Karpacka Państwowa Uczelnia w Krośnie

Załącznik Nr 3 do SWZ
w postępowaniu
znak: DTG/144/ZP-9/22

Opis przedmiotu zamówienia w postępowaniu na „dostawę oprogramowania”

Część I – Oprogramowanie 1

Legenda:

1. Oferowany przedmiot zamówienia musi być zgodny z opisem.
2. Parametry minimalne są warunkami granicznymi tzn. niespełnienie któregokolwiek z wymienionych parametrów, będzie skutkowało odrzuceniem oferty.
3. Jeżeli w opisie przedmiotu zamówienia wskazane zostały znaki towarowe, lub pochodzenie, a przy tym znaku towarowym znajduje się dopisek *„lub równoważne”,* Zamawiający może zaoferować rozwiązania równoważne do podanych przez Zamawiającego.
4. Kryteria stosowane w celu oceny równoważności: Wykonawca który oferuje rozwiązania równoważne ma obowiązek wykorzystać wszelkie dostępne mu środki w celu wykazania, iż oferowane przez niego rozwiązanie jest równoważne. Wówczas obowiązkiem wykonawcy jest podanie opisu rozwiązania równoważnego. Opis ten musi być na tyle szczegółowy, żeby zamawiający przy ocenie ofert mógł ocenić czy zaproponowane rozwiązania równoważne spełniają jego wymagania i będą należycie spełniały cel postępowania. Opis rozwiązania równoważnego należy podać w niniejszym załączniku i powinien być tak szczegółowy, żeby zamawiający w toku badania ofert mógł stwierdzić, czy zaproponowane rozwiązanie spełnia wymagania zamawiającego.

Wymagane parametry techniczno-użytkowe (minimalne):

Wszystkie licencje muszą być rejestrowane na dane zamawiającego (adres siedziby, e-mail aktywacja@kpu.krosno.pl).

L.p.	Oprogramowanie o następujących funkcjach lub równoważne:				
1. Oprogramowanie – 20 szt.		VAT	Cena netto	Wartość netto (cena netto x ilość)	Wartość brutto (wartość netto + VAT)
Oferowane oprogramowanie (pełna nazwa):		23 %			
1.1	Oprogramowanie graficzne, wyposażone w zaawansowane narzędzia do tworzenia ilustracji, układu stron, edycji zdjęć. Oprogramowanie umożliwiające projektowanie logotypów, broszur, materiałów sprzedażowych, marketingowych, szkoleniowych, plakatów i innych rodzajów prac. Pakiet oprogramowania: - do projektowania grafiki wektorowej - do edycji zdjęć – do przekształcania map bitowych w edytowalne grafiki wektorowe - do przechwytywania obrazów z ekranu komputera Aplikacje pomocnicze: – pozwalające na szybkie edytowanie zdjęć w formacie RAW (wersja angielska) – umożliwiające animowanie zdjęć (wersja angielska) Wersja językowa: polska Obszar zastosowań: edukacyjna, prowadzenie zajęć z zakresu grafii komputerowej Okres licencji: bezterminowa Platforma: na komputery stacjonarne PC. Najnowsza aktualna wersja oferowana przez producenta oprogramowania z dnia składania oferty.				

2. Oprogramowanie – 16 szt.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa): ..... Opis rozwiązania równoważnego (jeśli Wykonawca oferuje rozwiązanie równoważne): …… …… ……		23 %			
2.1	Subskrypcja na 12 miesięcy. Oprogramowanie pod nazwą "Adobe Photoshop CC" lub równoważne (najnowsza aktualna wersja oferowana przez producenta systemu z dnia składania oferty). Platforma: na komputery stacjonarne PC i MAC. Subskrypcja na użytkownika Wersja oprogramowania przeznaczona do prowadzenia zajęć dydaktycznych. Wersja wielojęzykowa/polska. Początek obowiązywania subskrypcji wrzesień 2022 r.				
3. Oprogramowanie – 16 szt.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa): ..... Opis rozwiązania równoważnego (jeśli Wykonawca oferuje rozwiązanie równoważne): …… …… ……		23 %			
3.1	Subskrypcja na 12 miesięcy. Oprogramowanie pod nazwą "Illustrator CC" lub równoważne (najnowsza aktualna wersja oferowana przez producenta systemu z dnia składania oferty). Platforma: na komputery stacjonarne PC i MAC. Subskrypcja na użytkownika Wersja oprogramowania przeznaczona do prowadzenia zajęć dydaktycznych. Wersja wielojęzykowa. Początek obowiązywania subskrypcji wrzesień 2022 r.				
4. Oprogramowanie – 1 szt.		VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):		23 %			
4.1	Subskrypcja na 12 miesięcy. Platforma: na komputery stacjonarne PC. Subskrypcja na użytkownika Wersja wielojęzykowa. Początek obowiązywania subskrypcji wrzesień 2022 r. Oprogramowanie do remapowania samochodów. Identyfikacja i indeksacja tabel kalibracyjnych jednostek sterujących silnika (ECU) i jednostek sterujących skrzyń biegów (TCU). Moduły do usuwania DTC, sum kontrolnych, natychmiastowych rozwiązań i automatycznego rozpoznawania map. Możliwość usuwania lub modyfikowania krzywych ECU i TCU. Wizualizację map 2D i 3D. Automatycznie wykrywanie mapy elektroniki pojazdu (Bosch, Siemens, Delphi, Temic, Luca, Visteon, Motorola itp.)				
5. Oprogramowanie – 1 szt.		VAT	Cena netto	Wartość netto	Wartość brutto

Oferowane oprogramowanie (pełna nazwa): ..... Opis rozwiązania równoważnego (jeśli Wykonawca oferuje rozwiązanie równoważne): …… …… ……	23 %			

5.1	Subskrypcja na 12 miesięcy. Oprogramowanie pod nazwą "TurboMAP" lub równoważne (najnowsza aktualna wersja oferowana przez producenta systemu z dnia składania oferty). Platforma na komputery stacjonarne PC Subskrypcja na użytkownika Początek obowiązywania subskrypcji wrzesień 2022 r.

6. Oprogramowanie – 25 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

6.1	Subskrypcja na 12 miesięcy. Wymagania dotyczące oprogramowania antywirusowego dla systemów typu Windows serwer: 1. Ochrona serwerów: a. Microsoft Windows Server 2008 R2 b. Microsoft Small Business Server 2011, Standard edition c. Microsoft Small Business Server 2011, Essentials d. Microsoft Windows Server 2012 e. Microsoft Windows Server 2012 Essentials f. Microsoft Windows Server 2012 R2 g. Microsoft Windows Server 2012 R2 Essentials h. Microsoft Windows Server 2012 R2 Foundation i. Microsoft Windows Server 2016 Standard j. Microsoft Windows Server 2016 Essentials k. Microsoft Windows Server 2016 Datacenter l. Microsoft Windows Server 2016 Core m. Microsoft Windows Server 2019 Standard n. Microsoft Windows Server 2019 Essentials o. Microsoft Windows Server 2019 Datacenter p. Microsoft Windows Server 2019 Core 2. Ochrona całego systemu monitorowana i zarządzana z pojedynczej konsoli. 3. Zarządzanie aplikacją poprzez interfejs dostępny przez protokół https. 4. Możliwość określenia adresów sieciowych, z których można zarządzać aplikacją. 5. Możliwość określenia portu, na którym dostępny będzie interfejs zarządzający aplikacją. 6. Integracja z systemem antywirusowym dla serwerów MS Exchange dostarczanym przez producenta poprzez wspólny lokalny interfejs zarządzający. 7. Co najmniej trzy różne silniki antywirusowe, każdy z dedykowanymi bazami sygnatur, funkcjonujące jednocześnie i skanujące wszystkie dane. 8. Zintegrowany silnik „antyrootkitowy”. 9. Co najmniej dwa dedykowane silniki „antyspyware”. 10. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie plików i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu. 11. Możliwość wywołania skanowania na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta. 12. Możliwość wywołania skanowania w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera. 13. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.

	14. Możliwość wywołania szybkiego skanowania pod kątem programów typu rootkit. 15. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie operacyjnym. 16. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów. 17. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe. 18. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów. 19. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „wirus", „keylogger", „dialer", „trojan". 20. Program powinien posiadać kwarantannę wirusów, spyware oraz riskware. 21. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona. 22. Mikrodefinicje wirusów – przyrostowe (inkrementalne) pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji). 23. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty, w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2. 24. Automatyczne usuwanie wirusów i zgłaszanie alertów w przypadku wykrycia wirusa. 25. Automatyczne uruchamianie procedur naprawczych. 26. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione. 27. Gwarancja na dostarczenie szczepionki na nowego wirusa w czasie krótszym niż 48 godzin. 28. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365). 29. Automatyczne powiadomienie użytkowników oraz administratora o pojawiających się zagrożeniach wraz z określeniem stacja robocza jest odpowiednio zabezpieczona. 30. Możliwość zarządzania za pomocą centralnej konsoli 31. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich. 32. Aktualizator aplikacji powinien spełniać role programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji. 33. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej. 34. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów. 35. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV. 36. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji. 37. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 38. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces

7. Oprogramowanie – 790 szt.	VAT	Cena netto	Wartość netto	Wartość brutto
Oferowane oprogramowanie (pełna nazwa):	23 %			

7.1	Subskrypcja na 12 miesięcy. Wymagania dotyczące system ochrony anty wirusowej z zaporą ogniową dla stacji roboczych. 1. Ochrona antywirusowa stacji roboczych: - Microsoft Windows 7 (32-bit i 64-bit) - Microsoft Windows 8.1 (32-bit i 64-bit)

- Microsoft Windows 10 (32-bit i 64-bit)

2. Ochrona antywirusowa wyżej wymienionego systemu monitorowana i zarządzana z pojedynczej, centralnej konsoli.

3. Możliwość instalacji konsoli zarządzania niezależnie na kilku wybranych stacjach.

4. Polski interfejs użytkownika aplikacji ochronnej.

Wymagania dotyczące technologii:

1. Ochrona antywirusowa realizowana na wielu poziomach, tj.: monitora kontrolującego system w tle, modułu skanowania heurystycznego, modułu skanującego nośniki i monitora poczty elektronicznej, monitora ruchu http oraz moduł antyrootkitowy.

2. Co najmniej trzy różne silniki antywirusowe, funkcjonujące jednocześnie i skanujące wszystkie dane.

3. Oddzielny silnik skanujący do wykrywania niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan".

4. Aktualizacje baz definicji wirusów dostępne 24h na dobę na serwerze internetowym producenta, możliwa zarówno aktualizacja automatyczna programu oraz na żądanie, jak i ściągnięcie pliku offline ze strony producenta i ręczna aktualizacja na stacjach roboczych bez dostępu do Internetu.

5. Możliwość wywołania skanowania komputera na żądanie lub według harmonogramu ustalonego przez administratorów dla określonych grup klientów za pomocą centralnej konsoli lub lokalnie przez określonego klienta.

6. Możliwość wywołania skanowania komputera w określone dni i godziny tygodnia i miesiąca, a także po określonym czasie bezczynności komputera.

7. Możliwość wywołania skanowania podczas uruchamiania systemu operacyjnego lub po zalogowaniu użytkownika.

8. Aktualizacja definicji wirusów czy też mechanizmów skanujących nie wymaga zatrzymania procesu skanowania na jakimkolwiek systemie.

9. Mikrodefinicje wirusów – przyrostowe (inkrementalne) - pobieranie jedynie nowych definicji wirusów i mechanizmów skanujących bez konieczności pobierania całej bazy (na stację kliencką pobierane są tylko definicje, które przybyły od momentu ostatniej aktualizacji).

10. Możliwość pobierania aktualizacji definicji wirusów bezpośrednio z serwerów producenta, centralnej konsoli, dedykowanego proxy lub z innej stacji roboczej gdzie zainstalowane jest oprogramowanie antywirusowe.

11. Brak konieczności restartu systemu operacyjnego po dokonaniu aktualizacji mechanizmów skanujących i definicji wirusów.

12. Heurystyczna technologia do wykrywania nowych, nieznanych wirusów.

13. Wykrywanie niepożądanych aplikacji takich jak oprogramowanie typu „spyware", „adware", „keylogger", „dialer", „trojan", „rootkit".

14. Możliwość umieszczenia oprogramowania typu „spyware", „adware", „keylogger", „dialer", „trojan" w kwarantannie.

15. Ochrona pliku 'hosts' przed niepożądanymi wpisami.

16. Mechanizm centralnego zarządzania elementami kwarantanny znajdującymi się na stacjach klienckich.

17. Mechanizm skanujący wspólny dla wszystkich platform sprzętowych i programowych, wszystkich maszyn, wszystkich wersji oprogramowania, w tym bez względu na wersję językową oprogramowania – bez względu na to jak duża jest sieć lub jak bardzo jest złożona.

18. Mechanizm określania źródeł ataków prowadzonych przy użyciu zagrożeń hybrydowych, takich jak Code Red i Nimda.

19. Obsługa plików skompresowanych obejmująca najpopularniejsze formaty w tym, co najmniej: ZIP JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2 HQX.

20. Automatyczne usuwanie wirusów oraz oprogramowania typu malware i zgłaszanie alertów w przypadku wykrycia wirusa.

21. Logowanie historii akcji podejmowanych wobec wykrytych zagrożeń na stacjach roboczych. Dostęp do logów z poziomu GUI aplikacji.

22. Automatyczne uruchamianie procedur naprawczych.

23. Uaktualnienia definicji wirusów posiadają podpis cyfrowy, którego sprawdzenie gwarantuje, że pliki te nie zostały zmienione.

24. Średni czas reakcji producenta na nowy wirus poniżej 8 godzin, 24 godziny na dobę przez cały rok (24/7/365).

25. Automatyczne powiadomienie użytkowników oraz administratora o wykrytych zagrożeniach wraz z określeniem czy stacja robocza jest odpowiednio zabezpieczona.

26. Możliwość zablokowania wychodzącej wiadomości e-mail, jeżeli zostanie w niej wykryty zainfekowany załącznik.

27. Skanowanie przez program na komputerze klienckim, danych pobieranych i wysyłanych danych przy pomocy protokołu http.

28. Blokowanie przez program na komputerze klienckim określonego przez administratora rodzaju zawartości oraz nazwy lub rozszerzeń poszczególnych plików pobieranych przy pomocy protokołu http.

29. Skanowanie http oraz blokowanie zawartości może być deaktywowane dla witryn określonych, jako zaufane przez serwery reputacyjne producenta.

30. Automatyczna kwarantanna blokująca ruch przychodzący i wychodzący, włączająca się w momencie, gdy stacja robocza posiada stare sygnatury antywirusowe.

31. Wsparcie dla technologii Microsoft Network Access Protection (NAP).

32. Ochrona przeglądarki internetowej, w tym: blokowanie wyskakujących okienek, blokowanie ciasteczek (cookies), blokowanie możliwości zmian ustawień w IE, analiza uruchamianych skryptów ActiveX i pobieranych plików.

33. Ochrona podczas przeglądania sieci Internet na podstawie badania reputacji – moduł działający na bazie Network Interceptor Framework (niezależnie od rodzaju i wersji przeglądarki).

34. Możliwość zabezpieczenia połączenia do witryn skategoryzowanych przez producenta, jako ‘bankowość elektroniczna’ poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z bankiem.

35. Kontrola połączenia umożliwia zabezpieczenie sesji do dowolnej witryny HTTPS wskazanej przez administratora poprzez uniemożliwienie nawiązania nowych sesji do niezaufanych hostów na czas połączenia z daną witryną HTTPS.

36. Możliwość ręcznego aktualizowania baz definicji wirusów poprzez odrębny plik wykonywalny dostarczony przez producenta.

37. Ochrona rejestrów systemowych, w tym odpowiedzialnych za konfigurację przeglądarki Internet Explorer, listę uruchamianych aplikacji przy starcie, przypisania rozszerzeń plików do zadanych aplikacji.

38. Kontrola oraz możliwość blokowania aplikacji próbujących uzyskać połączenie z Internetem lub siecią lokalną.

39. Osobista zapora ogniowa (tzw. personal firewall) z możliwością definiowania profili bezpieczeństwa możliwych do przypisania dla pojedynczej stacji roboczej lub grup roboczych.

40. Profile bezpieczeństwa zapory ogniowej zawierają predefiniowane reguły zezwalające na bezproblemową komunikację w sieci lokalnej.

41. Możliwość automatycznego przełączenia profilu bezpieczeństwa zapory ogniowej po spełnieniu określonych warunków (np. zmiana adresacji karty sieciowej na stacji roboczej)

42. Blokowanie dostępu do witryn WWW na podstawie dostarczonych przez producenta kategorii bez konieczności ręcznego wpisywanie poszczególnych adresów.

43. Użytkownik podczas próby przejścia na witrynę znajdująca się w zablokowanej przez Administratora kategorii musi zostać powiadomiony o nałożonej na niego blokadzie komunikatem w przeglądarce internetowej.

44. Możliwość blokowania witryn na podstawie kategorii zarówno dla protokołu HTTP jak i HTTPS.

45. Brak konieczności restartu komputera po zainstalowaniu aplikacji w środowisku Windows

46. Moduł kontroli urządzeń zapewniający możliwość zezwolenia lub zablokowania dostępu do urządzeń zewnętrznych (np. napędy USB, urządzenia bluetooth, czytniki kart pamięci, napędy CD/DVD, stacje dyskietek).

47. Moduł kontroli urządzeń zarządzany z poziomu konsoli centralnego zarządzania.

48. Moduł kontroli urządzeń umożliwia dodanie ‘zaufanego urządzenia’ poprzez podanie jego identyfikatora sprzętowego.

49. Moduł aktualizatora aplikacji, który okresowo skanuje i umożliwia aktualizację do najnowszych wersji aplikacji firm trzecich.

50. Aktualizator aplikacji powinien spełniać role programu łatającego podatności a nie tylko i wyłącznie pasywnego skanera luk w bezpieczeństwie aplikacji.

51. Administrator ma możliwość wykluczenia aplikacji, które maja nie podlegać aktualizacji poprzez wpisanie nazwy aplikacji na listę wykluczeń w konsoli zarządzającej.

52. System raportowania powinien pokazywać status podatności aplikacji na komputerach dotyczące całej domeny lub pojedynczych komputerów.

53. Aktualizator aplikacji nie może wymagać instalowania dodatkowych agentów oprócz agenta AV.

54. Aktualizator powinien dać możliwość aktualizacji poprawek w sposób akcji wymuszonej lub reguły wykonującej się w sposób zaplanowany: dzień, godzina, opcje restartu komputera, wykluczenia aplikacji.

	55. Administrator konsoli zarządzającej powinien mieć możliwości zapoznania się z opisem danej podatności aplikacji uruchamiając aktywny link z konsoli zarządzającej z przekierowaniem na strony producenta aplikacji. 56. Aktualizator aplikacji nie wymaga uprawnień administratora lokalnego do instalacji poprawek i jest realizowany, jako dedykowany proces.

....., dnia .....

(miejscowość)

.....

podpis osoby uprawnionej

do reprezentowania Wykonawcy