

## Rozdział II SWZ - OPIS PRZEDMIOTU ZAMÓWIENIA

### 1. Nazwa zamówienia

**Dostawa licencji na oprogramowanie antywirusowe.**

### 2. Oznaczenie przedmiotu zamówienia wg kodów CPV:

48760000-3 Pakiety oprogramowania do ochrony antywirusowej

72611000-6 Usługi w zakresie wsparcia technicznego

### 3. Termin dostawy licencji

Dostawa licencji na Oprogramowanie ma nastąpić w terminie do 3 dni roboczych od dnia zawarcia umowy<sup>1</sup> z zastrzeżeniem, że dostarczone licencje mogą zostać aktywowane nie wcześniej niż dnia 01.07.2021 r. (data aktywacji). Jeśli dostawa Oprogramowania z licencjami nastąpi po tej dacie dostarczone licencje będą aktywowane w dniu dostawy Oprogramowania z licencjami.

### 4. Przedmiot zamówienia

4.1. Przedmiot zamówienia obejmuje dostawę licencji na oprogramowanie antywirusowe, zwanego dalej „**Oprogramowaniem**” na okres 36 miesięcy od daty aktywacji dla 8604 użytkowników (w tym maksymalnie 2868 serwerów).

4.2. Wykonawca w terminie wskazanym w punkcie 3 dostarczy dokumenty licencyjne umożliwiające korzystanie z Oprogramowania w okresie wskazanym w pkt 4.1 powyżej. m.in. certyfikat, warunki licencjonowania oraz klucze licencyjne i instrukcje instalacji do Oprogramowania na adres e-mail wskazany w umowie lub do siedziby Zamawiającego.

4.3. Wykonawca dostarczy Oprogramowanie o parametrach i funkcjonalnościach nie gorszych niż poniżej:

4.3.1. musi umożliwiać automatyczną (zdalną) instalację na stacjach klienckich, bez dostępu do Internetu;

4.3.2. musi umożliwiać automatyczną dystrybucję bazy sygnatur wirusów i aktualizacji komponentów programu w sieci wydzielonej, bez dostępu do Internetu (funkcjonalność serwera kopii dystrybucyjnej);

4.3.3. musi posiadać wbudowane narzędzie do analizy i gromadzenia wszystkich ważnych informacji o danym komputerze, bez konieczności korzystania z żadnych zewnętrznych stron internetowych, w szczególności o następujących funkcjonalnościach:

- 1) możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach;
- 2) konsola zarządzająca zapewniająca automatyczną synchronizację z Active Directory;
- 3) możliwość automatycznego wykrywania i usuwania innego oprogramowania antywirusowego podczas instalacji;
- 4) możliwość ukrycia interfejsu przed użytkownikiem końcowym;
- 5) posiadać kwarantannę dla programów szpiegujących (spyware oraz riskware);
- 6) możliwość stworzenia pliku diagnostycznego do analizy problemów;

<sup>1</sup> Termin stanowi kryterium oceny ofert

- 7) możliwość wysłania próbki wirusa bezpośrednio do laboratorium antywirusowego producenta;
  - 8) posiadać narzędzie ręcznej aktualizacji stacji roboczych we wszystkich sygnaturach dla poszczególnych silników skanujących;
  - 9) automatyczne powiadamianie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem, czy stacja robocza jest odpowiednio zabezpieczona;
- 4.3.4. musi posiadać wbudowany moduł heurystyczny;
  - 4.3.5. musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika;
  - 4.3.6. musi być wyposażony w system zapobiegania włamaniom działający na hoście zapewniający pracę z regułami, gdzie aplikacja automatycznie tworzy i wykorzystuje reguły; tworzenie reguł musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego;
  - 4.3.7. musi umożliwiać całkowitą, niekolidującą z pracą systemu operacyjnego i automatyczną deinstalację Oprogramowania na stacji klienckiej;
  - 4.3.8. do instalacji serwera centralnej administracji nie może być wymagane zainstalowanie żadnych dodatkowych płatnych silników baz danych; serwer centralnej administracji musi mieć własną wbudowaną bazę;
  - 4.3.9. Wykonawca dostarczy licencję na system operacyjny umożliwiający zainstalowanie i korzystanie z serwera centralnej administracji,
  - 4.3.10. serwer centralnej administracji musi oferować administratorowi możliwość współpracy przynajmniej z jednym z wymienionych zewnętrznych silników baz danych: Microsoft SQL Server, MySQL Server;
  - 4.3.11. Oprogramowanie musi umożliwiać instalację i poprawne funkcjonowanie klienta AV na następujących systemach operacyjnych: Windows 7 i nowsze, Windows Server 2008R2 i nowsze, Linux.
- 4.4. Wraz z dostawą Oprogramowania z licencjami Wykonawca zobowiązuje się do:
- 4.4.1. dostarczenia instrukcji konfiguracji serwera aktualizacji w ramach zasobów Zamawiającego;
  - 4.4.2. dostarczenia instrukcji instalacji Oprogramowania na serwerze aktualizacji;
  - 4.4.3. dostarczenia instrukcji konfiguracji Oprogramowania;
  - 4.4.4. dostarczenia instrukcji generowania pakietów instalacyjnych na stacje robocze użytkowników końcowych;
  - 4.4.5. dostarczenia dokumentacji eksploatacyjnej obejmującej instrukcje związane z administracją i eksploatacją rozwiązania, procedury awaryjne i testowe;
  - 4.4.6. dostarczenia instrukcji instalacji pakietów na stacjach roboczych przez użytkowników;
  - 4.4.7. przeszkolenia dwóch administratorów.
- 4.5. Szkolenie dla administratorów przy oferowaniu oprogramowania o którym mowa w pkt. 4.3 powyżej, musi spełniać następujące wymagania:
- 4.5.1. być przeprowadzone przez certyfikowanego trenera oferowanego Oprogramowania;
  - 4.5.2. obejmować zakresem:
    - 1) konfigurowanie i administrowanie od strony klienta;

- 2) konfigurowanie i administrowanie od strony konsoli zarządzającej Oprogramowaniem;
- 4.5.3. odbyć się online w terminie uzgodnionym z Zamawiającym jednak nie później niż w ciągu 5 dni roboczych od dostawy Oprogramowania z licencjami .
5. 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 z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (tj. Dz. U. z 2020 r. poz. 1369 z późn. zm.), 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.
  6. Warunki licencjonowania mają umożliwiać Zamawiającemu (Licencjobiorcy) na objęcie dostarczonym Oprogramowaniem stacji roboczych należących do podmiotów administracji publicznej na warunkach zdefiniowanych w dokumencie OPZ.
  7. Zamawiający zastrzega, że niniejszy przedmiot zamówienia jest przeznaczony do dalszej odsprzedaży. Wszelkie dokumenty licencyjne, itp. muszą być wystawione na docelowego użytkownika jakim będzie Skarb Państwa reprezentowany przez Ministra Cyfryzacji lub inny organ pełniący funkcję organu założycielskiego lub nadzorującego wobec Zamawiającego lub następcą prawny Ministra Cyfryzacji.
  8. 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.
  9. Pozostałe warunki realizacji zamówienia zawarte są w Rozdziale III SWZ – Projektowane postanowienia umowy.