Załącznik nr 1 do Zapytania ofertowego/
Załącznik nr 1 do Umowy nr CeZ/…/2023

Opis Przedmiotu Zamówienia

1. Przedmiotem zamówienia jest dostawa 1000 szt. licencji na oprogramowanie **ESET PROTECT Advanced ON-PREM** lub dostawa licencji na oprogramowanie równoważne.
2. Oznaczenie przedmiotu zamówienia wg Kod CPV:

   48760000-3 Pakiety oprogramowania do ochrony antywirusowej

   48000000-8 Pakiety oprogramowania i systemy informatyczne

   72611000-6 Usługi w zakresie wsparcia technicznego
3. Zamawiający posiada licencje ESET PROTECT Advanced ON-PREM:
   3.1. Liczba chronionych stacji roboczych, urządzeń mobilnych i serwerów: 1000 szt.
   3.2. Licencja ważna do: **2023-04-11**.
4. Licencje na oprogramowanie zabezpieczające przed złośliwym oprogramowaniem, zostaną dostarczone w terminie 3 dni roboczych od daty zawarcia umowy.
5. Licencja na Oprogramowanie zostanie udzielona w terminie 3 dni roboczych od dnia podpisania Umowy, nie wcześniej niż 2023-04-11, na 24 miesiące.
6. Wykonawca dostarczy dokumenty licencyjne, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do Oprogramowania na adres e-mail: administrator@cez.gov.pl.
7. Udzielona na oprogramowanie licencja musi umożliwiać co najmniej:
   7.1. Dostęp do subskrypcji aktualnych baz sygnatur.
   7.2. Dostęp do najnowszej wersji oprogramowania.
   7.3. Wsparcia technicznego producenta lub dystrybutora oprogramowania.
8. Parametry i funkcjonalności dostarczonego oprogramowania, nie mogą być gorsze niż wskazane poniżej:
   8.1. System musi zapewniać ochronę antywirusową:
      a) serwera plików,
      b) stacji roboczych,
      c) urządzeń przenośnych (smartfony, tablety).
   8.2. Dla stacji roboczych system musi zapewniać ponadto: ochronę dostępu do sieci (firewall), zapewniać kontrolę podłączanych urządzeń (np. pamięci USB, zewnętrzne napędy, itp.).
   8.3. Konfiguracja, nadzór nad pracą poszczególnych modułów oraz instalacja musi być wykonywana z centralnej konsoli zarządzającej (Zamawiający posiada już konsolę do zarządzania dla oprogramowania ESET PROTECT Advanced ON-PREM).
   8.4. Wsparcie techniczne musi odbywać się w języku polskim przez cały czas trwania umowy w trybie zgłoszeniowym w Dni Robocze (tj. od poniedziałku do piątku z wyłączeniem sobót, świąt i dni wolnych od pracy) na adres e-mail w godzinach od 8.00 do 16.00.
   8.5. Zamawiający wymaga rozwiązania zgłoszonego problemu dotyczącego eksploatacji oprogramowania w ciągu 5 Dni Roboczych.
   8.6. Moduł ochrony antywirusowej i antispyware musi poprawnie współpracować z następującymi systemami operacyjnymi wykorzystywanymi przez Zamawiającego: Microsoft Windows (10 lub wyższą), Microsoft Windows Server (2008 R2 lub wyższą), Linux Debian, RedHat, CentOS i MAC OS (10.13 lub wyższa) .

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

8.7. Moduł ochrony stacji roboczych musi posiadać polskojęzyczny interfejs.

8.8. Moduł antywirusowej i antispyware powinien zapewniać ochronę przed wszystkimi rodzajami wirusów, trojanów, narzędzi hackerskich, oprogramowania typu spyware i adware, rootkit, auto-dialerami i innymi potencjalnie niebezpiecznymi programami.

8.9. Moduł ochrony antywirusowej.

8.9.1. Ochrona antywirusowa musi być realizowana na podstawie:

a) sygnatur,
b) heurystyki (z możliwością jej wyłączenia),
c) na bieżąco weryfikowanej informacji o nowych zagrożeniach w bazie producenta dostępnej przez Internet.

8.9.2. Moduł musi mieć możliwość określenia listy reguł wykluczeń dla wybranych obiektów, rodzajów zagrożeń oraz składników ochrony.

8.9.3. Moduł musi umożliwiać skanowanie antywirusowe w chwili dostępu (real time), na żądanie i według harmonogramu z następującymi warunkami:

a) skanowanie na żądanie i wg harmonogramu musi mieć możliwość przerwania w dowolnym momencie,
b) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy na baterii,
c) skanowanie na żądanie musi mieć możliwość wstrzymania w przypadku wykrycia pracy w trybie pełnoekranowym (np. prezentacja).

8.9.4. Moduł musi wykrywać zagrożenia: na dyskach, w plikach w tym archiwach plikowych, na stronach web, w przesyłkach email w tym w załącznikach, na podłączanych nośnikach przenośnych.

8.9.5. Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołów POP3, SMTP, IMAP w czasie rzeczywistym niezależnie od klienta pocztowego.

8.9.6. Moduł musi zapewniać ochronę komunikacji przy wykorzystaniu protokołu HTTP w czasie rzeczywistym niezależnie od przeglądarki.

8.9.7. Moduł musi zawierać warstwę ochronną przeglądarki działającą na stacjach użytkowników i ostrzegające ich o złośliwej zawartości strony internetowej wraz z możliwością aktywnego blokowania dostępu do wybranych stron internetowych, określonych centralnie przez administratora systemu. Rozwiązanie musi realizować także możliwość określenia blokowanych stron web na podstawie kategorii strony (np. pornografia, strony społecznościowe, itp.).

8.9.8. Moduł musi umożliwiać ustawienia priorytetu procesu skanowania.

8.9.9. Aktualizacja wzorców wirusów musi odbywać się co najmniej raz dziennie.

8.9.10. Moduł musi umożliwiać aktualizację wzorców wirusów z archiwum internetowego lub z centralnego punktu dystrybucji wzorców wirusów.

8.9.11. Moduł musi umożliwiać pobieranie aktualizacji za pośrednictwem serwera Proxy.

8.9.12. Po wykryciu zagrożenia musi istnieć możliwość oczyszczenia zainfekowanego pliku a jeśli nie jest to możliwe – usunięcia bądź umieszczenia go w lokalnej kwarantannie.

8.9.13. W przypadku zainstalowania na urządzeniach przenośnych musi nastąpić automatyczna zmiana punktu dystrybucji wzorców na archiwum internetowe bez konieczności ingerencji użytkownika.

8.9.14. Moduł musi umożliwiać konfigurowanie dostępności i zakresu ingerencji użytkownika w proces skanowania.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

8.9.15. Moduł musi umożliwiać zabezpieczanie hasłem przed zmianą konfiguracji, deinstalacją i zatrzymaniem programu.
8.9.16. Moduł musi wymuszać odświeżanie wzorców wirusów.
8.9.17. Moduł musi mieć możliwość instalacji oprogramowania klienckiego przy pomocy systemu SCCM.
8.9.18. Uaktualnienia oprogramowania (silnik) musi być dostępne przez cały okres trwania abonamentu bazy wzorców wirusów (trwania umowy).

9. Moduł firewall.
   9.1. Zapora osobista musi umożliwiać:
      a) tworzenie reguł monitorowania aktywności sieciowej dla wszystkich zainstalowanych aplikacji w oparciu o charakterystyki pakietów sieciowych,
      b) tworzenie nowych zestawów warunków i działań wykonywanych na pakietach sieciowych oraz strumieniach danych dla określonych protokołów, portów i adresów IP,
      c) pracę w trybie stanowym (stateful) dla aplikacji i procesów systemu operacyjnego,
      d) blokowanie określonych portów sieciowych,
      e) pracę firewall w trybie nauki,
      f) tworzenie reguł firewalla działających w zależności od rodzaju połączenia (sieć firmowa, sieć publiczna),
      g) blokowanie połączeń do innych sieci (np. przez WiFi) w czasie, kiedy stacja jest podłączona do sieci firmowej,
      h) ciągłe aktualizowanie danych o reputacji adresów IP, do których/z których jest nawiązywane połączenie ze stacji oraz blokowanie połączeń związanych z wysokim ryzykiem. Informacja o reputacji musi być dostępna na bieżąco przez Internet z bazy danych prowadzonej przez producenta rozwiązania.
   9.2. Moduł musi umożliwiać tworzenie list sieci zaufanych.
   9.3. Moduł musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
   9.4. Moduł musi mieć wbudowany system IDS/IPS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
   9.5. Moduł musi mieć możliwość wykrywania zmian w aplikacjach korzystających z sieci i informowanie o tym zdarzeniu.
   9.6. Program musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
   9.7. Moduł musi umożliwiać tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci, w tym:
      a) musi istnieć możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci,
      b) musi być możliwość automatycznego przełączania profili, bez ingerencji użytkownika lub administratora.
   9.8. Autoryzacja stref musi odbywać się co najmniej w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowanie sieci bezprzewodowej lub jego braku, aktywność połączenia bezprzewodowego lub jego braku, aktywność wyłącznie jednego połączenia sieciowego lub wielu połączeń sieciowych, konkretny interfejs sieciowy w systemie.
10. Moduł ochrony urządzeń mobilnych

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

10.1. Ochronę urządzeń pracujących pod kontrolą wykorzystywanych przez Zamawiającego systemów Android oraz Apple iOS.
10.2. Ochronę plików w czasie rzeczywistym.
10.3. Skanowanie plików systemowych, bibliotek, plików archiwum oraz innych.
10.4. Skanowanie dostępnego w urządzeniu nośnika pamięci SD.
10.5. Ochronę proaktywną wykrywającą nieznane zagrożenia.
10.6. Określenie poziomu głębokości skanowania plików archiwum.
10.7. Określenie domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia: przeniesienia do kwarantanny, usunięcia lub zignorowania.
10.8. W przypadku wykrycia zagrożenia użytkownik musi otrzymać powiadomienie.
10.9. Włączenie blokady urządzenia mobilnego na hasło alfanumeryczne o zadanej złożoności: np. minimum 8 znaków składających się z liter małych i dużych, oraz cyfr i znaków specjalnych.
10.10. Ustalenie czasu po którym włącza się blokada urządzenia (np. blokada ekranu po 5 minutach nieaktywności użytkownika).
10.11. Pamięć historii haseł blokady urządzenia, wykluczająca możliwość użycia co najmniej 5 ostatnich haseł.
10.12. Możliwość wykrywania ingerencji w oryginalne oprogramowanie urządzenia.
10.13. Możliwość blokowania aplikacji po jej nazwie.

11. Centralna konsola zarządzająca.
11.1. Konfiguracja, nadzór nad pracą poszczególnych modułów musi być wykonywana z centralnej konsoli zarządzającej. Zamawiający posiada już centralną konsolę zarządzającą.
11.2. Wykonawca dokona konfiguracji centralnej konsoli zarządzającej w celu uruchomienia połączenia pomiędzy urządzeniem komórkowym - oprogramowaniem (zainstalowanym na urządzeniu przenośnym), a centralą przez serwer PROXY (zamawiający nie posiada skonfigurowanego serwera PROXY zlokalizowanego w strefie DMZ), który zostanie skonfigurowany przez Wykonawcę.
11.3. Zamawiający dostarczy maszynę wirtualną wraz z oprogramowaniem Windows lub Linux.
11.4. Moduł musi zapewnić centralną instalację programów służących do ochrony stacji roboczych Windows oraz urządzeń mobilnych na OS Android.
11.5. Moduł musi zapewnić centralne zarządzanie wszystkimi programami służącymi do ochrony: stacji roboczych, serwerów plików, serwerów pocztowych, serwerów portalu wielofunkcyjnego, aplikacji mobilnych.
11.6. Moduł musi posiadać centralną bazę przechowującą informacje o konfiguracji stacji i urządzeń końcowych.
11.7. Moduł musi posiadać centralną bazę przechowującą informacje o zdarzeniach i wykrytych zagrożeniach.
11.8. Centralna konsola zarządzająca musi umożliwić zdalną instalację produktów na komputerach z domeny Microsoft Active Directory objętych ochroną, bez konieczności stosowania dodatkowych narzędzi i oprogramowania, z możliwością zaplanowania z wyprzedzeniem momentu wykonania instalacji dla poszczególnych komputerów i grup komputerów.
11.9. Oferowane rozwiązania musi umożliwiać selektywne wskazanie, który z produktów ochronnych wchodzących w skład systemu zostanie wdrożony na którym z komputerów – nie jest dopuszczalne wdrożenie pakietu w postaci jednej paczki instalacyjnej obejmującej kilka produktów na raz.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

11.10. Moduł musi mieć możliwość definiowania komputerów, które mają być objęte wdrożeniem poszczególnych produktów i polityk. Musi być możliwe tworzenie grup statycznych i dynamicznych niezależnie parametrów komputera.
11.11. Moduł nie musi zawierać dodatkowego agenta do centralnej instalacji i zarządzania.
11.12. Moduł musi szyfrować komunikację między serwerem a klientami.
11.13. Moduł musi zapewnić centralną konfigurację i zarządzanie ochroną antywirusową, antyspyware'ową, zaporą osobistą i kontrolą dostępu do stron internetowych zainstalowanymi na stacjach roboczych w sieci.
11.14. Moduł musi być wyposażony w kreator konfiguracji zapory osobistej stacji klienckich pracujących w sieci, umożliwiający podgląd i utworzenie globalnych reguł na podstawie dowolnych już istniejących reguł.
11.15. Moduł musi mieć możliwość uruchomienia centralnego skanowania wybranych stacji roboczych z opcją wygenerowania raportu ze skanowania i przesłania do konsoli zarządzającej.
11.16. Moduł musi mieć możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania skanera na żądanie i skanerów rezydentnych).
11.17. Moduł musi mieć możliwość sprawdzenia z centralnej konsoli zarządzającej podstawowych informacji dotyczących stacji roboczej: adresów IP, adresów MAC, wersji systemu operacyjnego oraz domeny, do której dana stacja robocza należy.
11.18. Moduł musi umożliwiać centralną aktualizację stacji roboczych z serwera w sieci lokalnej lub z Internetu.
11.19. Moduł musi mieć możliwość utworzenia centralnego punktu dystrybucji wzorców wirusów.
11.20. Moduł musi mieć możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
11.21. Moduł musi mieć możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
11.22. Moduł musi mieć możliwość importowania konfiguracji programu z wybranej stacji roboczej a następnie przesłanie (skopiowanie) jej na inną stację lub grupę stacji roboczych w sieci.
11.23. Moduł musi mieć możliwość zmiany konfiguracji na stacjach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko, jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło zabezpieczające ustawienia konfiguracyjne).
11.24. Moduł musi mieć możliwość uruchomienia serwera centralnej administracji i konsoli zarządzającej na wykorzystywanych przez Zamawiającego stacjach z systemem Windows.
11.25. Centralna konsola zarządzająca musi posiadać możliwość powiadamiania o wszystkich zdarzeniach za pomocą poczty elektronicznej, wiadomości SNMP i syslog lub wywołania komendy/skryptu.
11.26. Centralna konsola zarządzająca musi mieć możliwość integracji z Active Directory zarówno w rozumieniu powielenia struktury komputerów jak i autentykacji administratorów i dynamicznego przypisywania uprawnień w serwerze zarządzającym w zależności od przynależności do odpowiedniej grupy w Active Directory.
11.27. Centralna konsola zarządzająca musi umożliwiać zdefiniowanie wielu kont administratorów i przydzielenie im szczegółowych ról umożliwiających co najmniej:

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

ograniczenie dostępu do wskazanych grup maszyn, ograniczenie administracji do poszczególnych produktów i ich specyficznych funkcji.

12. Opis równoważności.
    12.1. Zamawiający dopuszcza możliwość dostawy rozwiązania równoważnego do opisanych w pkt. 8-12.
    12.2. Za rozwiązanie równoważne Zamawiający uzna rozwiązanie spełniające wymagania opisane w pkt. 8-12 oraz poniższe wymagania:
        12.2.1. Dostawę oprogramowania o funkcjonalności nie gorszej od posiadanych przez Zamawiającego.
        12.2.2. Zapewnienie usługi kompletnej nieinwazyjnej deinstalacji dotychczasowego oprogramowania antywirusowego i oprogramowania antyspamowego z całej infrastruktury informatycznej (komputerów, serwerów i urządzeń mobilnych) Zamawiającego.
        12.2.3. Zapewnienie usługi kompletnej nieinwazyjnej instalacji i konfiguracji nowego rozwiązania w infrastrukturze informatycznej Zamawiającego.
        12.2.4. Zapewnienia dodatkowego wsparcia technicznego (zdalnego oraz, w razie potrzeby, bezpośredniego – realizowanego w siedzibie Zamawiającego) przez Wykonawcę przez okres miesiąca od daty wdrożenia produkcyjnego rozwiązania równoważnego.
        12.2.5. Przeszkolenie 5 pracowników Zamawiającego z zakresu obsługi, konfiguracji i administracji całości rozwiązania równoważnego.
        12.2.6. Wdrożenie, szkolenie, asysta techniczna i dodatkowe wsparcie techniczne Wykonawcy – w języku polskim w siedzibie Zamawiającego.
        12.2.7. Usługi wdrożeniowe równoważnego oprogramowania antywirusowego i oprogramowania antyspamowego zostaną zrealizowane przez Wykonawcę nie później niż w terminie wygaśnięcia posiadanych przez Zamawiającego licencji.
    12.3. Oprogramowanie nie może naruszać bezpieczeństwa publicznego lub istotnego interesu bezpieczeństwa państwa, mając na względzie m.in. fakt, że Zamawiający zgodnie z art. 4 pkt. 7 Ustawy o Krajowym systemie cyberbezpieczeństwa (tj. Dz. U z 2018r. poz. 1560), dalej: „Ustawa”, należy do Krajowego systemu cyberbezpieczeństwa, którego celem jest zgodnie z art. 3 Ustawy, zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym zapewnienie niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów. Tym samym, Oprogramowanie musi być zgodne z celem Krajowego systemu cyberbezpieczeństwa i przepisami Ustawy oraz nie zagrażać cyberbezpieczeństwu, bezpieczeństwu publicznemu lub istotnemu interesowi bezpieczeństwa państwa.
    12.4. Warunki licencjonowania mają umożliwiać Zamawiającemu (Licencjobiorcy) objęcie dostarczonym oprogramowaniem stacji roboczych należących do podmiotów administracji publicznej, na warunkach zdefiniowanych w dokumencie OPZ.
    12.5. Dostarczana licencja Oprogramowania musi pochodzić z autoryzowanego przez producenta kanału dystrybucji. Wykonawca jest zobowiązany dostarczyć Zamawiającemu dowody poświadczające autentyczność zakupionych licencji na zasadach określonych przez producenta wraz z dostawą Oprogramowania.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706