KW.PF.042.8.2023.97

Starachowice, 28.02.2024 r.

ZAPROSZENIE DO SKŁADANIA OFERT
(zamówienie którego wartość nie przekracza wyrażonej w złotych równowartości kwoty 30.000 euro)

na „zakup i dostawę wyposażenia do Centrum Kreatywności Pałacyk – etap 2 część 2 – podcastownia" w ramach projektu pn. „Kierunek Przyszłość – Starachowicki Program Rozwoju Lokalnego", finansowanego z Norweskiego Mechanizmu Finansowego na lata 2014-2021 (85%) oraz budżetu państwa (15%) w ramach Programu Rozwój Lokalny.

ZAMAWIAJĄCY
Gmina Starachowice, ul. Radomska 45, 27-200 Starachowice
NIP: 664-19-09-150
REGON: 291009892
Strona www: www.starachowice.eu
tel.: 41 273-82-52

1. Informacje wprowadzające:

1. Celem zapytania jest wyłonienie Wykonawcy, który przedstawi najkorzystniejsze, w rozumieniu postanowień niniejszego zapytania ofertowego, warunki zakupu i dostawy wyposażenia do Centrum Kreatywności Pałacyk – etap 2 część 2 w ramach projektu „Kierunek Przyszłość – Starachowicki Program Rozwoju Lokalnego" w zakresie szczegółowo określonym poniżej.
2. Niniejsze postępowanie realizowane jest w związku z zasadą konkurencyjności.
3. Zamawiający nie dopuszcza składania ofert wariantowych.
4. Zamawiający nie dopuszcza składania ofert częściowych.
5. Zakup wyposażenia dotyczy Nowe Skrzydła budynku Centrum Kreatywności Pałacyk. Zakup jest jednym z elementów projektu „Kierunek Przyszłość – Starachowicki Program Rozwoju Lokalnego".
6. Użyte w zapytaniu terminy i skróty mają następujące znaczenie:
   a. „Postępowanie" – postępowanie prowadzone przez „Zamawiającego" na podstawie niniejszego zapytania.
   b. „Zamówienie" – zamówienie, którego przedmiot został w sposób szczegółowy opisany w punkcie II niniejszego zapytania.

c. „Wykonawca” – osoba fizyczna lub firma, która ubiega się o wykonanie zamówienia, złoży ofertę na jego wykonanie albo zawrze z Zamawiającym umowę w sprawie wykonania zamówienia.

2. Zakres rzeczowy zamówienia:

Słownik CPV:

32341000-5 – Mikrofony
32342400-6 – Sprzęt nagłaśniający
32342100-3 – Słuchawki
30237136-1 – Karty dźwiękowe
44112600-4 - Izolacja dźwiękoszczelna
30213000-5 - Komputery osobiste

Lp.	Przedmiot	Opis	J.miary	Liczba
1	POP Filtr Mikrofonowy	– rodzaj: Pop filtr – kompatybilność: uniwersalny – materiał wykonania: metal, tworzywo sztuczne – kolor – czarny – wysokość [mm]:359mm Szerokość [mm]:122Waga [g]:95	szt.	2
2	Mikrofon studyjny	– RODE NT 1000 – wielkomembranowy – Rodzaj: pojemnościowy – Zastosowanie: instrumentalny – Charakterystyka kierunkowa: kardioidalna – Pasmo przenoszenia: 20 Hz - 20 kHz, – Impedancja wyjściowa: 100 Ohm, – Stosunek sygnału do szumu: 88 dB, – Ekwiwalentny poziom szumów: 6 dBA SPL [IEC651, IEC268-15] +/-1 dB, – Maks. SPL: 140 dB [THD 1% dla obciążenia 1 kOhm], – Czułość: -36 dB, 1 V/Pa [16 mV przy 94 dB SPL] +/-1 dB, – Dynamika [DIN IEC651]: 134 dBA [IEC268-15], – kolor złoty	szt.	1

Lp.	Przedmiot	Opis	J.miary	Ilość
3	Wysięgnik mikrofonu BLUE	– Materiał aluminium – Zakres obrotu: 360 stopni; Maksymalny zasięg w poziomie: 81 cm; Gwint standardowo 5/8 cala, z adapterem do 3/8 cala; – maksymalna grubość biurka: 66.675 mm – Uchwyt: zacisk biurkowy – Kolor: czarny	szt.	1
4	Mikser	• Do przesyłania strumieniowego, podcastów, filmów z YouTube, studiów i małych konfiguracji na żywo • min. 9 tłumików • min. 4 inteligentne pokrętła • 6 sampli padów z 4 bankami • kolorowy wyświetlacz dotykowy o przekątnej 10,1 cala • przedwzmacniacze Onyx 80 dB • mix Agent z ustawieniem automatycznego wzmocnienia • możliwość przełączania zasilania phantom +48V • cyfrowe przetwarzanie sygnału: 24-bity / 48 kHz • wielościeżkowe nagrywanie/streaming do podłączonego komputera, karty SD lub pamięci USB (do 14 kanałów, wejścia + podkładki samplera + Bluetooth + miks sumujący; nośniki danych opcjonalne, nie wchodzą w skład zestawu) • kompatybilny z Windows i MacOS • Bluetooth 5.0 (rozmowy można prowadzić poprzez Bluetooth) • 2 stereofoniczny powrót USB • 4 wejścia mikrofonowe/instrumentalne/liniowe: XLR/jack 6,3 mm • 2 wejścia liniowe: gniazdo 6,3 mm • wejście liniowe stereo: minijack 3,5 mm • 2 wyjścia liniowe: jack 6,3 mm • 4 wyjścia słuchawkowe stereo, oddzielnie regulowane • Wymiary (szer. × wys. × gł.): 330 × 104 × 381 mm • lub tożsame	szt.	1

Lp.	Przedmiot	Opis	J.miary	Ilość
5	Słuchawki	• Wokółuszne • Zamknięte • Dynamiczne • Sterownik: 40 mm • Magnesy neodymowe • Maksymalny SPL: 92 dB • Impedancja: 32 Ohm • Zakres częstotliwości: 10 – 30 000 Hz • Prowadzenie kabli z jednej strony • Długość kabla: 2 m • Waga: 323 g • adapter do gniazda stereo 6,3 mm • lub tożsame	szt	2
6	Kabel mikrofonowy XLR - jack	• symetryczny kabel mikrofonowy/sygnałowy wyposażony w żeńskie złącze wtyczkowe XLR i wtyczkę jack stereo 6,3 mm • długość - 5m	szt	2

Lp.	Przedmiot	Opis	J.miary	Ilość
7	Karta dźwiękowa	• maksymalna jakość nagrywania: 24 bity / 96 khz • kapsuła mikrofonowa x/y xyh-6 (w zestawie) • wymienne mikrofony przypinane • kapsuła ambisonic dostępna opcjonalnie (nie wchodzi w skład zestawu) • 4 x wejścia mikrofonowe: xlr • 2 x wejścia mikrofonowe/liniowe/instrumentalne: gniazdo combo xlr/trs • zasilanie phantom dla 6 wewnętrznych wejść xlr: +12v/+24v/+48v • regulacja wzmocnienia i tłumiki -20 db na każdym wejściu • wejścia mikrofonowe/liniowe z możliwością rozbudowy poprzez moduł • port usb (micro b) do użytku jako 12-kanałowy i stereofoniczny interfejs audio dla komputerów pc / mac / ipad • formaty nagrywania wav, bwf i mp3 • obsługuje karty sd / sdhc / sdxc do 512 gb • kolorowy ekran dotykowy lcd 2,4" (320x240) ze zoptymalizowanym interfejsem użytkownika do nagrywania w terenie, nagrań muzycznych i podcastów • wbudowany głośnik • wbudowane efekty i tuner chromatyczny • wyjście liniowe stereo: gniazdo 3,5 mm • wyjście słuchawkowe stereo: jack 3,5 mm • zasilanie: 4x baterie aa (brak w zestawie) lub usb • wymiary h8 bez mikrofonu (szer. x gł. x wys.): 116,4 x 163,3 x 48,6 mm • wymiary xyh-6 (szer. x gł. x wys.): 78,9 x 60,2 x 45,2 mm • waga h8 bez mikrofonu: 354 g • waga xyh-6: 130 g • lub produkt zbliżony	szt.	1
8	Panele akustyczne	– pomieszczenie 8,53 m.kw. – Panele akustyczne samoprzylepne – Długość szerokość: 50 cm na 50 cm – Grubość: 7 cm – Kolor jasnoszary i pomarańczowy – Montaż w cenie	kpl.	1

Lp.	Przedmiot	Opis	J.miary	Ilość
9	Komputer przenośny	Komputer przeznaczony będzie do obróbki materiałów audio-video. Zaproponowany sprzęt musi uwzględniać konieczność zapewnienia odpowiednich warunków pracy podzespołów podczas renderowania filmów (np. odpowiednio dobrane systemy zasilania i chłodzenia). Minimalne parametry sprzętowe: Komputer przenośny: 1. Procesor: 1. architekturze x86_64, wynik min. 13 700 pkt, osiągający w teście https://www.cpubenchmark.net, wynik dla oferowanego procesora musi być opublikowany na stronie https://www.cpubenchmark.net (oferent załączy do oferty wydruk z w/w strony).. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu; 2. min. 8 core/8 wątków 2. pamięć operacyjna: 32 GB;	szt.	1

3. parametry pamięci masowej:
   1. rodzaj pamięci: ssd m.2
   2. pojemność 512 GB
4. Obudowa: komputer powinien być oznaczony niepowtarzalnym numerem seryjnym umieszczonym na obudowie
5. Matryca
   1. Przekątna ekranu min 16”
   2. obsługiwana rozdzielczość: min. 1920x1200 pikseli
6. karta graficzna
   1. pamięć dedykowana min. 2GB
   2. wynik min. 6 000 pkt, osiągający w teście https://www.videocardbenchmark.net, wynik dla oferowanej karty graficznej musi być opublikowany na stronie https://www.videocardbenchmark.net (oferent załączy do oferty wydruk z w/w strony)
7. karta dźwiękowa – zintegorowana
8. komunikacja:
   1. wi-fi 802.11ax – gen.6
   2. bluetooth 5.2
   3. ethernet (zamawiający dopuszcza zastosowanie zewnętrznego modułu usb-rj45 1Gb)
9. złącza:
   1. usb 3.1 typ A – min. 2 szt
   2. usb 3.1 typ C – min. 1 szt
   3. HDMI – min. 1 szt
   4. minijack (audio) – 1 szt
10. pozostałe elementy:
    1. wbudowane 2 głośniki stereo
    2. wbudowana kamera
    3. wbudowany mikrofon
    4. wydzielona klawiatura numeryczna
    5. szyfrowanie TPM 2.0
    6. dedykowany przez producenta zasilacz
    7. Slot umożliwiający fizyczne zabezpieczenie komputera np. Kensington;
    8. Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera, bez dodatkowego oprogramowania z zewnętrznych i podłączonych do niego urządzeń zewnętrznych odczytania z BIOS informacji o:
       1. - wersji BIOS
       2. - nr seryjnym komputera
       3. - Ilości zainstalowanej pamięci RAM
       4. - typie procesora i jego prędkości
          - informacja o licencji systemu operacyjnego, która została zaimplementowana w BIOS;
       5. Administrator z poziomu BIOS musi mieć możliwość wykonania poniższych czynności:
          1. Możliwość ustawienia hasła Administratora
          2. Możliwość ustawienia hasła Użytkownika
          3. Możliwość ustawienia hasła dysku twardego
          4. Możliwość włączania/wyłączania wirtualizacji z poziomu BIOS
          5. Możliwość ustawienia kolejności bootowania oraz wyłączenia poszczególnych urządzeń z listy startowej.
11. system operacyjny:
    1. Najnowsza dostępna wersja systemu.
    2. Obsługa rozszerzonego pulpitu oraz personalizacji pulpitu.
    3. Możliwość dokonywania aktualizacji i poprawek systemu przez

		Internet z możliwością wyboru instalowanych poprawek. 4. Możliwość dokonywania uaktualnień sterowników urządzeń przez Internet – witrynę producenta systemu. 5. Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych; zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v.4 i v.6. 6. Wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play, Wi-Fi). 7. Interfejs użytkownika działający w trybie graficznym, zintegrowana z interfejsem użytkownika interaktywna część pulpitu służącą do uruchamiania aplikacji, które użytkownik może dowolnie wymieniać i pobrać ze strony producenta. 8. Możliwość zdalnej automatycznej instalacji, konfiguracji, administrowania oraz aktualizowania systemu. 9. Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 10. Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych. 11. Zintegrowane z systemem operacyjnym narzędzia zwalczające złośliwe oprogramowanie; aktualizacje dostępne u producenta nieodpłatnie bez ograniczeń czasowych. 12. Zintegrowany z systemem operacyjnym moduł synchronizacji komputera z urządzeniami zewnętrznymi. 13. Wbudowany system pomocy w języku polskim. 14. Możliwość przystosowania stanowiska dla osób niepełnosprawnych (np. słabo widzących). 15. Możliwość zarządzania stacją roboczą poprzez polityki – przez politykę rozumiemy zestaw reguł definiujących lub ograniczających funkcjonalność systemu lub aplikacji. 16. Rozbudowane polityki bezpieczeństwa – polityki dla systemu operacyjnego i dla wskazanych aplikacji. 17. Możliwość pełnej integracji z usługą katalogową 12. Oprogramowanie antywirusowe: Licencje muszą być kompatybilne z posiadanym przez Zamawiającego systemem ESET Protect Advanced On-Prem – licencja na okres 36 miesięcy lub system antywirusowy równoważny 1. Opis równoważności: 1. Oprogramowanie antywirusowe spełniające poniższe funkcjonalności: 2. Ochrona stacji roboczych - Windows 1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10/Windows 11 – Zamawiający dopuszcza rozwiązanie w ramach którego na podstawie otrzymanej licencji będzie upoważniony do zainstalowania poprzednich wersji otrzymanego oprogramowania wspierającego również systemy operacyjne Windows 7 i 8. 2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows. 3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim. 4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji. 5. Pomoc w programie (help) i dokumentacja do programu		

		dostępna w języku polskim oraz angielskim. 6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives. Ochrona antywirusowa i antyspyware 7. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. 8. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor. 9. Wbudowana technologia do ochrony przed rootkitami. 10. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji. 11. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików. 12. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu. 13. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania. 14. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania). 15. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym. 16. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu. 17. Możliwość skanowania dysków sieciowych i dysków przenośnych. 18. Skanowanie plików spakowanych i skompresowanych. 19. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach. 20. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku. 21. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu. 22. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu. 23. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera. 24. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji. 25. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera. 26. 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.
27. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
28. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
29. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
30. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
31. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
32. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
33. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
34. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
35. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
36. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
37. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
38. Możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
39. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
40. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
41. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
42. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
43. W przypadku, gdy stacja robocza nie będzie posiadała

			dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne. 44. Wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie. 45. Możliwość automatycznego wysyłania nowych do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie. 46. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika. 47. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe. 48. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta. 49. Możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie. 50. Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło. 51. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo. 52. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji. 53. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu. 54. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń. 55. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku. 56. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym. 57. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.		

58. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
59. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
60. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
61. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
62. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
63. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
64. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
65. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    1. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    2. tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    3. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    4. tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
    5. tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
66. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
67. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
68. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
69. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
70. Program ma być wyposażony we wbudowaną funkcję,

			która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników. 71. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa. 72. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie. 73. Automatyczna, inkrementacyjna aktualizacja silnika detekcji. 74. Możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera. 75. Możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji. 76. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów. 77. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP. 78. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback). 79. Program wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa). 80. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym. 81. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji. 82. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym. 83. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń. 84. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu. 85. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji. 86. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie		

			poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline. 87. Możliwość podejrzenia informacji o licencji, która znajduje się w programie. 88. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM. 89. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji. 90. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. 91. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia. 92. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny. 93. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika. 94. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki. 95. Możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych. 96. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji. 97. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie. 98. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego. 99. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia. 100. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup. 101. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny. 102. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”. 103. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty. 104. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta		

określonych plików i folderów.

105. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
106. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
107. Wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
108. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
109. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

Ochrona przed spamem

110. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
111. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
112. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
113. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
114. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
115. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
116. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
117. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
118. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
119. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
120. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

121. Zapora osobista ma pracować w jednym z czterech trybów:
    1. tryb automatyczny – program blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    2. tryb interaktywny – program pyta się o każde nowo nawiązywane połączenie,
    3. tryb oparty na regułach – program blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,

		4. tryb uczenia się – program automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu. 122. Program musi oceniać reguły zapory systemu Windows. 123. Możliwość tworzenia list sieci zaufanych. 124. Możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie. 125. Możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego. 126. Możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj. 127. Możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji. 128. Możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet. 129. Wykrywanie modyfikacji w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu. 130. Możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci. 131. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. 132. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora. 133. Autoryzacja stref ma się odbywać min. 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, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie. 134. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6. 135. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci. 136. Program musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów: 1. z aplikacją lokalną, którą administrator wskazuje z listy, 2. z połączeniem z urządzeniem zdalnym, na podstawie jego adresu IP. Kontrola dostępu do stron internetowych 137. Aplikacja musi być wyposażona w zintegrowany		

		moduł kontroli dostępu do stron internetowych. 138. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory. 139. Aplikacja musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii. 140. Podstawowe kategorie, w jakie aplikacja musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii. 141. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych. 142. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta. 143. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych. 144. Aplikacja musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj. 145. Program musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej. Bezpieczna przeglądarka 146. Aplikacja musi być wyposażona w moduł bezpiecznej przeglądarki. 147. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika. 148. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki. 149. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę. 150. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki. 151. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki. 13. Gwarancja: 1. Min. 3 lata od daty dostawy w miejscu instalacji komputera. czas reakcji na zgłoszenie 24 godziny, czas na usunięcie awarii - do 5 roboczy po otrzymaniu zgłoszenia (przyjmowanie zgłoszeń w dni robocze w godzinach 8.00 — 16.00). 2. W przypadku awarii dysku uszkodzone urządzenie pozostaje w zasobach Zamawiającego		

1. W zaproponowanej cenie, Oferent musi zawrzeć wszystkie koszty niezbędne do właściwego wykonania przedmiotowej usługi, łącznie z kosztami dostarczenia produktów do siedziby Zamawiającego.
2. Sposób transportu oraz opakowanie sprzętów muszą zapewniać zabezpieczenie przed uszkodzeniami. Za szkody powstałe z winy nienależytego opakowania oraz/lub transportu winę ponosi Wykonawca.
3. Zamawiający wymaga, aby dostarczony sprzęt stanowiący przedmiot zamówienia był fabrycznie nowy, nieużywany, znajdował się w stanie nieuszkodzonym, technicznie sprawnym, kompletnym i gotowym do użytkowania oraz spełniał wymagane polskim prawem normy i był wolny od wad prawnych. Zamawiający wyklucza dostawę sprzętu powystawowego.
4. Zamawiający wymaga, aby dostarczone urządzenia miały legalnie zainstalowane oprogramowanie (jeżeli dotyczy).
5. Dostawa przedmiotu zamówienia nastąpi w dni robocze tj. poniedziałek – piątek, po wcześniejszym uzgodnieniu z Zamawiającym.
6. Wykonawca ma obowiązek dostarczyć sprzęt do pomieszczeń wskazanych przez Zamawiającego,
7. Jeżeli opis przedmiotu zamówienia wskazywałyby w odniesieniu do niektórych materiałów lub urządzeń znaki towarowe, patenty lub pochodzenie – Zamawiający dopuszcza oferowanie materiałów lub urządzeń równoważnych. Materiały lub urządzenia pochodzące od konkretnych producentów określają minimalne parametry jakościowe, cechy użytkowe, jakim musza odpowiadać materiały lub urządzenia oferowane przez Wykonawcę, aby spełnione zostały wymagania stawiane przez Zmawiającego. Materiały i urządzenia pochodzące od konkretnych producentów stanowią wyłącznie wzorzec jakościowy przedmiotu zamówienia. Pod pojęciem „minimalne parametry jakościowe i cechy użytkowe" Zamawiający rozumie wymagania dotyczące materiałów lub urządzeń zawarte w ogólnie dostępnych źródłach, katalogach, stronach internetowych producentów. Operowanie przykładowymi nazwami producenta ma na celu doprecyzowanie poziomu oczekiwań Zamawiającego w stosunku do określonego rozwiązania. Posługiwanie się nazwami produktów/producentów ma wyłącznie charakter przykładowy. Zamawiający wskazując oznaczenie konkretnego producenta (dostawcy) lub konkretny produkt w opisie przedmiotu zamówienia, dopuszcza jednocześnie produkty równoważne o parametrach użytkowych i cechach jakościowych co najmniej na poziomie parametrów wskazanego produktu, uznając tym samym każdy produkt o wskazanych lub lepszych parametrach.
8. W każdym przypadku, gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych, dopuszcza rozwiązania równoważne opisywanym.
9. W każdym przypadku, w którym Zamawiający żąda aby oferowany sprzęt posiadał deklarację CE oznacza to deklarację wynikającą z dyrektyw tzw. "Nowego Podejścia" Unii Europejskiej.
10. Wykonawca, który powołuje się na rozwiązania równoważne opisanym przez Zamawiającego, jest zobowiązany wykazać, że oferowane przez niego dostawy spełniają wymagania określone przez Zamawiającego.
11. Wykonawca zobowiązany jest dołączyć do oferty specyfikację dotyczącą parametrów technicznych oferowanego sprzętu.

12. Oferowany przedmiot zamówienia musi być w I gatunku, nieuszkodzony, wolny od wad fizycznych i prawnych, w pełni sprawny i funkcjonujący bez jakichkolwiek zakłóceń oraz zastrzeżeń. Przedmiot zamówienia nie może pochodzić z żadnych pokazów ani wystaw pozbawiony praw i obciążeń osób trzecich, a także odpowiadający obowiązującym normom i posiadający niezbędne certyfikaty i atesty zgodnie z obowiązującymi przepisami prawa, które zostaną przekazane Zamawiającemu w dniu dostawy.
13. Wykonawca dostarczy przedmiot zamówienia kompletny, gotowy do uruchomienia i użytkowania bez dodatkowych nakładów i zakupów.
14. Wykonawca dostarczy przedmiot zamówienia dopuszczony do obrotu i stosowania w krajach UE.
15. Wykonawca dostarczy dołączone przez producenta sprzętu nośniki z oprogramowaniem oraz niezbędną dokumentację i instrukcje.
16. Wykonawca dostarczy przedmiot zamówienia na koszt własny w opakowaniach zabezpieczających przed uszkodzeniem w czasie transportu.
17. Wykonawca udzieli gwarancji jakości oraz zapewnieni świadczenie usługi serwisu gwarancyjnego przez autoryzowany serwis producenta oferowanego sprzętu komputerowego na okres i warunkach nie gorszych niż gwarancja producenta.
18. Wykonawca zapewni zamawiającemu dostęp do aktualizacji sterowników za pośrednictwem serwisu internetowego (o ile dotyczy).
19. Wykonawca wyszczególni na fakturze lub w załączniku do faktury kwoty jednostkowe do każdej pozycji
20. Miejsce dostawy: Centrum Kreatywności Pałacyk ul. Konstytucji 3 Maja 15, 27-200 Starachowice, tel. 41 3221156; email: palacyk@starachowice.eu
21. Termin dostawy: 5 kwietnia 2024 r.

III. Kryteria wymagane wobec Wykonawcy:

1. W postępowaniu mogą brać udział Wykonawcy, którzy spełniają warunki, dotyczące:
   a. posiadania uprawnień do wykonywania określonej działalności lub czynności, jeżeli przepisy prawa nakładają obowiązek ich posiadania,
   b. posiadania wiedzy i doświadczenia niezbędnego do wykonania usługi,
   c. dysponowania odpowiednim potencjałem technicznym oraz osobami zdolnymi do wykonania zamówienia,
   d. znajdują się w sytuacji ekonomicznej i finansowej zapewniającej wykonanie zamówienia.
2. Wykonawca może polegać na wiedzy i doświadczeniu, potencjale technicznym, osobach zdolnych do wykonania zamówienia lub zdolnościach finansowych innych podmiotów, niezależnie od charakteru prawnego łączących go z nimi stosunków. Wykonawca w takiej sytuacji zobowiązany jest udowodnić Zamawiającemu, iż będzie dysponował zasobami niezbędnymi do realizacji zamówienia, w szczególności przedstawiając w tym celu pisemne zobowiązanie tych podmiotów do oddania mu do dyspozycji niezbędnych zasobów na okres korzystania z nich przy wykonywaniu zamówienia.
3. Wykonawca, który zamierza powierzyć wykonanie części przedmiotu zamówienia innej firmie lub osobie (podwykonawcy) jest zobowiązany do:
   a. określenia w złożonej ofercie informacji, jaki zakres przedmiotu zamówienia będzie realizowany przez podwykonawców,
   b. przy realizacji zamówienia z udziałem podwykonawcy zastosowanie mają przepisy art. 738 Kodeksu Cywilnego.

4. Wykonawca ponosi pełną odpowiedzialność za realizację przedmiotu zamówienia przez podwykonawcę.
5. Wykonawca przed podpisaniem umowy, musi przedłożyć Zamawiającemu kopie oświadczeń bądź umów ze wskazanymi w ofercie podwykonawcami, a w przypadku konsorcjum umowę regulującą wzajemną współpracę i zobowiązania jego członków.
6. W celu uniknięcia konfliktu interesów Zamawiający nie może udzielać zamówienia podmiotom powiązanym z nim osobowo lub kapitałowo. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przygotowaniem i przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:
   a. uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   b. posiadaniu co najmniej 10 % udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez Operatora Programu,
   c. pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   d. pozostawaniu w takim stosunku prawnym lub faktycznym, który może budzić uzasadnione wątpliwości, co do bezstronności w wyborze wykonawcy, w szczególności pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia lub w stosunku przysposobienia, opieki lub kurateli. Operator Programu może wyrazić zgodę na udzielenie zamówienia pomimo wystąpienia przesłanek, o których mowa powyżej.

IV. Dokumenty jakie powinni dostarczyć Wykonawcy:

1. Formularz ofertowy, stanowiący załącznik nr 1 do niniejszego zapytania ofertowego wraz z oświadczeniem o braku powiązań kapitałowych lub osobowych z Zamawiającym.
2. Zaparafowany wzór umowy.

V. Informacja o sposobie porozumiewania się z wykonawcami

1. Wszelkiego rodzaju oświadczenia, wnioski, zawiadomienia, informacje, uzupełnienia, pytania itp. (zwane dalej Korespondencją, wyłączając umowę na realizację usługi, aneksy oraz protokoły odbioru) Zamawiający i Wykonawca zobowiązują się przekazywać pisemnie – pocztą elektroniczną.
2. Nie udziela się żadnych ustnych i telefonicznych informacji, wyjaśnień czy odpowiedzi na kierowane do Zamawiającego zapytania w sprawach wymagających zachowania pisemności postępowania.
3. Na etapie składania ofert, wszelkie pytania należy składać poprzez adres email: kamil.stanos@starachowice.eu.

VI. Opis sposobu przygotowania oferty

1. Wykonawcy zobowiązani są zapoznać się dokładnie z informacjami zawartymi w zapytaniu ofertowym i przygotować ofertę zgodnie z wymaganiami określonymi w tym dokumencie.
2. Podane w „Formularzu oferty" ceny muszą uwzględniać wszystkie koszty związane z realizacją zamówienia i nie mogą ulec zmianie w trakcie trwania umowy. Wykonawca przedstawi w ofercie cenę całkowitą netto i brutto obejmującą całość przedmiotu zamówienia, podając ją w zapisie liczbowym i słownie. Cena oferowana musi zawierać wszystkie koszty związane z realizacją zadania, w tym podatek VAT w ustawowej wysokości, a także inne koszty niezbędne do zrealizowania zamówienia. Cena oferty ma być wyrażona w PLN.
   W przypadku oferty złożonej przez osobę fizyczną, zaoferowana cena musi uwzględniać wszelkie składki ZUS i US (tzw. kwota brutto brutto).
3. Każdy Wykonawca może przedstawić tylko jedną ofertę.

VII. Miejsce i termin składania ofert

1. Termin składania ofert upływa **7 marca 2024 r. o godz. 09.00**. Oferty złożone po tym terminie zostaną odrzucone. Liczy się termin wpływu do Zamawiającego.
2. Oferty należy złożyć bezpośrednio poprzez Bazę Konkurencyjności załączając wszystkie wymagane załączniki podpisane elektronicznie lub zeskanowane.
3. Oferty złożone przez pocztę elektroniczną zostaną odrzucone.

VIII. Opis kryteriów i sposobu oceny oferty

1. Zamawiający ma prawo odrzucić ofertę, jeżeli:
   a. jej treść nie odpowiada treści niniejszego zapytania,
   b. została złożona przez Wykonawcę wykluczonego z udziału w postępowaniu o udzielenie zamówienia (wykluczenie dotyczy sytuacji, gdy Wykonawca nie spełni warunków udziału w postępowaniu, określonych w pkt. 3 – zostaje on wówczas wykluczony z postępowania a jego ofertę uznaje się za odrzuconą).
2. Wykonawca może złożyć ofertę na wszystkie części bądź na poszczególne części.
3. Każda część będzie oceniana osobno.
4. Kryterium wyboru oferty do każdej części: cena brutto oferty – 100 pkt.

Punktacja dla kryterium cena brutto oferty dla każdej części wyliczana będzie według następującego wzoru P_1 – 100 pkt.

$$P_1 = \frac{Cmin}{Co} \times 100$$

gdzie:
Cmin - najniższa cena brutto
Co - cena badanej oferty

5. Zamawiający uzna i wybierze, jako najkorzystniejszą ofertę z najwyższą liczbą punktów do każdej części.
6. Zamawiający udzieli zamówienia Wykonawcy/Wykonawcom, którego/ych oferta odpowiada wszystkim wymaganiom określonym w niniejszym zapytaniu i została oceniona, jako najkorzystniejsza w oparciu o podane kryterium wyboru, podpisując umowę, której projekt stanowi załącznik nr 2 do niniejszego zapytania.
7. Zamawiający może w toku badania i oceny ofert żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert.
8. Zamawiający może wezwać Wykonawcę do uzupełnienia brakujących oświadczeń lub dokumentów lub poprawienia oświadczeń lub dokumentów zawierających błędy.
9. Zamawiający odrzuci ofertę jeżeli będzie ona zawierała cenę brutto wyższą niż kwota, którą dysponuje Zamawiający na realizację usługi. Z tego tytułu Wykonawcom nie przysługują żadne roszczenia przeciwko Zamawiającemu.
10. Zamawiający zastrzega sobie możliwość negocjacji ceny z Wykonawcą, który zaoferuje cenę najniższą a która przewyższać będzie możliwości finansowe Zamawiającego.

IX. Warunki zmiany umowy

1. Zamawiający przewiduje możliwość wprowadzenia zmian postanowień zawartej, z wybranym Wykonawcą, umowy, w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy. Strony wprowadzą zmiany do umowy w przypadku zaistnienia jednej z okoliczności określonych poniżej (w podpunktach a)-f)) – w przypadku gdy ta okoliczność ma wpływ na postanowienia umowy. Zmiany nie mogą naruszać obowiązujących przepisów prawa ani Wytycznych w zakresie kwalifikowalności wydatków w ramach Norweskiego Mechanizmu Finansowego na lata 2014-2021. Dopuszczalne będą zmiany wynikające w szczególności ze:

a. Zmian w podatku VAT – wynikających ze zmiany przepisów.
b. Zmian jakichkolwiek rozporządzeń, przepisów i innych dokumentów, w tym dokumentów programowych Norweskiego Mechanizmu Finansowego na lata 2014-2021, mających wpływ na realizację umowy.
c. Zmian w zakresie osób wykonujących zamówienie – Zamawiający dopuszcza możliwość zmiany osób osobiście wykonujących zamówienie lub dołączenie do grona osób osobiście wykonujących zamówienie dodatkowej osoby pod warunkiem uzyskania przez Wykonawcę

akceptacji na piśmie ze strony Zamawiającego, przy czym akceptację może uzyskać jedynie kandydatura osoby spełniającej wymogi niniejszego zapytania ofertowego. Zmiana osoby wykonującej zamówienie bez zgody Zamawiającego skutkować będzie naruszeniem warunków umowy, a tym samym uprawniać Zamawiającego do odstąpienia od umowy

d. Zmian w zakresie osób wykonujących zamówienie – na wniosek Zamawiającego, w przypadku niewywiązywania się osób wykonujących zamówienie z powierzonych im obowiązków lub nieprawidłowego wykonywania powierzonych obowiązków. Osoba zastępująca musi spełniać wymogi niniejszego zapytania ofertowego.
e. Zmian terminu realizacji zamówienia z przyczyn uwzględniających potrzeby prawidłowej realizacji projektu i osiągnięcia, założonych w projekcie, wskaźników, np. uzasadnionych zmian harmonogramu realizacji działań projektowych,
f. Wystąpienia okoliczności na które Zamawiający i/lub Wykonawca nie miał wpływu i nie mógł przewidzieć na czas realizacji zamówienia, a które w istotny sposób wpływają na obopólne zobowiązania Zamawiającego i Wykonawcy (dalej: Strony), w przypadku zmiany przepisów prawa istotnych dla realizacji zamówienia, zmian gospodarczych i ustrojowych oraz w przypadku wystąpienia tzw. siły wyższej. Dla celów umowy „siła wyższa" oznacza zdarzenia zewnętrzne, na wystąpienie których Strona nie ma wpływu, których nie można było przewidzieć i których nie dało się uniknąć nawet w przypadku dołożenia przez Strony najwyższej staranności, i które uniemożliwiają wykonanie zobowiązań wynikających z umowy, a w szczególności takie jak wojna, zamach terrorystyczny, rozruchy, trzęsienie ziemi, pożar, eksplozja, strajk, lokaut, generalny brak środków transportu, materiałów lub siły roboczej lub ograniczenia w dostawie energii. Strona, u której wyniknęły utrudnienia w wykonaniu umowy wskutek działania siły wyższej, jest obowiązana do niezwłocznego poinformowania drugiej Strony o wystąpieniu i ustaniu działania siły wyższej. Brak powiadomienia lub zwłoka z powiadomieniem drugiej Strony o wystąpieniu siły wyższej spowoduje, iż Strona ta nie będzie mogła skutecznie powoływać się na siłę wyższą jako przyczynę zwolnienia z odpowiedzialności za niewykonanie lub nienależyte wykonanie zobowiązania. Strona, u której wyniknęły utrudnienia w wykonaniu umowy na skutek działania siły wyższej, jest obowiązana do podjęcia wszelkich możliwych i prawem przewidzianych działań w celu zminimalizowania wpływu działania siły wyższej na wykonanie umowy. Daty lub terminy wypełnienia zobowiązań wynikających z umowy zostaną przełożone lub przedłużone o okres, w którym istniała siła wyższa. Siła wyższa nie obejmuje zdarzeń, będących wynikiem niewykonania lub nienależytego wykonywania umowy, których wystąpienie Strona przy dołożeniu należytej staranności mogła przewidzieć w chwili zawierania umowy lub mogła im zapobiec.

X. Osoba do kontaktów: Iwona Tamiołło, adres e-mail: palacyk@starachowice.eu

XI. Załączniki:

Następujące załączniki stanowią integralną część zaproszenia:

a. Załącznik 1 – Formularz ofertowy
b. Załącznik 2 – Wzór umowy