Opis Przedmiotu Zamówienia

na dostawę licencji oprogramowania do tworzenia i obróbki dokumentów w formacie zgodnym ze standardem ISO 32000-2:2020 oraz licencji oprogramowania antywirusowego

Część nr 2 – dostawa licencji oprogramowania antywirusowego

Przedmiot zamówienia:

Przedmiotem zamówienia jest oprogramowanie antywirusowe – 200 licencji na okres 24 miesięcy na stacje robocze i urządzenia mobilne – telefon komórkowy (Android, iOS) wraz z konsolą centralnego zarządzania oprogramowaniem AV.

Zastosowanie:

Ochrona stacji roboczych i urządzeń mobilnych – zarządzanie oprogramowaniem z poziomu pojedynczej, centralnej konsoli.

Lp.	Atrybut	Parametr wymagany
1.	Typ produktu	Oprogramowanie ochrony antywirusowej
2.	Producent	Wykonawca w ofercie zobowiązany jest do podania nazwy produktu oraz producenta
3.	Wymagania systemów operacyjnych dla ochrony stacji roboczych	Microsoft Windows 10 i 11
4.	Wymagania dla telefonów komórkowych	Android iOS
5.	Wymagania systemów operacyjnych (Konsola zarządzająca w przypadku instalacji lokalnej)	Możliwość instalacji na serwerach z systemem. operacyjnym: Windows Serwer 2019 Linux CentOS 7-8
6.	Język interfejsu	Polski lub angielski
7.	Czas reakcji producenta na nowe wirusy	Maksymalnie 24 godziny przez cały rok (24/7/365)
8.	Sposoby monitorowania i ochrony	- monitorowanie systemu operacyjnego (non stop) - monitorowanie ruchu http - skanowanie nośników - skanowanie heurystyczne - ochrona anty-ransomware - monitorowanie poczty elektronicznej (bez agentów) - wykrywanie oprogramowania typu: spyware, adware, keylogger, trojan itp.
9.	Aktualizowanie baz wirusowych	- Oprogramowanie musi umożliwiać automatyczne i na żądanie aktualizowanie baz z serwerów producenta za pośrednictwem Internetu dostępnych 24h/dobę, - Aktualizowanie bez potrzeby zatrzymywania mechanizmu skanującego i bez konieczności restartu aktualizowanych systemów.

10.	Metody skanowania	- Skanowanie wg ustalonego harmonogramu czasowego, - Skanowanie ręczne na żądanie z komputera lokalnego oraz z centralnej konsoli zarządzania, - Skanowanie wielu komputerów wywoływane z poziomu konsoli zarządzania,
11.	Kwarantanna	- Centralnie zarządzana z możliwością przeprowadzania operacji na elementach zgromadzonych w odizolowanej przestrzeni stacji roboczych, - Umożliwiająca izolację podejrzanych plików typu „spyware", „adware", „keylogger", „trojan"
12.	Obsługa plików skompresowanych	Wymagane co najmniej: ZIP, RAR, JAR, ARJ, TAR, LZH, TGZ, GZ, CAB, BZ2
13.	Wymagane akcje i reakcje systemu na incydenty zagrożenia bezpieczeństwa.	- Automatyczne usuwanie wykrytych wirusów, - Automatyczne uruchamianie procedur naprawczych, - Automatyczne powiadomienia o wykrytych zagrożeniach użytkownika stacji i administratora systemu AV, - Automatyczne informowanie o stanie ochrony stacji roboczej, - Logowanie incydentów oraz historii akcji w pliku lub bazie loga z możliwością podglądu przez administratora systemu.
14.	Wymagane reakcje blokady	- Blokowanie plików pobieranych przez protokół http o określonych przez administratora rozszerzeniach, nazwach, zawartości, - Blokowanie zawartości stron WWW w zakresie ochrony przeglądarki, kodu infekującego, wyskakujących okienek pop-up, cookies, pobieranie zainfekowanych plików, analizy skryptów. - Możliwość kontroli dopuszczania i blokowania dowolnych aplikacji, - Blokowanie ruchu do serwerów DNS określonych jako niezaufane albo podejrzane z możliwością zmiany klasyfikacji przez administratora lub dodania strony do „zaufanych".
15.	Kontrola sesji	Zabezpieczenie połączenia do dowolnych witryn https klasyfikowanych przez administratora i/lub producenta oprogramowania poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów w czasie aktywnego połączenia z taką stroną.
16.	Kontrola urządzeń	Możliwość blokowania oraz dopuszczania z poziomu konsoli zarządzającej dostępu na stacjach roboczych do urządzeń zewnętrznych np. urządzenia bluetooth, czytniki kart pamięci, napędy USB, CD/DVD
17.	Funkcjonalności konsoli administracyjnej	- Pełna administracja konfiguracją i monitorowanie stacji roboczych w tym: centralna instalacja, konfiguracja, zarządzanie, raportowanie i administrowanie oprogramowaniem. - Centralne blokowanie i odblokowywanie dostępu dla użytkownika do zmian konfiguracji oprogramowania klienckiego, - Możliwość zdalnego zarządzania wszystkimi ustawieniami oprogramowania klienckiego, - Możliwość tworzenia grup klientów, w celu zarządzania oraz wymuszania określonych zasad bezpieczeństwa, - Możliwość zaimportowania struktury drzewa domeny z Microsoft Active Directory, - Możliwość tworzenia reguł powiadamiania o nowych, niezarządzanych stacjach roboczych w domenie Microsoft Active Directory,

		- Możliwość blokowania wszystkich ustawień konfiguracyjnych stacji roboczych w celu uniemożliwienia ich modyfikacji przez użytkowników, - Możliwość włączania oraz wyłączania widoczności komunikatów o znalezionych zagrożeniach na wybranych lub wszystkich stacjach klienckich, - Automatyczne uaktualnianie bazy definicji wirusów oraz mechanizmów skanujących w interwałach co najmniej dobowych, - Automatyczne pobieranie zaktualizowanych definicji wirusów, jeśli aktualnie przechowywane pliki są przestarzałe, - Konsola musi umożliwiać wybór reakcji administratora w przypadku wykrycia wirusa (kwarantanna, usunięcie itp.), - Konsola powinna posiadać system raportowania dostępny przez przeglądarkę internetową, w tym podgląd statystyk aktywności i działania oprogramowania oraz statystyk monitorowanych stacji klienckich, - System raportowania musi umożliwiać wysyłanie raportów poprzez pocztę elektroniczną zgodnie z harmonogramem określonym przez administratora oraz wykonanie powiadomienia co najmniej przez SNMP, zapis loga do dziennika systemowego, zapis loga do systemu centralnego zarządzania.
18.	**Uwaga**	W odniesieniu do oprogramowania antywirusowego Kaspersky Lab Ministerstwo Obrony Narodowej RP, odnosząc się do stanowiska Stanów Zjednoczonych i Narodowego Centrum Cyberbezpieczeństwa Wielkiej Brytanii, zarekomendowało zaprzestanie używania ww. oprogramowania. https://www.gov.pl/web/cyfryzacja/interpelacja-w-sprawie-stosowania-programu-antywirusowego-kaspersky-przez-jednostki-administracji-publicznej Mając na uwadze powyższe rekomendacje Zamawiający (Agencja Badań Medycznych) nie dopuszcza zaoferowania ww. oprogramowania i jego pochodnych. **W przypadku zaoferowania takiego oprogramowania oferta Wykonawcy zostanie odrzucona.**
19.	Zakładka „Pomoc” (centrum pomocy)	Dostępna z poziomu aplikacji zakładka „Pomoc” umożliwiająca dostęp do - pomocy programu, - informacji o programie.

Lp.	Atrybut	Parametr stanowiący kryterium oceny ofert
1.	Komunikacja zarządzania za pomocą konsoli	Wymagane zarządzanie za pomocą przeglądarki WWW Komunikacja zarządzania z konsoli Dopuszczalny protokół: http (nieszyfrowany) Preferowany protokół : https (szyfrowany)
2.	Aktualizacje oprogramowania firm trzecich	Agentowy lub bezagentowy moduł lub silnik aktualizatora aplikacji, umożliwiającego aktualizację aplikacji firm trzecich do najnowszych wersji. – zaoferowanie modułu/silnika jest preferowane, ale jego niezaoferowanie jest dopuszczalne.
3.	Ilość licencji i możliwość ich płynnego przenoszenia	Wymagana ilość licencji przewidziana dla postępowania to: Stacje robocze (komputer): 120 Urządzenia mobilne (telefon komórkowy): 80 Dodatkowo Zamawiający premiuje punktowo rozwiązanie umożliwiające przenoszalność licencji pomiędzy stacjami

		roboczymi (komputerem) a urządzaniami mobilnymi i odwrotnie.

Na przedmiot zamówienia Wykonawca musi udzielić gwarancji na co najmniej 24 miesiące od daty odbioru przedmiotu Zamówienia.

Oferowany przedmiot dostawy musi obejmować wyspecyfikowane elementy, które będą kompletne i po uruchomieniu będą gotowe do pracy zgodnie z przeznaczeniem bez żadnych dodatkowych zakupów inwestycyjnych.