Załącznik nr 2 do postępowania,
znak sprawy: **WOD.042.1.10.2022**

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

1. Zakup i dostawa komputerów typu laptop wraz z oprogramowaniem w ramach Konkursu Grantowego Cyfrowa Gmina -Wsparcie dzieci z rodzin pegeerowskich w rozwoju cyfrowym –„Granty PPGR" Oś V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia Program Operacyjny Polska Cyfrowa na lata 2014 – 2020"
2. Sprzęt zaproponowany przez Wykonawcę musi być fabrycznie nowy i wolny od obciążeń prawami osób trzecich; posiadać dołączone niezbędne instrukcje i materiały dotyczące użytkowania, w języku polskim. Sprzęt powinien posiadać wszelkie certyfikaty i dopuszczenia. Zaproponowany sprzęt musi być kompletny, posiadać kable, podzespoły. Gotowy do uruchomienia i użytkowania bez dodatkowych zakupów. Sprzęt musi być dopuszczony do obrotu i stosowania w krajach UE. Do wszystkich ujętych w zamówieniu systemów operacyjnych i licencji zalecane jest dołączenie nośników, a także instrukcji instalacji i obsługi oraz certyfikatów potwierdzających prawo Zamawiającego do korzystania z Oprogramowania w ramach niniejszego zamówienia. Wykonawca powinien być uprawniony do wprowadzenia do obrotu oprogramowania dostarczonego wraz z licencją na korzystanie z niego.
3. Wszystkie parametry wskazane w Opisie Przedmiotu Zamówienia są parametrami minimalnymi lub równoważnymi.
4. Komputer przenośny będzie wykorzystywany dla potrzeb aplikacji biurowych, aplikacji edukacyjnych, dostępu do Internetu oraz poczty elektronicznej.
5. W przypadku wystąpienia wątpliwości co do legalności systemu będzie przeprowadzana weryfikacja oryginalności dostarczonych programów komputerowych u Producenta oprogramowania

1. Laptop – 7 szt.

Opis minimalnych wymaganych parametrów sprzętu	
Matryca	Komputer przenośny typu notebook z ekranem 15,6" o rozdzielczości min. FHD z podświetleniem LED, matryca matowa
Procesor	Procesor osiągający wynik min. 6274 punktów w teście według Passmark - Average CPU Mark https://www.cpubenchmark.net , architektura 64-bitowa. **Potwierdzeniem spełnienia powyższych wymagań będzie dołączony do oferty wydruk raportu**
Pamięć RAM	Min. 8GB z możliwością rozbudowy
Pamięć masowa	min. 256GB SSD
Karta graficzna	Zintegrowana z procesorem.
Multimedia	wbudowane głośniki stereo, cyfrowy mikrofon wbudowany w obudowę matrycy. Kamera internetowa o rozdzielczości min. HD, trwale zainstalowana w obudowie matrycy.
Bateria i zasilanie	Bateria min. 40 Wh,
BIOS	BIOS zgodny ze specyfikacją UEFI, Funkcja blokowania/odblokowania portów USB
Bezpieczeństwo	System diagnostyczny z graficzny interfejsem dostępny z poziomu BIOS lub menu BOOT'owania. Pełna funkcjonalność systemu diagnostycznego musi być dostępna również w przypadku braku lub uszkodzenia oraz sformatowania dysku twardego. Dedykowany układ szyfrujący TPM 2.0
Certyfikaty	Certyfikat ISO 9001 dla producenta sprzętu , Deklaracja zgodności CE
Waga	Waga komputera z oferowaną baterią nie większa niż 1,77kg

System operacyjny	1. Licencja na system operacyjny Microsoft Windows 10 Professional 64bit PL z możliwością bezpłatnego upgrade'u do najnowszej dostępnej wersji lub równoważny (opis równoważności znajduje się poniżej) 2. Zamawiający nie dopuszcza urządzeń z wersją edukacyjną Windows. 3. Dostarczone przez Wykonawcę licencje muszą pochodzić z legalnych źródeł oraz zostać dostarczone Zamawiającemu ze wszystkimi składnikami niezbędnymi do potwierdzenia legalności ich pochodzenia (np.: certyfikat autentyczności, kod aktywacyjny wraz z instrukcją aktywacji jeśli takowy nie jest zapisany w BIOS'ie itp.). 4. System operacyjny musi być zainstalowany przez producenta oprogramowania. 5. Fabrycznie nowy system operacyjny, nieużywanego oraz nieaktywowanego nigdy wcześniej na innym urządzeniu. 6. Warunki równoważności - oprogramowanie typu Microsoft Windows 10 Professional 64bit PL w najnowszej dostępnej wersji lub równoważne, spełniające łącznie poniższe warunki: 1) System operacyjny dla komputerów przenośnych, z graficznym interfejsem użytkownika. 2) System operacyjny ma pozwalać na instalację, uruchomienie i pracę z aplikacjami MS Office 2016, 2019, 365. Nie jest dopuszczalne uruchamianie wymienionych aplikacji poprzez mechanizm wirtualizacji. 3) System ma udostępniać dwa rodzaje graficznego interfejsu użytkownika: a. Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b. Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych. 4) Interfejsy użytkownika dostępne w wielu językach do wyboru – w tym polskim i angielskim. 5) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, odtwarzacz multimediów, pomoc, komunikaty systemowe. 6) Wbudowany system pomocy w języku polskim. 7) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim. 8) Możliwość dokonywania bezpłatnych aktualizacji i poprawek w ramach wersji systemu operacyjnego poprzez Internet, mechanizmem udostępnianym przez producenta systemu z możliwością wyboru instalowanych poprawek oraz mechanizmem sprawdzającym, które z poprawek są potrzebne. 9) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora. 10) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 11) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6.
Wymagania dodatkowe	Wbudowane porty i złącza- wymagane min: HDMI, RJ-45 (1 Gb/s), USB co najmniej 3 szt., czytnik kart SD, złącze słuchawkowe stereo/ mikrofonowe, zintegrowana karta sieci WiFi, moduł bluetooth. Klawiatura (układ US-QWERTY) z wydzieloną klawiaturą numeryczną, touchpad z strefą przewijania.
Warunki gwarancji	3-letnia gwarancja producenta.
Akcesoria	Torba do laptopa, mysz.

2. Oprogramowanie antywirusowe – 7 szt.

Pełne wsparcie dla systemu Windows: 11,10, 8.x, 7, Vista, Server 2016, Server 2012, Server 2008, 2003 Server.
Wsparcie dla systemów XP SP3 32-bit, Linux 32/64-bit, OS X (tylko klient).
Interfejsy programu, pomoce i podręczniki w języku polskim.
Pomoc techniczna w języku polskim.

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych programów: adware, spyware, scareware, phishing, hacktools
3. Wbudowana technologia do ochrony przed rootkitami wykrywająca aktywne i nieaktywne rootkity.
4. Klient oprogramowania antywirusowego dla stacji roboczych z systemami Linux.
5. Klient oprogramowania antywirusowego dla linuksowych serwerów Samba.
6. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
7. 2 niezależne skanery antywirusowe (nie heurystyczne!) z 2 niezależnymi bazami sygnatur wirusów wykorzystywane przez skaner dostępowy, skaner na żądanie oraz skaner poczty elektronicznej.
8. Możliwość konfiguracji programu do pracy z jednym skanerem i dwoma skanerami antywirusowymi jednocześnie.
9. Dodatkowy i niezależny od skanerów plików, trzeci skaner poczty oparty o technologię cloud security.
10. Możliwość wykluczenia ze skanowania skanera dostępowego: napędów, katalogów, plików lub procesów.
11. Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików na żądanie lub według harmonogramu.
12. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rodzaj plików do skanowania, priorytet skanowania).
13. Skanowanie na żądanie pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
14. Technologia zapobiegająca powtórnemu skanowaniu sprawdzonych już plików, przy czym maksymalny czas od ostatniego sprawdzenia pliku nie może być dłuższy niż 4 tygodnie, niezależnie od tego czy plik był modyfikowany czy nie.
15. Możliwość określania poziomu obciążenia procesora podczas skanowania na żądanie i według harmonogramu.
16. Możliwość skanowania dysków sieciowych i dysków przenośnych.
17. Rozpoznawanie i skanowanie wszystkich znanych formatów kompresji.
18. Możliwość definiowania listy procesów, plików, folderów i napędów pomijanych przez skaner dostępowy.
19. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
20. Skanowanie i oczyszczanie poczty przychodzącej POP3 w czasie rzeczywistym, zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
21. Automatyczna integracja skanera POP3 z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
22. Możliwość definiowania różnych portów dla POP3, SMTP i IMAP na których ma odbywać się skanowanie.
23. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
24. Dodatek do aplikacji MS Outlook umożliwiający podejmowanie działań związanych z ochroną z poziomu programu pocztowego.
25. Dodatek do aplikacji MS Outlook umożliwia ponowne skanowanie wszystkich nieprzeczytanych wiadomość znajdujących się w skrzynce
26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany a użytkownikowi wyświetlane jest stosowne powiadomienie.
27. Dedykowany moduł chroniący przeglądarki przed szkodnikami atakującymi sesje z bankami i sklepami online.
28. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
29. Możliwość definiowania różnych portów dla HTTP, na których ma odbywać się skanowanie.
30. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
31. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń powinny być w pełni anonimowe.
32. Możliwość automatycznego wysyłania powiadomienia o wykrytych zagrożeniach do dowolnej stacji roboczej w sieci lokalnej.
33. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e mail.
34. Możliwość zabezpieczenia hasłem dostępu do opcji konfiguracyjnych programu.

35. Aktualizacja dostępna z bezpośrednio Internetu lub offline – z pliku pobranego zewnętrznie.
36. Obsługa pobierania aktualizacji za pośrednictwem serwera proxy.
37. Możliwość określenia częstotliwości aktualizacji w odstępach 1 godzinowych.
38. Możliwość samodzielnej aktualizacji sygnatur wirusów ze stacji roboczej (np. komputery mobilne).
39. Program wyposażony w tylko w jeden serwer skanujący uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, skaner HTTP).
40. Możliwość ukrycia programu na stacji roboczej przed użytkownikiem.
41. Kontrola zachowania aplikacji (Behaviour Blocking) do wykrywania podejrzanie zachowujących się aplikacji.
42. Skanowanie w trybie bezczynności - pełne skanowanie komputera przynajmniej raz na 2 tygodnie uruchamiane i wznawiane automatycznie, podczas gdy nie jest on używany.
43. Ochrona przed urządzeniami podszywającymi się po klawiatury USB.
44. Moduł do ochrony przed exploitami (ataki 0-day).

1. Integracja z Active Directory – import kont komputerów i jednostek organizacyjnych.
2. Ochrona dla urządzeń z systemem Android.
3. Zarządzanie urządzeniami z systemem iOS.
4. Opcja automatycznej instalacji oprogramowania klienckiego na wszystkich podłączonych komputerach Active Directory.
5. Zdalna instalacja i centralne zarządzanie klientami na stacjach roboczych i serwerach Windows.
6. Zdalna instalacja i centralne zarządzanie klientami Linux / OS X.
7. Do instalacji zdalnej i zarządzania zdalnego nie jest wymagany dodatkowy agent. Na końcówkach zainstalowany jest sam program antywirusowy.
8. Możliwość zarządzania ochroną urządzeń mobilnych z poziomu konsoli (przynajmniej aktualizacje, ochronę przeglądarek, skanowania zasobów, synchronizacji raportów).
9. Możliwość kontekstowego zastosowania ustawień danej stacji dla całej grupy.
10. Możliwość eksportu/importu ustawień dla stacji/grupy stacji. 11. Możliwość zarządzania dowolną ilością serwerów zarządzających z jednego okna konsoli.
11. Możliwość zarządzania różnymi wersjami licencyjnymi oprogramowania producenta z jednego okna konsoli.
12. Możliwość tworzenia hierarchicznej struktury serwerów zarządzających (serwer główny i serwery podrzędne).
13. Możliwość zainstalowania zapasowego serwera zarządzającego, przejmującego automatycznie funkcje serwera głównego w przypadku awarii lub odłączenia serwera głównego.
14. Możliwość zdalnego zarządzania serwerem spoza sieci lokalnej przy pomocy połączenia VPN.
15. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez przeglądarki internetowe (z sieci lokalnej i spoza niej).
16. Możliwość zdalnego zarządzania serwerem centralnego zarządzania przez urządzenia mobilne (smartfony, tablety) oparte o system Android (z sieci lokalnej i spoza niej).
17. Szyfrowanie komunikacji między serwerem zarządzającym a klientami.
18. Możliwość uruchomienia zdalnego skanowania wybranych stacji roboczych.
19. Możliwość sprawdzenia z centralnej konsoli zarządzającej stanu ochrony stacji roboczej (aktualnych ustawień programu, wersji programu i bazy wirusów, wyników skanowania).
20. Możliwość przeglądania list programów zainstalowanych na stacjach/serwerach (nazwa, wersja, producent, data instalacji).
21. Możliwość stworzenia białej i czarnej listy oprogramowania, i późniejsze filtrowanie w poszukiwaniu stacji je posiadających.
22. Odczyt informacji o zasobach sprzętowych stacji (procesor i jego taktowanie, ilość pamięci RAM i ilość miejsca na dysku/partycji systemowej).
23. Możliwość centralnej aktualizacji stacji roboczych z serwera w sieci lokalnej lub Internetu.
24. Możliwość skanowania sieci z centralnego serwera zarządzającego w poszukiwaniu niezabezpieczonych stacji roboczych.
25. Możliwość tworzenia grup stacji roboczych i definiowania w ramach grupy wspólnych ustawień konfiguracyjnymi dla zarządzanych programów.
26. Możliwość zmiany konfiguracji na stacjach i serwerach z centralnej konsoli zarządzającej lub lokalnie (lokalnie tylko jeżeli ustawienia programu nie są zabezpieczone hasłem lub użytkownik/administrator zna hasło

zabezpieczające ustawienia konfiguracyjne). 27. Możliwość generowania raportów w formacie XML. 28. Możliwość przeglądania statystyk ochrony antywirusowej w postaci tekstu lub wykresów. 29. Możliwość przesłania komunikatu, który wyświetli się na ekranie wybranej stacji roboczej lub grupie stacji roboczych. 30. Komunikat można wysłać do wszystkich lub tylko wskazanego użytkownika stacji roboczej. 31. Możliwość zminimalizowania obciążenia serwera poprzez ograniczenie ilości jednoczesnych procesów synchronizacji, aktualizacji i przesyłania plików do stacji roboczych. 32. Możliwość dynamicznego grupowania stacji na podstawie parametrów: nazwa komputera, adres IP, brama domyślna, nazwa domeny.
Możliwość utworzenia raportów statusu ochrony sieci. Możliwość generowania raportów w przynajmniej 3 językach. Możliwość wysyłania raportów z określonym interwałem.
Licencja na 3 lata

WÓJT
Marcin Zawadka

GŁÓWNY SPECJALISTA DS. INFORMATYKI
Ewa Woźniak