Lublin, 29.07.2024 r.

Zapytanie ofertowe nr 6/2024

dotyczące dostawy klastra dwóch urządzeń do ochrony sieci

I. Nazwa i adres Zamawiającego

Nazwa: „INTROGRAF-LUBLIN" SPÓŁKA AKCYJNA

Adres: ul. Vetterów 22

Miejscowość: 20-277 Lublin

NIP: 7122321973

II. Tryb udzielania zamówienia

1. Zamówienie realizowane będzie w ramach projektu „Robotyzacja i cyfryzacja procesów produkcyjnych zachodzących w przedsiębiorstwie "INTROGRAF-LUBLIN" S.A.", który został złożony w odpowiedzi na konkurs w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, Komponent A „Odporność i konkurencyjność gospodarki", Cel szczegółowy: A2. Rozwój narodowego systemu innowacji: wzmocnienie koordynacji, stymulowanie potencjału innowacyjnego oraz współpracy pomiędzy przedsiębiorstwami i organizacjami badawczymi, w tym w zakresie technologii środowiskowych, Reforma: A2.1. Przyśpieszenie procesów robotyzacji i cyfryzacji i innowacji; Inwestycja: A2.1.1. Inwestycje wspierające robotyzację i cyfryzację w przedsiębiorstwach.
2. Zapytanie ofertowe zostało opublikowane na stronie www.introgaf.com.pl
3. W niniejszym postępowaniu o udzielenie zamówienia nie mają zastosowania przepisy ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (tj. Dz. U. 2022 poz. 1710 ze zm.)
4. Językiem obowiązującym w ramach postępowania jest język polski.

III. Nazwa i kod zamówienia

1. Nazwa zamówienia: Dostawa klastra dwóch urządzeń do ochrony sieci
2. Kategoria zamówienia: dostawy
3. Podkategoria zamówienia: dostawy sprzętu IT
4. Kody CPV:

   Kod główny: 32420000-3 Urządzenia sieciowe

   Kody pomocnicze: 48210000-3: Pakiety oprogramowania dla sieci

   30200000-1 - Urządzenia komputerowe

   48800000-6 - Systemy i serwery informacyjne

IV. Cel zamówienia

Celem zamówienia jest wybór dostawcy klastra dwóch urządzeń do ochrony sieci w ramach projektu Robotyzacja i cyfryzacja procesów produkcyjnych zachodzących w przedsiębiorstwie ”INTROGRAF-LUBLIN” S.A.”.

V. Skrócony opis przedmiotu zamówienia

Przedmiotem zamówienia jest dostawa klastra dwóch urządzeń do ochrony sieci w ramach projektu Robotyzacja i cyfryzacja procesów produkcyjnych zachodzących w przedsiębiorstwie ”INTROGRAF-LUBLIN” S.A.”.

VI. Szczegółowy opis przedmiotu zamówienia

Zamawiający oczekuje dostawy klastra dwóch urządzeń o poniższych wymaganiach minimalnych:

1. **Wymagania Ogólne**
   Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza internetowego. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca ma zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
   System realizujący funkcję Firewall ma dać możliwość pracy w jednym z trzech trybów: Routera z funkcją NATlub transparentnym lub monitorowania na porcie SPAN.
   W ramach dostarczonego systemu bezpieczeństwa ma być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall’a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Ma być zapewniona możliwość dedykowania co najmniej 3 administratorów do poszczególnych instancji systemu.
   System ma wspierać IPv4 oraz IPv6 w zakresie:
   - ✓ Firewall.
   - ✓ Ochrony w warstwie aplikacji.
   - ✓ Protokołów routingu dynamicznego.

2. **Redundancja, monitoring i wykrywanie awarii**
   a. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – ma istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach ma istnieć funkcja synchronizacji sesji firewall.
   b. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   c. Monitoring stanu realizowanych połączeń VPN.
   d. System ma umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Ma istnieć możliwość tworzenia interfejsów redundantnych.

3. **Interfejsy, Zasilanie:**
   a. System realizujący funkcję Firewall ma dysponować minimum:
   - ✓ 8 portami Gigabit Ethernet RJ-45.
   - ✓ 8 gniazdami SFP 1 Gbps.
   - ✓ 2 gniazdami SFP+ 10 Gbps.

   b. System Firewall ma posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   c. W ramach systemu Firewall ma być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN’y w oparciu o standard 802.1Q.
   d. System ma być wyposażony w dwa zasilania AC.

4. **Parametry wydajnościowe:**
   a. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln jednoczesnych połączeń oraz nie mniej niż 56 tys. nowych połączeń na sekundę.
   b. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
   c. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
   d. Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B.
   e. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps.
   f. Wydajność szyfrowania IPSec VPN nie mniej niż 11 Gbps.
   g. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.6 Gbps.
   h. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
   i. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

5. **Funkcje Systemu Bezpieczeństwa:**
   W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   a. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
   b. Kontrola Aplikacji.
   c. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
   d. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
   e. Ochrona przed atakami - Intrusion Prevention System.
   f. Kontrola stron WWW.
   g. Kontrola zawartości poczty – Antyspam dla protokołów: SMTP, POP3.
   h. Zarządzanie pasmem (QoS, Traffic shaping).
   i. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
   j. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych (lub innej metody wysyłania kodów jednorazowych). W ramach postępowania mają zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
   k. Analiza ruchu szyfrowanego protokołem SSL.
   l. Analiza ruchu szyfrowanego protokołem SSH.

6. **Polityki, Firewall**
   a. Polityka Firewall ma uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
   b. System ma zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
      ✓ Translację jeden do jeden oraz jeden do wielu.
      ✓ Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
   c. W ramach systemu ma istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   d. Element systemu realizujący funkcję Firewall ma integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
      ✓ Amazon Web Services (AWS).
      ✓ Microsoft Azure
      ✓ Cisco ACI.
      ✓ Google Cloud Platform (GCP).
      ✓ Nuage Networks VSP.

- ✓ OpenStack.
- ✓ VMware vCenter (ESXi).
- ✓ VMware NSX.

7. Połączenia VPN

a. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   - ✓ Wsparcie dla IKE v1 oraz v2.
   - ✓ Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
   - ✓ Obsługa protokołu Diffie-Hellman grup 19 i 20.
   - ✓ Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
   - ✓ Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
   - ✓ Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
   - ✓ Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
   - ✓ Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
   - ✓ Mechanizm „Split tunneling" dla połączeń Client-to-Site.

b. System ma umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji ma zapewniać:
   - ✓ Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system ma zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
   - ✓ Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
   - ✓ Producent rozwiązania ma dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

8. Routing i obsługa łączy WAN

a. W zakresie routingu rozwiązanie ma zapewniać obsługę:
   - ✓ Routingu statycznego.
   - ✓ Policy Based Routingu.
   - ✓ Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.

9. Zarządzanie pasmem

a. System Firewall ma umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
b. System ma mieć możliwość określania pasma dla poszczególnych aplikacji.
c. System ma zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware

a. Silnik antywirusowy ma umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
b. System ma umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
c. System ma dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
d. System ma współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania ma zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
e. System ma umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.

11. Ochrona przed atakami

a. Ochrona IPS ma opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
b. System ma chronić przed atakami na aplikacje pracujące na niestandardowych portach.
c. Baza sygnatur ataków ma zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
d. Administrator systemu ma mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur.
e. System ma zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
f. Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies.
g. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.

12. Kontrola aplikacji

a. Funkcja Kontroli Aplikacji ma umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
b. Baza Kontroli Aplikacji ma zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
c. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) mają być kontrolowane pod względem wykonywanych czynności, np. pobieranie, wysyłanie plików.
d. Baza ma zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa tj. proxy, P2P.
e. Administrator systemu ma mieć możliwość definiowania wyjątków oraz własnych sygnatur.

13. Kontrola WWW

a. Moduł kontroli WWW ma korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
b. W ramach filtra www mają być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
c. Filtr WWW ma dostarczać kategorii stron zabronionych prawem: Hazard.
d. Administrator ma mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
e. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
f. System ma umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
g. Administrator ma mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
h. W ramach systemu mai istnieć możliwość określenia, dla których kategorii URL lub wskazanych URL - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

14. Uwierzytelnianie użytkowników w ramach sesji

a. System Firewall ma umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - ✓ Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - ✓ Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - ✓ Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.

b. Ma istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
c. Rozwiązanie ma umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.

15. Zarządzanie

a. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
b. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
c. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
d. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
e. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
f. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
g. Element systemu realizujący funkcję Firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

16. Logowanie

a. Elementy systemu bezpieczeństwa mają realizować logowanie do aplikacji (logowania, raportowania, korelacji zdarzeń, powiadamiania o incydentach) udostępnianej w chmurze, lub w ramach zapytania musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
b. W ramach logowania system pełniący funkcję Firewall ma zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ma być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
c. Logowanie ma obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
d. Ma istnieć możliwość logowania do serwera SYSLOG.

17. Certyfikaty

Poszczególne elementy oferowanego systemu bezpieczeństwa mają posiadać następujące certyfikacje: ICSA lub EAL4 dla funkcji Firewall lub równoważne w zakresie bezpieczeństwa.

18. Serwisy i licencje

W ramach postępowania mają zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Mają one obejmować: Kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analizę typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 60 miesięcy.

19. Gwarancja oraz wsparcie

a. System ma być objęty serwisem gwarancyjnym producenta przez okres 60 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości.

W ramach tego serwisu producent ma zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

b. Dostawca ma zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5.
c. Wykonawca ma przeprowadzić przynajmniej 5-godzinne szkolenie z obsługi oferowanego rozwiązania dla maksymalnie 3 administratorów. Szkolenie ma być przeprowadzone w ciągu 12 miesięcy od dostawy rozwiązania do Zamawiającego.
d. Dostawca ma zapewnić wdrożenie oferowanego rozwiązania w oparciu o aktualne trendy panujące w sferze zagrożeń sieciowych. W ramach wdrożenia Dostawca wykona rejestrację i instalację urządzeń, aktualizację oprogramowania, konfigurację urządzeń zgodnie z założeniami polityki bezpieczeństwa przedsiębiorstwa (interfejsy sieciowe, routing, polityki firewall, DNS, Web filtering, anti-spam, anti-virus, controla aplikacji, ips, ids, virtual private network, integracja z domeną, zarządzanie pasmem, uwierzytelnianie użytkowników, sieci bezprzewodowe, redundancja dostępu do internetu, logowanie oraz raportowanie, alerty administracyjne, dostosowanie do współpracy z zewnętrznym systemem logowania i raportowania). Po wdrożeniu Dostawca wykona kopię bezpieczeństwa i zweryfikuje poprawność implementacji oferowanego rozwiązania (testy akceptacyjne).
e. Przez okres roku od wdrożenia Dostawca zapewni dodatkową usługę konsultacji oraz rekonfiguracji uruchomionego systemu.

VII. Termin realizacji zamówienia

Dostawa przedmiotu zamówienia zostanie zrealizowana w nieprzekraczalnym terminie do **31.12.2024 r.**

Cena musi uwzględniać wszystkie wymagania specyfikacji określone w niniejszym zapytaniu ofertowym oraz obejmować wszelkie koszty jakie poniesie Oferent z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia.

Zamawiający przewiduje płatność jednorazową lub częściową wg poniższych założeń:

a. Transza nr 1: o wartości 70% oferowanej ceny zostanie zapłacona w terminie do 30 dni po podpisaniu umowy na podstawie prawidłowo wystawionej faktury.

b. Rozliczenie końcowe o wartości 30% oferowanej ceny zostanie zapłacone w terminie do 14 dni na podstawie prawidłowo wystawionej faktury poprzedzonej protokołem odbioru podpisanym przez każdą ze stron.

VIII. Zamówienia częściowe i wariantowe

Zamawiający nie dopuszcza składania ofert częściowych.

Zamawiający nie dopuszcza składania ofert wariantowych.

IX. Miejsce realizacji zamówienia

Siedziba Zamawiającego.

X. Warunki udziału w postępowaniu i opis sposobu dokonywania ich oceny

O udzielenie zamówienia mogą ubiegać się Oferenci, którzy łącznie spełniają następujące warunki:

a. Znajdują się w dobrej sytuacji ekonomicznej i finansowej, zapewniającej realizację umowy;

   Zamawiający nie stawia warunku szczegółowego.

   Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

b. Dysponują potencjałem technicznym niezbędnym do wykonania zamówienia;

   Zamawiający nie stawia warunku szczegółowego.

   Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

c. Dysponują osobami zdolnymi do wykonania zamówienia
   Zamawiający wymaga, aby Oferent dysponował co najmniej:

   1. Trzema osobami – inżynierami posiadającymi aktualny certyfikat producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden z inżynierów musi posiadać najwyższy stopień certyfikacji)
   2. Dwoma osobami – inżynierami posiadającymi certyfikat Fortinet_Certified_Solution_Specialist_Network_Security lub równoważnymi w zakresie kompetencji związanych z sieciami komputerowymi i konfiguracją urządzeń sieciowych, w tym konfiguracji urządzeń klasy firewall.

   Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego. Dodatkowo Zamawiający wymaga dołączenia do oferty posiadanych certyfikatów.

d. Posiadają niezbędną wiedzę i doświadczenie do prawidłowego wykonania przedmiotu zamówienia;

   Wymagane jest, aby Oferent posiadał udokumentowane doświadczenie w okresie ostatnich 2 lat lub jeśli okres prowadzenia działalności przez Oferenta jest krótszy w tym okresie, w postaci co najmniej 5 szkoleń z obszaru objętego zapytaniem ofertowym dla firm zatrudniających powyżej 100 osób.

   Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

e. Posiadają uprawnienia do wykonania określonej działalności zgodnie z ustawodawstwem kraju, na terenie którego prowadzimy działalność;

   Zamawiający wymaga, aby Oferent posiadł odpowiednie uprawnienia, by w razie zgłoszenia przez Zamawiającego problemu do producenta oferowanego rozwiązania, Oferent miał możliwość zmiany priorytetu zgłoszenia.

   Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

f. Nie podlegają wykluczeniu, tj. nie otwarto wobec nich likwidacji i nie ogłoszono upadłości;

Zamawiający nie stawia warunku szczegółowego.

Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

g. Zgadzają się ze wszystkimi wymaganiami niniejszego postępowania.

Zamawiający nie stawia warunku szczegółowego.

Sposób oceny spełniania warunku: Weryfikacja nastąpi w oparciu o oświadczenie Oferenta – wg załącznika nr 1 do Zapytania ofertowego.

Ocena spełnienia warunków nastąpi według formuły „spełnia/nie spełnia".

Termin związania ofertą wynosi 60 dni od ostatecznego terminu składania ofert.

Oferent samodzielnie lub na wniosek Zamawiającego może przedłużyć termin związania ofertą, z tym, że zamawiający może tylko raz, co najmniej na 3 dni przed upływem terminu związania ofertą, zwrócić się do oferentów o wyrażenie zgody na przedłużenie tego terminu o oznaczony okres, nie dłuższy jednak niż 60 dni.

XI. Kryterium wyboru ofert

Zamawiający dokona oceny ofert, które nie zostały odrzucone, na podstawie następujących kryteriów oceny ofert:

a) Cena netto (waga kryterium: 100%) obydwu zadań łącznie

Sposób wyliczania punktów w ramach kryterium Cena netto:

$$\boldsymbol{C = \frac{CB}{Cob} x [100]}$$

gdzie:

C – liczba punktów przyznanych Wykonawcy za zaoferowaną cenę,

CB – najniższa zaoferowana cena w postępowaniu,

COB – cena zaoferowana w ofercie badanej.

Końcowy wynik powyższego działania zostanie zaokrąglony do dwóch miejsc po przecinku.

Zamówienie zostanie udzielone Oferentowi, którego oferta nie będzie podlegać odrzuceniu i w wyniku oceny zajmie najwyższe miejsce według liczby punktów.

XII.Termin, miejsce i sposób złożenia oferty

Termin składania ofert: **do 12.08.2024 r.**

1. Oferta powinna zawierać:
    a. wypełniony i podpisany Formularz ofertowy (Załącznik nr 1)
    b. wypełniony i podpisany formularz Oświadczenie o braku podstaw do wykluczenia z udziału w postępowaniu (Załącznik nr 2)
    c. dokumenty potwierdzające spełnienie warunków udziału w postępowaniu określone w punkcie X.

2. Ofertę należy przesłać elektronicznie na adres: sekretariat@introgaf.com.pl lub przesłać do siedziby Spółki do dnia **12.08.2024 r.**(termin składania ofert).
3. Wyjaśnienia dotyczące warunków zamówienia będą udzielane na podstawie zapytań mailowych kierowanych na adres: it@introgaf.com.pl
4. Otwarcie ofert nastąpi niezwłocznie po zakończeniu terminu składania ofert.
5. Oferta powinna być podpisana zgodnie z reprezentacją wynikającą z dokumentu rejestrowego. O ile prawo do reprezentowania Oferenta nie wynika wprost z dokumentu rejestrowego, wraz z ofertą należy przedłożyć stosowne pełnomocnictwo do złożenia oferty.
6. Zamawiający zastrzega sobie prawo do wezwania Oferentów do uzupełnień/wyjaśnień, w tym także w przypadku złożenia oferty na niewłaściwym formularzu.
7. Umowa z Wykonawcą, który złoży najkorzystniejszą ofertę, zostanie podpisana w dogodnym dla obu stron terminie.

XIII. Wykluczenia z udziału w postępowaniu

1. Zamawiający wykluczy Wykonawcę, który jest powiązany z Zamawiającym 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 przeprowadzeniem procedury wyboru wykonawcy a Wykonawcą, polegające w szczególności na:

   a. uczestniczenie w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   b. posiadanie co najmniej 10 % udziałów lub akcji (o ile niższy próg nie wynika z przepisów prawa),
   c. pełnienie funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   d. pozostawanie w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa lub powinowactwa w linii bocznej do drugiego stopnia, lub związanie z tytułu przysposobienia, opieki lub kurateli albo pozostawanie we wspólnym pożyciu z wykonawcą, jego zastępcą prawnym lub członkami organów zarządzających lub organów nadzorczych wykonawców ubiegających się o udzielenie zamówienia,
   e. pozostawanie z wykonawcą w takim stosunku prawnym lub faktycznym, że istnieje uzasadniona wątpliwość co do ich bezstronności lub niezależności w związku z postępowaniem o udzielenie zamówienia.

   Zamawiający, w celu potwierdzenia braku powiązań osobowych lub kapitałowych, wymaga przedłożenia przez Wykonawcę oświadczenia (wzór oświadczenia stanowi Załącznik nr 2 do Zapytania ofertowego).

2. Z udziału w postępowania wykluczeni zostaną również Oferenci wobec których zachodzą przesłanki wykluczenia z postępowania określone w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

Zamawiający, w celu potwierdzenia podstaw do wykluczenia z udziału w postępowaniu, wymaga przedłożenia przez Wykonawcę oświadczenia (wzór oświadczenia stanowi Załącznik nr 2 do Zapytania ofertowego).

XIV. Kary umowne

1. Zamawiający może żądać od Dostawcy zapłaty następujących kar umownych:

   a. za opóźnienie w wykonaniu zlecenia w ramach przedmiotu umowy – w wysokości 1% wartości brutto przedmiotu zamówienia za każdy dzień opóźnienia;

   b. w wypadku odstąpienia od umowy przez Zamawiającego z przyczyn leżących po stronie Dostawcy, tj. w przypadku niewykonania lub nienależytego wykonania zobowiązań przez Dostawcę w wysokości 10% wartości brutto przedmiotu zamówienia;

2. W przypadku gdy wysokość szkody poniesionej przez Zamawiającego jest większa od kary umownej, a także w przypadku, gdy szkoda powstała z przyczyn, dla których nie zastrzeżono kary umownej, Dostawca jest uprawniony do żądania odszkodowania na zasadach ogólnych, wynikających z przepisów Kodeksu cywilnego – niezależnie od tego, czy realizuje uprawnienia do otrzymania kary umownej.

3. Dostawca zapłaci karę umowną w terminie 14 dni od daty otrzymania od Zamawiającego żądania jej zapłaty, przelewem na rachunek bankowy wskazany przez Zamawiającego w żądaniu zapłaty.

XV. Zmiany umowy zawartej w wyniku przeprowadzonego postępowania o udzielenie zamówienia

Zmiany umowy zawartej w wyniku przeprowadzonego niniejszego postępowania są możliwe pod warunkiem, że nie wpłyną one negatywnie na realizację przedmiotu umowy oraz są przepisami prawa powszechnie obowiązującego.

Jakakolwiek umowa zawarta w konsekwencji niniejszego Zapytania ofertowego, powinna być wynikiem negocjacji i wzajemnej akceptacji warunków umowy pomiędzy Zamawiającym a Wykonawcą, w tym m.in. w zakresie terminu realizacji zamówienia, własności intelektualnej, poufności, wyboru prawa, ewentualnego odszkodowania z tytułu roszczeń osób trzecich pomiędzy Zamawiającym a Wykonawcą.

Zamawiający przewiduje możliwość dokonania zmian postanowień zawartej umowy w stosunku do treści oferty, na podstawie której dokonano wyboru wykonawcy, w następującym zakresie:

1. Rozwiązania umowy, bez regresu odszkodowawczego ze strony Wykonawcy, jeżeli z Zamawiającym zostanie rozwiązana umowa o dofinansowanie projektu przez Instytucję Pośredniczącą.

2. Zmiany harmonogramu realizacji umowy wynikającej z postanowień umowy Zamawiającego z Instytucją udzielającą wsparcia, jeżeli umowa ta została zmieniona po udzieleniu zamówienia.

3. Zmiana istotnych postanowień umowy w stosunku do treści oferty jest dopuszczalna w sytuacji, gdy nie była możliwa do przewidzenia na etapie podpisywania umowy.

4. Przesunięcie terminu wykonania przedmiotu zamówienia w przypadku, jeśli wystąpi zdarzenie zewnętrzne, niemożliwe do przewidzenia („siła wyższa"), w wyniku którego nie będzie możliwe dotrzymanie pierwotnego terminu wykonania przedmiotu zamówienia.

5. Zmiany w umowie mogą zostać dokonane, jeśli nastąpi na tyle istotna zmiana w procesie realizacji przedmiotu zamówienia (np. kwestie związane z łańcuchem dostaw), że realizacja umowy nie będzie mogła się odbyć zgodnie z pierwotną propozycją, a zmian tych nie dało się przewidzieć w momencie zawarcia umowy.

Ponadto dokonanie zmian postanowień zawartej umowy w stosunku do treści oferty wskazane jest w szczególności, gdy:

1. nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu umowy;
2. wynikną rozbieżności lub niejasności w umowie, których nie można usunąć w inny sposób, a zmiana będzie umożliwiać usunięcie rozbieżności i doprecyzowanie Umowy w celu jednoznacznej interpretacji jej postanowień przez Strony.

XVI. Sposób porozumiewania się Zamawiającego z Wykonawcami

Pytania dotyczące zapytania ofertowego można przesyłać wyłącznie poprzez <adres mailowy>.

Pytania, które wpłyną później niż na co najmniej 48 godzin przed terminem składania ofert pozostaną bez odpowiedzi.

XVII. Zamówienia uzupełniające

Zamawiający nie dopuszcza możliwości zamówień uzupełniających.

XVIII. Negocjacje

Zamawiający zastrzega możliwość podjęcia negocjacji z oferentem, którego Oferta zostanie uznana za najkorzystniejszą zgodnie z kryteriami określonymi w punkcie X.

Negocjacje zostaną przeprowadzone w sposób ustny w formie spotkania stacjonarnego w siedzibie Zamawiającego lub spotkania on-line z wykorzystaniem powszechnie dostępnych kanałów komunikacyjnych. Przeprowadzenie negocjacji oraz treść rozmów zostaną udokumentowane protokołem podpisanym przez każdą ze stron.

Negocjacjami objęte będą te aspekty oferty, które podlegały ocenie w ramach kryteriów określonych w punkcie XI niniejszego postępowania.

XIX. Informacje dodatkowe

1. Zamawiający wybierze jedną, najkorzystniejszą spośród złożonych ofert spełniających warunki udziału w postępowaniu o udzielenie zamówienia.
2. Zamawiający zastrzega sobie prawo do zmiany treści niniejszego zapytania ofertowego. Jeżeli zmiany będą mogły mieć istotny wpływ na składane w postępowaniu oferty, Zamawiający przedłuży termin składania ofert. Informacja o zmianach zostanie umieszczona tak jak ogłoszenie, na stronie: **www.introgaf.com.pl**
3. Cena w złożonej ofercie musi być wyrażona w PLN.
4. W przypadku, gdy wybrany Wykonawca odstąpi od podpisania umowy Zamawiający może podpisać umowę z kolejnym Wykonawcą, który w postępowaniu o udzielenie zamówienia uzyskał kolejną najwyższą liczbę punktów.
5. Zamawiający zastrzega sobie prawo unieważnienia postępowania o udzielenie zamówienia na każdym etapie bez podania przyczyny.

XX. Załączniki

1. Załącznik nr 1: Wzór formularza oferty.
2. Załącznik nr 2: Oświadczenie o braku podstaw do wykluczenia z udziału w postępowaniu.