**Příloha č. 1**

## Předmět plnění

Cílem tohoto zadávacího řízení je výběr partnera pro následné uzavření smlouvy, jejímž cílem bude:

Realizace projektu **„Dodávka a implementace antivirového řešení pro ochranu pracovních stanic“** tak, aby byla umožněna efektivní správa, ochrana a kontrola antivirového řešení v rámci všech koncových stanic. Plnění dále zahrnuje zaškolení pracovníků IT objednavatele.

V rámci přípravy a realizace výše zmíněného projektu zadavatel veřejné zakázky od dodavatele požaduje splnění těchto bodů:

**1) Poskytované plnění se bude skládat z následujících částí:**

a) dodání, instalaci, konfiguraci antivirového programu (dále jen „Software“) odpovídajícího níže uvedeným požadavkům a jeho uvedení do běžného provozu – do 2 týdnů od nabytí účinnosti smlouvy,

b) odinstalaci stávajícího antivirového programu (pouze v případě, že nebude totožný s nově pořizovaným) – do 2 týdnů od nabytí účinnosti smlouvy,

c) poskytnutí uživatelských licencí k dodanému Software v počtu 450 kusů - na 3 roky,

d) provedení úvodního školení správců - zaměstnanců zadavatele – do 2 týdnů od nabytí účinnosti smlouvy,

e) poskytování veškerých oficiálních aktualizací Software (tj. update, doplňování databází, záplat atd.) – po celou dobu trvání licencí, tj. 3 roky,

f) nepřetržitá konzultační podpora (tj. v režimu 24/7), s reakční dobou do 4 hodin – na 3 roky.

**2) Popis stávajícího prostředí**

VOP CZ, s.p. má v současné době zajištěnu antivirovou ochranu Software ESET včetně centrální správy v počtu 520 licencí. Antivirová ochrana je zajištěna do 23.03.2021.

**3) Kvalifikační (povinné) požadavky na centrální správu:**

a) Vzdálená instalace a odinstalace klientské části z lokálních serverů v každé lokalitě, včetně možnosti automatické odinstalace starších verzí antivirů, případně konkurenčních produktů.

b) Centrální distribuce virových vzorků z lokálních serverů v každé lokalitě s možností automatického přepnutí na aktualizační servery výrobce v okamžiku případného selhání lokálního distribučního serveru.

c) Podpora poboček, umožňující nezávislou správu místními správci lokálních poboček a zároveň centrální dohled nad všemi pobočkami z jednoho uživatelského pohledu včetně možnosti definovat úroveň oprávnění lokálních správců.

d) Možnost přihlášení do administračního rozhraní jak pomocí integrovaných administračních účtů, tak i pomocí bezpečnostní doménové skupiny.

e) Možnost vytváření politik a úloh hlavním administrátorem s možností přidělení administrátorovi na konkrétní pobočce.

f) Možnost přidělení přesného počtu licencí (poměrná část z celkového počtu licencí) pro konkrétní pobočku s možností definovat administrátory licencí na dané pobočce.

g) Možnost nastavit centrální politiky pro podnik jednotně přes všechny pobočky s možností definovat specifické politiky s granularitou: pobočka, skupina v Active Directory, jednotlivá pracovní stanice.

h) Podpora statických a dynamických skupin v rámci administračního rozhraní s možností provádění automatických úloh platných pro tyto skupiny včetně možnosti rozdílných politik pro statické i dynamické skupiny.

i) Nastavené bezpečnostní zásady musí být na koncových bodech aplikovány a vyžadovány i v případě, že není administrační server v provozu.

j) Logy ze všech koncových bodů musí být viditelné v centrální správě.

k) Automatické a parametricky nastavitelné notifikace a alerty distribuované pomocí emailu, konzoly centrální správy, SNMP a Syslogu v těchto případech:

   a. blížící se expirace licence
   b. možného síťového útoku
   c. virového útoku
   d. připojení nových počítačů
   e. zastaralých virových aktualizací na stanicích
   f. zastaralých virových aktualizací na serverech

l) Možnost centrální aktualizace koncových bodů nejen z pohledu virových databází, ale také klientských programových komponent a vlastního klientského software.

m) Možnost automatizované instalace antiviru na koncových bodech.

n) Centrální konfigurace firewallu a HIPS a jejich pravidel.

o) Lokalizované prostředí administrace (v češtině).

p) Možnost automatické konfigurace firewallu na bázi síťových profilů.

q) Možnost centrálního vytváření pravidel přístupu k USB portům (možnost zakázat nebo omezit přístup neoprávněným USB storage médiím na základě těchto parametrů: ID zařízení, druh média, sériového čísla) pro operační systémy Windows, macOS a Linux.

r) Možnost vytváření pravidel filtrování přístupu na webové stránky na úrovni konkrétní URL- kategorie URL s možností vytvoření skupin URL adres a kategorií.

s) Možnost definice časových úseků platnosti pravidel přístupu k USB a pravidel filtrování přístupu webové stránky.

t) Šifrovaná komunikace mezi koncovými body a centrální správou.

u) Automatická detekce operačního systému na koncových bodech při instalaci antiviru z centrální správy na koncové body.

v) Možnost ručního vynucení komunikace centrální správy s koncovými body.

w) Podpora dvoufaktorového ověření pro přihlášení do administračního rozhraní.

x) Možnost správy dalších bezpečnostních produktů a/nebo modulů v případě rozšíření licence (např. šifrování, cloudový sandboxing apod.).

y) Možnost integrace na SIEM.

z) Ochrana Anti-phishing

aa) Ochrana Prevent-secure-backscatter.

bb) Publikace (synchronizace) lokální karantény.

**4) Kvalitativní (nepovinné) požadavky na centrální správu:**

a) Nezávislost instalace centrálního managementu na nástrojích třetích stran, které by mohly způsobit skryté vícenáklady z pohledu licencí či nároků na údržbu systémů. Typicky nutnost provozu a licencování databázových serverů třetích stran na každé lokalitě atd.

b) Automatická detekce 32bitových a 64bitových systémů během vzdálené instalace (instalační balíček musí sám rozeznat koncový OS).

c) Automatická instalace koncové ochrany na stanici v okamžiku zařazení PC do Active Directory.

d) Možnost provádět veškeré akce na klientu (update, upgrade, scan disku, adresáře, souboru, odstranění škodlivého souboru, odstranění škodlivého kódu ze souboru, obnova souboru z karantény).

e) Možnost dočasného vypnutí vynucování politik administračním serverem (typicky v případě ladění nastavení antiviru a jeho testování); tato možnost musí být vyhrazena pouze pro definované uživatele.

f) Schopnost tvorby reportů a jejich automatizovaná distribuce, možnost opakovaných plánovaných reportů.

**g)** Možnost zabránit uživateli v narušení či znemožnění komunikace mezi počítačem a serverem centrální správy i v případě, kdy má k počítači oprávnění administrátora.

**5) Kvalifikační (povinné) požadavky na ochranu koncových bodů (pracovní stanice):**

a) Nastavitelná úroveň interakce koncové aplikace s uživatelem a možnost tuto interakci zcela potlačit.

b) Aktualizace virových databází bez nutnosti krátkodobé deaktivace antivirového motoru (aktualizace za běhu) s možností vytvoření zálohy aktualizací pro případ nutnosti návratu k předchozí verzi virových signatur a/nebo programových modulů antiviru.

c) Možnost off-line provozu antiviru – aktivace antiviru a aktualizace virových signatur a programových komponent antiviru musí být možná i na počítačích, které nemají přístup do internetu (off-line prostředí).

d) Pro ochranu koncových bodů podpora operačních systémů Microsoft Windows 8, Windows 10 v 32bitovém i 64bitovém režimu pro všechny uvedené verze.

e) Možnost instalovat antivir také na všechny výrobcem podporované operační systémy Windows Server.

f) Možnost kontroly nebo zakázání výměnných médií.

g) Antivirový systém musí obsahovat lokální anti-spamový filtr s úspěšností 98 procent a vyšší.

h) Podpora ochrany na IPv6.

i) Integrovaný firewall s podporou HIPS s možností převzetí již existujících pravidel Windows firewallu.

j) Ochrana proti ransomware, pokročilá kontrola paměti, blokování Exploitů, možnost spuštění služby jádra antiviru v chráněném režimu.

k) Možnost nastavení výjimek z karantény či z přehledu detekcí (souborový systém, HIPS, firewall i další moduly).

l) V případě false-positive detekce možnost nastavení výjimky pro konkrétní hrozbu (hash) bez ohledu na fyzické umístění souboru obsahujícího hrozbu.

m) Antivirový systém musí obsahovat ochranu proti logování kláves a přetečení zásobníku.

n) Rezidentní ochrana s nepřetržitou online kontrolou a ochranou, včetně modulu heuristické analýzy pro detekci nově vzniklých nebezpečí s možností využití strojového učení a lokálního sandboxu.

o) Možnost kontroly počítače při nečinnosti - kontrola počítače se automaticky spustí v případě neaktivity uživatele.

p) Ochrana proti rootkitům a zapojení do botnetu.

q) Podpora clusteru, terminál serverů a virtuálních serverů.

r) Podpora online Cloud reputační technologie.

s) Zabezpečený prohlížeč – ochrana bankovnictví a online plateb, pravidla pro definování chráněných webových stránek.

t) Možnost parametrického spouštění z příkazové řádky, pro tvorbu dávkových souborů a skriptů.

u) Možnost zabránit uživateli přístupu do nastavení antiviru či jeho odinstalaci i v případě, kdy má k počítači oprávnění administrátora.

v) Ochrana proti malware.

w) Rezidentní ochrana poštovních klientů pracujících na protokolech SMTP/POP3/IMAP4/NNTP, včetně modulu heuristické analýzy (detekce SPAMu).

x) Možnost definovat zakázané nebo povolené aplikace (blacklist, whitelist) a omezit jejich spuštění na klientské stanici.

y) Schopnost prohledávat a léčit komprimované soubory a složky (ZIP, RAR, PKZIP, CAB).

z) Ochrana provozu prohlížečů internetu, včetně blokování skriptů a nebezpečného obsahu, s možností blokování Adware, spyware, dialers. Možnost definovat nepovolené zdroje (http, http, ftp, atd.)

aa) Rezidentní scan provozu sítě na všech NIC s analýzou veškerého síťového provozu a detekcí výskytu škodlivého obsahu.

bb) Automatické aktualizace virové databáze i programu s možností nastavení periody kontrol dostupných aktualizací.

cc) Existence tzv. karantény (oblast kam sem ukládají odstraněné soubory), s možností obnovy souboru a automatickou kontrolou souborů v karanténě po aktualizaci virové databáze.

**6) Kvalitativní (nepovinné) požadavky na ochranu koncových bodů (pracovní stanice)**

a) Možnost definovat vlastní škodlivé aplikace.

b) Certifikace ICSA a pravidelná účast v testech Virus Buletin, AV-Comparatives.

c) Integrace do operačního systému, podpora Windows exploreru, kontextové menu pro vyvolání akce.

d) Detekce falešných poplachů (detekce SPAMů v emailové schránce zobrazujících se jako legitimní).

**7) Kvalifikační (povinné) požadavky na ochranu mobilních zařízení:**

a) Operační systém Android verze 5 a vyšší.

b) Antivirová ochrana v reálném čase.

c) Automatické aktualizace virových databází.

d) Kontrola při spuštění.

e) Podpora AntiTheft funkcí (vzdálené uzamčení, smazání, nalezení) včetně SMS příkazů a důvěryhodných SIM karet.

f) Blokování hovorů a nežádoucích SMS zpráv.

g) Ochrana před odinstalací.

h) Lokalizované prostředí (v češtině).

i) Ověřování souborů pomocí online reputace.

j) Možnost vynutit politiky pro správu zařízení (MDM) s OS Android (v 5 a vyšší) a iOS.

k) Správa instalovaných aplikací – definice pravidel pro kategorie aplikací nebo konkrétní aplikace.

l) Ochrana mobilních zařízení musí být kompletně spravována z centrální správy stejné jako u stanic.

m) Možnost vynucení politiky zámku obrazovky.

n) Možnost monitorování nastavení zařízení (stav GPS, stav připojení WiFi, stav šifrování apod.).

o) Možnost nastavení restrikcí uživatele (blokování instalace či odinstalace aplikací, blokování resetu zařízení do továrního nastavení, blokování konfigurace síťových připojení apod.).

**8) Požadavky implementaci:**

Součástí dodávky antivirového systému bude jeho instalace a implementace v místě plnění zahrnující minimálně:

a) Instalace a konfigurace serverové části – centrální správy.

b) Nastavení centrální správy (včetně pravidel a politik pro všechna koncová zařízení, reporting, alerting).

c) Odinstalace stávající antivirové ochrany ze všech zařízení.

d) Instalace nové antivirové ochrany na všechna koncová zařízení.

e) Vypracování a dodání podrobné technické dokumentace podle skutečného nasazení pro administrátory antivirového systému v elektronické podobě (ve formátu MS Office 2013 a vyšší), která musí obsahovat minimálně administrátorskou příručku a kompletní popis konfigurace a nastavení (technická dokumentace se po předání zadavateli stává jeho majetkem a může s ní nakládat dle svých potřeb).

f) Školení zaměstnanců zadavatele.

    a. Uchazeč zajistí školení zaměstnanců zadavatele z odboru IT na veškerý software dodaný v rámci této veřejné zakázky.

    b. Školení musí probíhat v místě plnění VZ a v rozsahu potřebném pro provoz a údržbu antivirového systému a všech jeho součástí (ukázka, popis, nastavení a vysvětlení jednotlivých součástí systému) minimálně v rozsahu 8 hodin.

    c. Školení se zúčastní max. 5 administrátorů (k dispozici je školící místnost s prezentační technikou v místě plnění).