW formou předání příslušných licenčních klíčů elektronickou poštou na adresu [redacted] a to bezodkladně, nejpozději však do 5 dnů od nabytí účinnosti této smlouvy. Spolu s antivirovým SW předá poskytovatel nabyvateli veškeré doklady potřebné k řádnému užívání antivirového SW v českém jazyce.
- 4.3 Instalaci antivirového SW jakož i aktualizace a upgrade podle čl. 2 odst. 2.2 písm. a) provádí nabyvatel svépomocí, přičemž má právo k tomu využít podporu poskytovatele podle čl. 2 odst. 2.2 písm. d) a ten je povinen mu ji bezodkladně poskytnout.

Čl. 5

Ukončení smlouvy

- 5.1 Každá ze smluvních stran je oprávněna tuto smlouvu vypovědět bez udání důvodu s 6měsíční výpovědní dobou počínající běžet prvního dne následujícího po jejím doručení.

- 5.2 Nabyvatel je kromě důvodů pro odstoupení od smlouvy stanovených občanským zákoníkem oprávněn odstoupit od této smlouvy v případě, že:
- poskytovatel je v prodlení s dodáním antivirového SW podle čl. 4 odst. 4.2 déle než 10 dnů,
 - antivirová ochrana prostřednictvím antivirového SW bude nedostupná déle než 24 hodin po sobě jdoucích,
 - proti poskytovateli bude zahájeno insolvenční řízení a insolvenční návrh nebude v zákonné lhůtě odmítnut pro zjevnou bezdůvodnost nebo insolvenční návrh prodávajícího bude zamítnut proto, že majetek prodávajícího nepostačuje ani k úhradě nákladů insolvenčního řízení, anebo prodávající vstoupí do likvidace,
 - ukáže-li se prohlášení poskytovatele podle čl. 2 odst. 2.5 nebo 2.6 nepravdivým.
- 5.3 Poskytovatel je oprávněn odstoupit od smlouvy v případě prodlení nabyvatel s úhradou odměny podle čl. 3 delšího než 30 dní.
- 5.4 Účinky odstoupení nastávají dnem doručení písemného oznámení o odstoupení druhé smluvní straně.
- 5.5 Odstoupením od smlouvy není dotčen nárok na smluvní pokutu ani na náhradu škody.

Čl. 6

Smluvní pokuty

- 6.1 V případě prodlení s dodáním antivirového SW podle čl. 4 odst. 4.2 je poskytovatel povinen zaplatit nabyvateli smluvní pokutu ve výši 1 000 Kč za každý i započatý den prodlení.
- 6.2 V případě nedostupnosti aktualizčních serverů pro aktualizaci antivirového SW je poskytovatel povinen uhradit nabyvateli smluvní pokutu, jejíž výše se určí jako procentní část roční částí odměny podle čl. 3 odst. 3.4 takto:

Měsíční dostupnost antivirového SW	Smluvní pokuta
Dostupnost nižší než 100 % - 99,0 % vč.	5 %
Dostupnost nižší než 99,0 % - 97,0 % vč.	10 %
Dostupnost nižší než 97,0 %	20 %

- 6.3 Nabyvatel je oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 500 Kč v případě porušení jakékoliv jiné povinnosti uvedené v této smlouvě za každý den prodlení s nápravou přes výzvu nabyvatele o více než 3 dny po doručení takovéto výzvy.
- 6.4 Úhradou smluvní pokuty není dotčeno právo na náhradu škody způsobené porušením povinnosti, pro kterou je smluvní pokuta sjednána.
- 6.5 Smluvní pokuta je splatná na základě písemné výzvy nabyvatele do 15 dnů od doručení výzvy poskytovateli převodem na účet uvedený v záhlaví této smlouvy.
- 6.6 Povinnost zaplatit smluvní pokutu může vzniknout i opakovaně a její celková výše není omezena.
- 6.7 Povinnost zaplatit smluvní pokutu trvá i po skončení této smlouvy či odstoupení od ní.
- 6.8 poskytovatel považuje smluvní pokuty sjednané v tomto článku za přiměřené a vzdává se práva domáhat se u soudu jejich snížení.
- 6.9 Nabyvatel je oprávněn jakoukoliv smluvní pokutu podle této smlouvy jednostranně započítat proti jakékoli pohledávce poskytovatele za nabyvatelem, včetně pohledávky poskytovatele na zaplacení odměny podle čl. 3.

Čl. 7

Odpovědnost za škodu

- 7.1 Odpovědnost za škodu se řídí ust. § 2894 a násl. občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k jejich minimalizaci.
- 7.2 Poskytovatel neodpovídá za újmy, které by mohly vzniknout v souvislosti s užíváním předmětu této licenční smlouvy.

7.3 Poskytovatel je povinen za nabyvatele úplně a bez jeho přispění vyřídit a urovnat jakékoli požadavky třetích osob vyplývající z případných autorských práv (jejich možného porušení, atp.) k předmětu smlouvy.

Čl. 8

Závěrečná ustanovení

- 8.1 V případě neplatnosti některého ustanovení této smlouvy nebo v případě, že se některé ustanovení této smlouvy stane neplatným později, nemá tato skutečnost vliv na platnost této smlouvy jako celku.
- 8.2 Tato smlouva může být změněna pouze písemnou dohodou obou smluvních stran formou vzestupně číslovaných dodatků.
- 8.3 Právní vztahy touto smlouvou neupravené se řídí ustanoveními občanského zákoníku.
- 8.4 Veškeré písemnosti si budou strany této smlouvy předávat osobně, zasílat na adresy uvedené v záhlaví této smlouvy nebo do datové schránky, nestanoví-li se v této smlouvě jinak. Pro vztahy z této smlouvy se písemnost zasláná doporučeně prostřednictvím České pošty, s. p., bude považovat za doručenou i v případě, že se z jakéhokoliv důvodu vrátí taková zásilka zasláná na adresu v záhlaví této smlouvy jako nedoručená, a to i v případě, že se na této adrese nebude smluvní strana zdržovat.
- 8.5 Tato smlouva se vyhotovuje ve 2 stejnopisech, z nichž každá strana smlouvy obdrží po jednom výtisku.
- 8.6 Strany této smlouvy prohlašují, že tuto smlouvu uzavřely svobodně a vážně a pokládají ji za určitou a srozumitelnou. Po jejím přečtení prohlašují, že s jejím zněním souhlasí, což stvrzují svými podpisy.
- 8.7 Smlouva nabývá platnosti dnem podpisu obou smluvních stran a účinnosti dnem jejího uveřejnění prostřednictvím 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), ve znění pozdějších předpisů. Smluvní strany se dohodly, že smlouvu bez zbytečného odkladu uveřejní podle předchozí věty nabyvatel. Nabyvatel se zavazuje vyrozumět poskytovatele o uveřejnění smlouvy prostřednictvím registru smluv bez zbytečného odkladu poté, kdy sám obdrží potvrzení o uveřejnění smlouvy.
- 8.8 Smluvní strany výslovně prohlašují, že žádné ustanovení této smlouvy není obchodním tajemstvím podle § 504 občanského zákoníku ani neobsahuje důvěrnou informaci o poměrech smluvní strany nebo skutečnostech, které má smluvní strana potřebu ochraňovat jako důvěrnou informaci nebo předmět obchodního tajemství.
- 8.9 Nedílnou součástí smlouvy jsou následující přílohy:
- a) Příloha č. 1 – Požadované technické parametry produktu,
 - b) Příloha č. 2 – Nabídka.
- 8.10 O uzavření této smlouvy rozhodla Rada města Sokolova dne 02.10.2018 usnesením č. 674/23RM/2018.

V Sokolově dne

11. 10. 2018

Za nabyvatele:



Bc. Jan Picka

V Praze dne

5. 10. 2018

Za poskytovatele:



Juraj Ferenc

Příloha č. 1 - Požadované technické parametry produktu:

- Podpora operačních systémů MS:
 - Windows XP a vyšší, Windows server 2003 a vyšší.
- Antivirový klient také pro ochranu systémů:
 - Linux, macOS a Android.
- Real-Time ochrana před všemi druhy malwaru:
 - viry, červy, trojskými koňmi (backdoor, adware, spyware, rootkit, bootkit, ransomware...).
- Napojení na centrální správu, ze které lze spravovat konfigurovat i MDM (Mobile Device Management).
- Heuristická analýza pro detekci neznámých hrozeb a škodlivých aplikací.
- Správa zařízení (včetně mobilních) pro Windows, macOS a Linux umožňující blokadu médií s podporou whitelistování na základě definování:
 - výrobce, modelu nebo sériového čísla,
 - uživatelů nebo skupin (např. administrátorů) v AD.
- Možnost blokace přístupu na definované weby nebo domény.

Technologie

- Antivirus a Antispyware pro aktivní ochranu před všemi typy hrozeb.
- Anti-Phishing s proaktivní technologií analyzující grafickou podobu stránky ve snaze eliminovat nově vytvořené falešné protějšky.
- Systém prevence vniknutí na bázi hostitele pro ochranu operačního systému a eliminaci aktivit ohrožující bezpečnost zařízení, systém pro blokadu exploitů využívajících zero-day zranitelností, jenž pokrývá nejpoužívanější vektory útoku:
 - Flash Player, Javu, Microsoft Office, webové prohlížeče, e-mailové klienty, PDF čtečky...
- Pokročilá kontrola RAM paměti pro lepší detekci malwaru využívající silnou obfuskaci a šifrování.
- Detekce potenciálně nechtěných, zneužitelných a podezřelých aplikací.
- Funkce pro ochranu před skriptovými útoky využívajícími:
 - JavaScript, Windows PowerShell, Windows Script Host.
- Kontrola s podporou cloudu pro odesílání a online vyhodnocování neznámých a potenciálně škodlivých aplikací.
- Lokální i cloudový sandbox.
- Systém reputace a cache pro získání informací o závadnosti stahovaných souborů a URL adres.
- Cloudový systém pro detekci nového malwaru ještě nezaneseného v aktualizacích signatur.
- Technologie pro detekci rootkitů obvykle se maskujících za součásti operačního systému.

Klient

Správa zařízení (včetně mobilních) pro Windows, macOS a Linux umožňující blokadu médií s podporou whitelistování na základě definování:

- výrobce, modelu nebo sériového čísla, uživatelů nebo skupin (např. administrátorů) v AD.

Provádění kontrol při nečinnosti zařízení:

- vypnuté obrazovce, aktivním spořiči obrazovky, uzamčení počítače, odhlášení uživatele.
- Možnost využití sdílené reputační cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolovány na jiném zařízeních a tím výrazně zrychlit kontrolu celé sítě).
- Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
- Podpora odebíratele obrazovky pro zrakově postižené.

Personální vypínatelný firewall s možností automatického přepínání režimů na základě typu připojení, stavu klienta, a dalších podmínek

Vzdálená správa – centrální řešení

Jediná konzole vzdálené správy pro konfiguraci bezpečnostních produktů na mobilní zařízení (MDM), desktopové systémy i servery.

- Uložení nastavení a logů (přístupy, události, výsledky skenů) v databázi na stávajícím MS SQL 2008 a novějším s možností načítat je do SIEM (Security Information and Management) a podpora SNMP Trap, Syslogu
- Centrální úložiště logů (provedené administrativní kroky – kdy, kdo a co nastavil, výsledky skenů jednotlivých stanic/serverů) s prohlížečem (možnost filtrace události dle PC, uživatele, data, typu události...)
- Nabízené řešení lze implementovat v českém a anglickém jazyce (veškeré hlášky antiviru jakož i administrativní část jsou lokalizovány do českého a anglického jazyka)
- Možnost tvorby spouštěcího CD/DVD/USB s antivirem a aktuálními definicemi vzorků pro offline skenování (potenciálně) napadeného počítače
- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Notifikace administrátora pomocí emailu v případě výskytu specifických událostí (lze si definovat konkrétní typy těchto specifických událostí), možnost zaslání pravidelného sumarizačního reportu mailem v definovaném intervalu (denně/týdně/měsíčně apod.)
- Na běžících antivirech na koncových stanicích/serverech/relacích uživatelů na terminálovém serveru lze administrovat oprávnění k pozastavení či úplnému vypnutí antivirového programu a jeho komponent
- Antivirový program a jeho komponenty musí obsahovat ochranný mechanismus chránící je před modifikací
- Antivir musí být schopen skenování externích médií (floppy, CD/DVD, USB připojená zařízení) ať už na pracovní stanici, tak i v terminálové relaci, kdy uživatel pracuje na tenkém klientu s nemodifikovatelným OS Windows XP/7 embedded, na který nelze antivir instalovat

Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí Příkazového řádku. ▪ Předpřipravená virtual appliance pro virtuální prostředí VMware, Microsoft Hyper-V a Microsoft Azure, Oracle Virtual Box.

- Nezávislý agent (pracuje i offline) vzdálené správy pro zajištění komunikace a ovládání operačního systému klienta a bezpečnostního programu.
- Offline uplatňování politik a spouštění úloh při výskytu definované události (například: odpojení od sítě při nalezení škodlivého kódu).
- Server/proxy architektura pro síťovou pružnost – snížení zátěže při komunikaci klientů ze vzdálených lokalit na server.
- Zabezpečení přístupu administrátorů do vzdálené správy pomocí 2FA.
- Možnost přihlašování administrátorů pomocí doménových účtů.
- Vzdálená aktivace bezpečnostního programu.
- Export/import konfigurace bezpečnostního programu z klienta.
- Jednorázové testování virtuálních stanic i bez nainstalovaného bezpečnostního programu.
- Správa karantény s možností vzdáleného vymazání / obnovení / obnovení a vyloučení objektu z detekce.
- Vzdálené získání škodlivého kódu z klienta.
- Detekce nespravovaných (rizikových) počítačů komunikujících na síti.
- Vzdálené odebrání licence klientovi.
- Odeslání zprávy na počítač, které se následně zobrazí uživateli na obrazovce.
- Vzdálená odinstalace antivirového řešení 3. strany.
- Vzdálené spuštění jakéhokoli příkazu na cílové stanici pomocí příkazového řádku.
- U mobilních zařízení dostupné vzdálené:
 - nalezení, uzamknutí, odemknutí, siréna, vymazání obsahu, rozšířený reset do továrního nastavení.

- Dynamické skupiny pro možnost definování podmínek, za kterých dojde k automatickému zařazení klienta do požadované skupiny.
- Dynamicky se měnící interaktivní přehledy pro okamžité zjištění stavu spravované sítě.
- Vzdálená správa umožňující management klientů pomocí mobilních zařízení (telefonu/tabletu).
- Automatické zasílání upozornění při dosažení definovaného počtu nebo procent ovlivněných klientů (například: 5 % všech počítačů / 50 klientů hlásí problémy).
- Podpora instalace skriptem - *.bat, *.sh, *.ini (GPO, SSCM...).
- Rychlé připojení na klienta pomocí RDP z konzole pro vzdálenou správu.
- Reportování stavu antiviru 3. strany, včetně vzdálené správy klientů chráněných jinými bezpečnostními programy.
- Po X neúspěšných pokusech o přihlášení do systému vzdálené správy z jedné IP adresy server přihlášení na tuto IP adresu na X minut zablokuje.

Ostatní vlastnosti

- Podpora Microsoft NAP.
- Velmi nízké systémové nároky umožňující bezproblémové použití i na málo výkonných zařízeních:
- Možnost odložení aktualizací a běžných klientských úloh pro lepší využití systémových prostředků.
- Provádění kontrol při nečinnosti zařízení:
 - vypnuté obrazovce, aktivním spořiči obrazovky, uzamčení počítače, odhlášení uživatele.
- Ovládání bezpečnostního programu pomocí Příkazového řádku.
- Podpora ochrany na IPv6.
- Možnost řízení šířky pásma pro stahování aktualizací.
- Systém prevence vniknutí na bázi hostitele (HIPS) s možností definovat pravidla pro systémové registry, procesy, aplikace a soubory.
- Možnost instalovat plnohodnotné antivirové řešení na virtuální stanici/server, modulární instalaci a podporu clusteru.
- Zabezpečení pro VMware vShield a NSX.
- Možnost importu/exportu nastavení.
- Prezentační režim umožňující potlačení méně důležitých upozornění při práci v celoobrazovkovém režimu aplikace.
- Možnost tvorby výjimek na procesy.
- Ochrana před neautorizovanou změnou nastavení / vyřazení z provozu / odinstalací antimalware řešení a kritických nastavení a souborů operačního systému.
- Možnost vzdáleného definování akce při připojení výměnných médií (kontrolovat, nekontrolovat, nechat na uživateli).
- Možnost využití sdílené reputační cache v rámci lokální sítě (umožňuje přeskočení skenování stejných souborů, které již byly zkontrolovány na jiném zařízeních a tím výrazně zrychlit kontrolu celé sítě).
- Duální aktualizací profil pro možnost stahování aktualizací z mirroru v lokální síti a zároveň vzdálených serverů při nedostupnosti lokálního mirroru (vhodné pro cestující uživatele s notebooky).
- Kontrola šifrovaných spojení (SSL, TLS, HTTPS, IMAPS...).
- Možnost odesílání e-mailových upozornění a událostí přímo z klienta.
- Komplexní diagnostický nástroj umožňující řešit problémy s infiltrací, jakožto i jiné softwarové a hardwarové nekorektní chování (obsahuje informace procesech, službách, síťových připojeních, ovladačích, problémových položkách v registrech...).
- Upozornění při připojení k nezabezpečené bezdrátové síti nebo síti se slabým zabezpečením, jejíž šifrování lze snadno prolomit.
- Využití Microsoft Antimalware Scan Interface (AMSI) pro kontrolu skriptů (PowerShell, wscript.exe a cscript.exe).
- Podpora Protected Services – službu produktu je možné chránit proti nechtěné modifikaci standardní součástí operačního systému.

Provozní

Požadované počty licencí

Zadavatel požaduje dodání licencí pro:

- 300 ks rezidentů na koncových zařízeních (stanice, servery, mobilní zařízení a terminálové relace)
- 1 ks MS Exchange 2010 server (pro 300 ks poštovních schránek)

Dodavatel navrhne optimální způsob licencování s ohledem na rozdílný počet uživatelů a zařízení.

Zadavatel požaduje dodávku výše uvedených licencí na dobu 4 let včetně podpory. Platby se předpokládají v následujícím režimu:

1. rok bude zaplácena cena za licence a za podporu na první rok
2. rok bude zaplácena cena za prodloužení podpory o další rok
3. rok bude zaplácena cena za prodloužení podpory o další rok
4. rok bude zaplácena cena za prodloužení podpory o další rok

Součástí instalace školení, konzultace, pomoc s instalací / nasazením / aktualizací / ověřením bezpečnostních politik v ceně.

Dále pak možnost vyžádat jednou ročně, 4 hodiny práce na místě/vzdáleně tíž v ceně dodávky.

Dodavatel musí mít také řešení pro:

Data Loss Prevention (DLP), dvou faktorové ověření (2FA), šifrování, patch management.

- Technická podpora v češtině.
- Technická podpora zdarma 12/5 poskytující pomoc na telefonu / přes e-mail / vzdáleně.



ENJOY SAFER TECHNOLOGY™

Cenová nabídka pro Město Sokolov

Nabídka č.: NAV11440/2018

Ze dne: 30. 8. 2018

Platnost do: 31. 10. 2018

Zpracoval: [REDACTED]

Řešení Sleva	Počet	Cena koncová Cena s DPH
Nová licence, ESET Secure Office Plus, 4 roky Sleva pro subjekty veřejné správy - 20 %	300	402 480,00 CZK 487 000,80 CZK
Nová licence, ESET Mail Security, 4 roky Sleva pro subjekty veřejné správy - 20 %	300	82 800,00 CZK 100 188,00 CZK

Celkem bez DPH: 485 280,00 CZK

Celkem s DPH: 587 188,80 CZK

ESET software spol. s r.o. si vyhrazuje právo na budoucí změnu cen.
V případě zájmu je možné představit produkty ESET v prostorách naší společnosti.

ESET software spol. s r. o., Classic 7 Business Park, Jankovcova 1037/49, 170 00 Praha 7

Telefon: [REDACTED] e-mail: [REDACTED]

