Mielec, 10.08.2021 r.

ZAPYTANIE OFERTOWE NR 6/1.4/IIE/20
dotyczące działań związanych z przeprowadzeniem audytu bezpieczeństwa

Zamawiający:
WDM Computers Jarosławska Maria
Ul. Wolności 1
39-300 Mielec
NIP: 8171079395 REGON: 690411898

WDM Computers Jarosławska Maria zaprasza do złożenia oferty na realizację usługi doradczej polegającej na przeprowadzeniu audytu bezpieczeństwa w ramach projektu pn. „WZMOCNIENIE KONKURENCYJNOŚCI FIRMY WDM COMPUTERS DZIĘKI WDROŻENIU STRATEGII WZORNICZEJ" realizowanego w ramach Programu Operacyjnego Polska Wschodnia, Oś priorytetowa 1 Przedsiębiorcza Polska Wschodnia, Działanie 1.4 Wzór na konkurencję, Etap II.

Postępowanie prowadzone jest w formie zapytania ofertowego zgodnie z zasadą konkurencyjności obowiązującą w ramach Wytycznych w zakresie kwalifikowalności wydatków w zakresie Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020.

I. PRZEDMIOT ZAPYTANIA OFERTOWEGO

1. Przedmiotem zapytania ofertowego jest zrealizowanie usługi doradczej polegającej na przeprowadzeniu audytu bezpieczeństwa obejmującego następujące kategorie badań:
    a. Aplikacja webowa – testy bezpieczeństwa blackbox
    b. Serwer webowy/aplikacyjny – testy bezpieczeństwa blackbox
    c. API testy bezpieczeństwa blackbox
    d. Systemy operacyjne – weryfikacja konfiguracji whitebox
    e. Bazy danych – weryfikacja konfiguracji whitebox
    f. Serwery http – weryfikacja konfiguracji whitebox

Testy bezpieczeństwa platformy do wideo/telekonferencji, ze szczególnym uwzględnieniem błędów i podatności, które mogą mieć negatywny wpływ na poufność, integralność oraz dostępność danych przetwarzanych w aplikacji. Audyt powinien być realizowany z perspektywy użytkownika anonimowego (niezalogowanego) oraz z poziomu użytkownika posiadającego konto w aplikacji (zalogowanego klienta), a także administratorów.

Aplikacja wykorzystuje API GraphQL poprzez WebSocket, za pomocą którego przesyła ok. 60 mutacji, 30 zapytań i 20 subskrypcji.
Architektura systemu oparta jest na Dockerze – każdy kontener ma swoje własne środowisko, zatem audyt powinien obejmować każde środowisko z osobna.

WW. OPIS PRZEDMIOTU ZAMÓWIENIA NIE JEST CAŁKOWITY. ZAMAWIAJĄCY ZE WZGLĘDU NA KONIECZNOŚĆ OCHRONY TAJEMNICY PRZEDSIĘBIORSTWA ZASTRZEGA POUFNOŚĆ CZĘŚCI INFORMACJI I UDOSTĘPNI CHRONIONY ZAKRES JEDYNIE WYKONAWCOM, KTÓRZY ZOBOWIĄŻĄ SIĘ DO ZACHOWANIA W POUFNOŚCI PRZEDMIOTOWYCH INFORMACJI (podstawa prawna – sekcja 6.5.2. pkt 6 Wytycznych w zakresie kwalifikowalności).
Szczegółowy opis techniczny platformy do wideo/telekonferencji został umieszczony w Załączniku nr 5 do Zapytania ofertowego. Ze względu na to, iż informacje zawarte w załączniku nr 5 stanowią tajemnicę przedsiębiorstwa (w rozumieniu art. 11 ust. 4 ustawy z

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej"*

dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji), wykonawca, który chce złożyć ofertę w ramach niniejszego postępowania, zobowiązany jest do wcześniejszego podpisania Oświadczenia o zobowiązaniu do zachowania poufności (Załącznik nr 4 do zapytania ofertowego) i przesłania podpisanej kopii w formie skanu na adres mailowy: anna.pelc@confly.pl. Po otrzymaniu podpisanego oświadczenia, Zamawiający niezwłocznie (maksymalnie w terminie 1 dnia roboczego) prześle Załącznik nr 5 drogą elektroniczną na podany przez wykonawcę adres e-mail.

2. Zakres prac:

A) APLIKACJA WEBOWA – TESTY BEZPIECZEŃSTWA BLACKBOX

- Rekonesans aktywny i pasywny
  - Próby lokalizacji aplikacji dostępnej pod innym adresem (np. Aplikacja deweloperska w infrastrukturze dostawcy, publicznie dostępna aplikacja w wersji testowej)
  - Próby lokalizacji ukrytych katalogów i plików
  - Próby wywołania błędów/wyjątków w aplikacji
  - Poszukiwanie innych domen dostępnych na tym samym adresie IP co domena bazowa
  - Poszukiwanie wycieków danych (np. Technika Google Hacking, analiza pliku robots.txt).
- Poszukiwanie podatności
  - Podatności klasy injection (np. SQL injection, LDAP injection, XPATH injection, NoSQL injection).
  - Podatność XXS (Cross Site Scripting) – błędy typu reflected oraz stored.
  - Analiza problemów z uwierzytelnieniem i autoryzacją (np. próby dostępu do zasobów bez uwierzytelnienia, próby dostępu do zasobów administracyjnych przez zwykłego użytkownika, próby przełamania ekranów logowania – w tym próby brute force danych dostępowych).
  - Możliwości otrzymania nieautoryzowanego dostępu na poziomie systemu operacyjnego i uzyskanie w ten sposób dostępu do źródeł aplikacji, bazy danych, innych poufnych informacji.
  - Próby realizacji aplikacyjnych ataków typu DoS
  - Analiza błędów logicznych
  - Próby wykrycia innych podatności, np. Path Travesal, Open Redirection, Cross Site Request Forgery, Server Side Request Forgery , Server Side Template Injection.
  - Detekcja ogólnie znanego oprogramowania (aplikacje, biblioteki, systemy wspomagające).
  - Po wykryciu nieaktualnych wersji, próby lokalizacji znanych, istotnych podatności w kilku wybranych źródłach.

B) SERWER WEBOWY/APLIKACYJNY – TESTY BEZPIECZEŃSTWA BLACKBOX

- Poszukowanie podatności/problemów bezpieczeństwa
  - Analiza konfiguracji SSL (certyfikat, skonfigurowane algorytmy kryptograficzne)
  - Analiza dostępności ewentualnego panelu zarządzania komponentem
  - Próby użycia domyślnych/prostych par login/hasło do panelu zarządzania
  - Analiza ujawnienia dokładnej wesji komponentu (nagłówki odpowiedzi/komunikaty błędów)
  - Po udanym pozyskaniu dokładnego wersji komponentu, próba zlokalizowania publicznie dostępnych podatności w tej wersji

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*

- Analiza domyślnych aplikacji typu „example“ lub „demo“ (dostarczanych domyślnie z serwerem webowym/aplikacyjnym)
- Min. 5 siłowych prób wymuszania wyświetlania błędów/wyjątków (np. przesłanie nieprawidłowego adresu URL, wysłanie niepoprawnego requestu)
- Analiza domyślnej domeny skonfigurowanej na komponencie (np. poprzez odwołanie się do adresu IP)
- Analiza obsługi nietypowych metod http (TRACE, DEBUG, PUT, DELETE)

C) API – TESTY BEZPIECZEŃSTWA BLACKBOX

- Poszukiwanie podatności
  - Analiza dostępnych metod http
  - Próby obejść restrykcji nałożonych na metody http (np. wykorzystanie nagłówka X-HTTPMethod – Override)
  - Weryfikacja akceptowanych formatów wejściowych (JSON/XML/YAML/inne)
  - Próby wykrycia w przekazywanych parametrach podatności charakterystycznych dla rozwiązań webowych (w szczególności: Server Side Request Forgery, problemy z uwierzytelnieniem i autoryzacją , SQL injection, OS command execution)
  - Próba wykrycia podatnych bibliotek i konkretnych, znanych publicznie podatności w tych bibliotekach (na przykład: Jackson Remote Code Execution, Apache Struts REST plugin Remote Code Execution, Node-jose Library JSON Web Tokens Re-sign Vulnerability)
  - Analiza bezpieczeństwa JWT – próby ominięcia weryfikacji podpisu tokena, analiza ewenualnych wycieków danych w tokenach, weryfikacja sprawdzenia kluczowych deklaracji (claims)
  - Analiza wykorzystania kluczy API – analiza ewentualnej struktury klucza, bezpieczeństwo tworzenia i przekazywania klucza
  - Analiza nałożonego ograniczenia na ilość requestów do API (rate limit)

D) SYSTEMY OPERACYJNE – WERYFIKACJA KONFIGURACJI

- Sprawdzenie udostępnionych usług sieciowych
- Sprawdzenie działających w systemie procesów
- Sprawdzenie podziału przestrzeni dyskowej na odpowiednie strefy
- Sprawdzenie wdrożenia dodatkowych metod ochrony (np. dodatkowe mechanizmy ochronne zaimplementowane na poziomie kernela, mechanizmy typu jail, chroot, BSD security levels, host IDS, host Firewall, file integrity checker, system antywirusowy)
- Sprawdzenie uprawnień do najistotniejszych zasobów
- Sprawdzenie wdrożonego mechanizmu instalacji aktualizacji
- Sprawdzenie wdrożonego mechanizmu kopii zapasowych
- Sprawdzenie wdrożonego systemu logowania zdarzeń
- Sprawdzenie zabezpieczenia systemu w fazie boot
- Sprawdzenie wykorzystywanego sposobu zarządzania systemem
- Możliwość sprawdzenia systemów: Windows Server, Linux, BSD, AIX, Solaris.

E) BAZY DANYCH – WERYFIKACJA KONFIGURACJI

- Sprawdzenie wdrożenia podstawowych zasad hardeningowych bazy (np. dostępność domyślnych użytkowników quest, partycjonowanie bazy, składowanie logów, logowanie nietypowych zdarzeń, dostępność wybranych niebezpiecznych procedur/funkcji składowanych,

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*

- Sprawdzenie komunikacji z klientem bazodanowym – wykorzystanie mechanizmów kryptograficznych (logowanie się klienta oraz transfer danych)
- Ogólna recenzja architektury bazy (wykorzystane mechanizmy autoryzacji oraz uwierzytelniania; segmentacja uprawnień, wykorzystanie widoków; wykorzystanie procedur składowanych)
- Weryfikacja sposobu wykonywania kopii zapasowych
- Analiza sposobu udostępniania RDBMS na poziomie sieciowym
- Możliwość analiz baz: SQL Server, Oracle, MySQL, PostgreSqL

F) SERWERY HTTP – WERYFIKACJA KONFIGURACJI

- Sprawdzenie konfiguracji udostępnionych metod HTTP
- Sprawdzenie konfiguracji uwierzytelniania/autoryzacji
- Sprawdzenie sposobu obsługi błędów
- Sprawdzenie udostępniania informacji o wersji serwera http/zainstalowanych modułach
- Sprawdzenie zainstalowanych oraz aktywnych modułów w serwerze http.
- Sprawdzenie sposobu konfiguracji logowania zdarzeń
- Sprawdzenie konfiguracji protokołu HTTPS (np. obsługiwane wersje protokołu https, obsługiwane szyfry sesyjne, sposób dostępu do klucza prywatnego certyfikatu)
- Sprawdzenie wersji http serwera oraz próba lokalizacji znanych podatności w wykrytej wersji
- Sprawdzenie konfiguracji mechanizmu PROXY
- Serwery: Nginx

Rezultatem usługi winien być raport zawierający:

- Dokładne wskazanie metod naprawy podatności (lub w bezpieczeństwie) – dla wykrytych podatności o stopniu niebezpieczeństwa wysokim i krytycznym
- Sugerowane meetody naprawy podatności
- Szacowany poziom zagrożenia
- Prezentacja proof of concept realnego ataku na podatność (dla wybranych przypadków)

II. KODY CPV PRZEDMIOTU ZAMÓWIENIA

- 72810000-1 Usługi audytu komputerowego
- 72000000-5 Usługi informatyczne: konsultacyjne, opracowywania oprogramowania, internetowe i wsparcia

III. TERMIN WYKONANIA PRZEDMIOTU ZAMÓWIENIA

Okres realizacji zamówienia:

- wykonanie audytu bezpieczeństwa - maksymalnie do 24.09.2021 r.

TERMIN WSKAZANY POWYŻEJ JEST TERMINEM NIEPRZEKRACZALNYM.

IV. WARUNKI UDZIAŁU W POSTĘPOWANIU

1. Przeprowadzenie audytu bezpieczeństwa:

    a. O realizację powyżej opisanych usług mogą ubiegać się wszystkie podmioty, które posiadają udokumentowane doświadczenie w zakresie przeprowadzania audytu bezpieczeństwa aplikacji webowych – oferenci muszą spełniać łącznie wszystkie poniższe wymagania:

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*

i. W ciągu ostatnich 3 lat zrealizowali minimum 3 projekty polegające na przeprowadzeniu audytu bezpieczeństwa aplikacji webowych obejmującego pełny zakres niniejszego zapytania ofertowego.

Zamawiający dopuszcza przedstawienie tego załącznika w formie listy referencyjnej stanowiącej załącznik nr 3 do niniejszego zapytania ofertowego, jednakże w sposób jednoznaczny musi z niego wynikać powyższy warunek.

Warunek uznaje się za spełniony jeśli Wykonawca przedstawi dokumenty lub referencje (oświadczenia) od nabywców potwierdzające realizację ww. usługi.

W sytuacji jeśli Oferent nie przedstawi referencji lub innych dokumentów równoważnych potwierdzających realizację usług wskazanych w załączniku nr 3, oferta zostanie odrzucona z uwagi na niespełnienie warunków formalnych.

2. Wykonawca winien dysponować potencjałem kadrowym w zakresie niezbędnym do prawidłowego wykonania zamówienia w postaci minimum 2 osobowego zespołu, w skład którego wchodzą:

    a. 1 specjalista posiadający co najmniej 3 lata doświadczenia w zakresie realizacji testów penetracyjnych i audytów bezpieczeństwa

    b. 1 specjalista posiadający co najmniej 3 lata doświadczenia w bezpieczeństwie webaplikacji

Wymagania dodatkowe w stosunku do kadry:

- Każdy z członków zespołu winien posiadać co najmniej jeden z poniżej wskazanych lub równoważnych certyfikatów:
    - OSCP (Offensive Security Certified Professional)
    - CEH (Certified Ethical Hacker)
    - CISM (Certified Information Security Manager)
    - CISA(Certified Information System Auditor)
    - CISSP(Certified Information Systems Security Professional)

Wyżej wskazane wymagania muszą zostać spełnione łącznie przez każdego z ekspertów dedykowanych do realizacji zamówienia. Wymagania będą weryfikowane na podstawie przedłożonego CV osób. W CV powinny być wskazane wszystkie elementy wymagane dla doświadczenia kadry realizującej usługę.

Zmiana członków zespołu jest możliwa tylko i wyłącznie do czasu podpisania umowy, jednakże osoby te winny posiadać nie mniejsze kwalifikacje i doświadczenie jak te wskazane w pierwotnej ofercie. Każdy z członków zespołu winien spełniać wszystkie powyżej wskazane wymogi.

3. Nie są powiązane z Zamawiającym osobowo lub kapitałowo, tzn. nie występują 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:

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*

- uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej;
- posiadaniu co najmniej 10% udziałów lub akcji;
- pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika;
- pozostawaniu 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.

V. WARUNKI DODATKOWE

a) Prowadzenia dokumentacji zgodnie z wytycznymi obowiązującymi dla Programu Operacyjnego Polska Wschodnia 2014-2020.
b) Poddania się zapowiedzianym kontrolom przez PARP bądź inne instytucje zaangażowane w proces zarządzania funduszami UE.
c) Zmiana członków zespołu realizującego usługę będącą przedmiotem niniejszego zapytania ofertowego może być dokonana wyłącznie za pisemną zgodą Zamawiającego. Niedopuszczalna jest zmiana kadry na osoby o mniejszym doświadczeniu czy niższych kompetencjach. W sytuacjach losowych związanych ze zmianą kadry Wykonawca winien do pisma z prośbą o zmianę dostarczyć komplet obiektywnych dokumentów potwierdzających okoliczności losowe (np. zaświadczenie z pobytu w szpitalu).
d) W ramach wynagrodzenia za świadczoną usługę doradczą Wykonawca winien skalkulować wszelkie koszty ponoszone w związku z realizacją usługi m.in.:
    a. Wynagrodzenie Wykonawcy,
    b. Wydatki bieżące związane z pracą Wykonawcy – telefon, materiały biurowe, itp.
e) Zamawiający zastrzega sobie możliwość prowadzenia bieżącego nadzoru na każdym etapie realizacji zamówienia. Sposób i rodzaj nadzoru będą doprecyzowane przez podpisaniem umowy.

VI. WYMAGANE ZAŁĄCZNIKI

Oferent, aby mógł ubiegać się o realizację powyższego zlecenia musi dołączyć do formularza oferty następujące załączniki:

1. Aktualny wypis z KRS lub wypis z ewidencji działalności gospodarczej lub inny dokument zaświadczający o prowadzonej działalności, nie starszy niż trzy miesiące,
2. CV osób dedykowanych do realizacji usługi spełniających wymogi wskazane w niniejszym zapytaniu ofertowym. W przypadku zaangażowania osób na podstawie umów cywilnoprawnych należy przedstawić deklaracje tych osób w zakresie współpracy wraz z informacją, iż posiadają one wiedzę o składanej ofercie. Wymóg ten nie obowiązuje w przypadku wykazywania osób zatrudnionych na podstawie umów o pracę bądź właścicieli/wspólników Oferenta.
3. Oświadczenie o braku powiązań osobowych lub kapitałowych pomiędzy Oferentem a Zamawiającym – załącznik nr 2 do niniejszego zapytania ofertowego,
4. Zestawienie potwierdzające, iż Oferenci posiadają udokumentowane doświadczenie w zakresie realizacji działań związanych z przeprowadzaniem audytu bezpieczeństwa wraz z referencjami potwierdzającymi zrealizowanie usługi – załącznik nr 3 do niniejszego zapytania ofertowego.

Powyższe załączniki należy przedstawić w oryginale lub poświadczyć za zgodność z oryginałem. W przypadku przedstawienia kserokopii poświadczonych za zgodność z oryginałem wybrany Oferent będzie zobowiązany przed podpisaniem umowy do przedstawienia oryginałów tych dokumentów.

VII. KRYTERIUM WYBORU OFERT

Zamawiający wybierze ofertę najkorzystniejszą, zgodnie z poniższymi kryteriami:
Wybór oferty:
WYMOGI OGÓLNE

a. Cena – 60 punktów,
b. Ilość osób dedykowanych do realizacji usługi posiadających doświadczenie w przeprowadzaniu audytów bezpieczeństwa systemów pokrewnych* – 40 punktów,

Ocena oferty zostanie obliczona z wykorzystaniem następującego wzoru:
Ocena=A+B, gdzie:

Ad. A Kryterium Cena zostanie ocenione wg następującego wzoru:
(najniższa zaproponowana cena/cena badanej oferty) x 60
Maksymalna liczba punktów jakie może otrzymać oferta w tym kryterium wynosi 60 punktów.

Przy czym, jeżeli cena oferty wyda się rażąco niska w stosunku do przedmiotu zamówienia i budzić będzie wątpliwości Zamawiającego co do możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi przez Zamawiającego lub wynikającego z odrębnych przepisów, w szczególności jest niższa o 30% od wartości zamówienia lub średniej arytmetycznej cen wszystkich ofert, Zamawiający zwróci się o udzielenie wyjaśnień w określonym terminie dotyczących elementów oferty mających wpływ na wysokość ceny. Obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny, spoczywa na Wykonawcy. Zamawiający oceniając wyjaśnienia, bierze pod uwagę obiektywne czynniki, w szczególności oszczędność metody wykonania zamówienia, wybrane rozwiązania techniczne, wyjątkowo sprzyjające warunki wykonania zamówienia dostępne dla Wykonawcy oraz wpływ pomocy publicznej udzielonej na podstawie odrębnych przepisów. Zamawiający odrzuca ofertę wykonawcy, który nie złożył wyjaśnień lub jeżeli dokonana ocena wyjaśnień wraz z dostarczonymi dowodami potwierdza, że oferta zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia.

Ad. B Kryterium Ilość osób dedykowanych do realizacji usługi posiadających doświadczenie w przeprowadzaniu audytów bezpieczeństwa systemów pokrewnych* spełniających wymagania wskazane w zapytaniu ofertowym zostanie obliczone według wzoru:

*Przez system pokrewny rozumie się system realizujący tożsamy lub zbliżony zakres funkcjonalny.

(największa liczba osób / liczba osób badanej oferty) x 40 punktów

Spełnienie niniejszego warunku winno bezpośrednio wynikać z CV osób wskazanych do realizacji zamówienia.

Maksymalna liczba punktów jaką może otrzymać oferta w niniejszym kryterium wynosi 40 punktów.

Punkty uzyskane przez ofertę w ocenie oferty w Kryterium A, Kryterium B zostaną dodane do siebie i na tej podstawie zostanie obliczona łączna ocena oferty. Oferta w łącznej ocenie oferty może uzyskać maksymalnie 100 punktów.
Zamawiający udzieli zamówienia Wykonawcy, którego oferta uzyska największą ilość punktów w łącznej ocenie ofert (łączna suma punktów uzyskanych przez Wykonawcę w kryterium A i B). Punkty będą liczone z dokładnością do dwóch miejsc po przecinku.

VIII. SPOSÓB PRZYGOTOWANIA I SKŁADANIA OFERT

a) Ofertę należy przedstawić na załączonym do zapytania ofertowego formularzu,
b) Nieodłączny element oferty stanowią załączniki wymagane w pkt. VI niniejszego zapytania ofertowego,
c) Oferta może być wypełniona odręcznie lub komputerowo, jednak w przypadku wypełnienia odręcznego należy tego dokonać dużymi drukowanymi literami w sposób czytelny,
d) Oferta musi być podpisana przez osobę do tego upoważnioną, która widnieje w Krajowym Rejestrze Sądowym, wypisie z ewidencji działalności gospodarczej lub innym dokumencie zaświadczającym o jej umocowaniu prawnym,
e) Wszystkie strony oferty wraz z załącznikami muszą być trwale spięte,
f) Wszelkie poprawki lub zmiany w treści muszą być parafowane przez osobę podpisującą ofertę,
g) Każdy z Wykonawców może złożyć tylko jedną ofertę,
h) Zamawiający odrzuci ofertę niespełniającą warunków formalnych lub złożoną po terminie. Wykonawcy z tego tytułu nie przysługują żadne roszczenia,
i) Zamawiający nie dopuszcza składania ofert wariantowych i częściowych,
j) Zamawiający zastrzega sobie prawo do zmiany lub uzupełnienia treści niniejszego zapytania ofertowego przed upływem terminu na składanie ofert. Informacja o wprowadzeniu zmian lub uzupełnienia treści zapytania ofertowego zostanie przekazana Oferentom niezwłocznie w formie pisemnej (e-mail), jak również zostanie opublikowana na stronie internetowej Zamawiającego pod adresem https://www.wdm.pl/ oraz na portalu Baza Konkurencyjności pod adresem www.bazakonkurencyjnosci.gov.pl.
k) Zamawiający zastrzega sobie prawo odwołania lub unieważnienia oraz zakończenie postępowania bez wyboru Wykonawcy, bez podania przyczyn.
l) Administratorem danych osobowych, które znajdą się w formularzu ofertowym oraz załącznikach do oferty jest WDM Computers Jarosławska Maria, ul. Wolności 1, 39-300 Mielec (dalej WDM). WDM będzie przetwarzał dane osobowe w określonych celach, np. analizy przedłożonej oferty, zawarcia i realizacji umowy. Każdy oferent ma prawo zażądać dostępu do treści danych, które go dotyczą – poprawić je, zaktualizować, sprostować, przenieść, usunąć lub ograniczyć ich przetwarzanie. Każdy Oferent może też wnieść sprzeciw wobec przetwarzania udostępnionych danych osobowych. Każdy z Oferentów ma prawo do wycofania wyrażonej zgody. Wycofanie zgody nie ma wpływu na zgodność z prawem przetwarzania danych sprzed wycofania zgody. Jeśli Oferent ma wątpliwości, czy dane są prawidłowo przetwarzane przez WDM, to może wnieść skargę do Prezesa Urzędu Ochrony Danych Osobowych.

Jakiekolwiek odstępstwo od sposobu przygotowania oferty wraz z załącznikami jest równoznaczne z jej odrzuceniem, ze względu na niespełnienie kryteriów formalnych.

Ofertę należy złożyć na jeden z poniższych sposobów:

- Za pośrednictwem bazy konkurencyjności znajdującej się pod adresem https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl/
- Osobiście, pocztą, listem poleconym, kurierem na adres firmy Zamawiającego, tj. ul. Wolności 1, 39-300 Mielec.

Ofertę należy złożyć w zamkniętej kopercie, opieczętowanej pieczęcią firmową Oferenta, adresem Zamawiającego (podanym poniżej) oraz zapisem: OFERTA NA REALIZACJĘ AUDYTU BEZPIECZEŃSTWA.

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*

Oferta musi zostać złożona w nieprzekraczalnym terminie do dnia 18.08.2021 r., do godz. 15.00 w siedzibie firmy WDM COMPUTERS Jarosławska Maria, ul. Wolności 1, 39-300 Mielec. W przypadku złożenia oferty drogą pocztową, decyduje godzina wpływu oferty.

Otwarcie ofert nastąpi w dniu 18.08.2021 r. o godz. 16.00 w siedzibie WDM COMPUTERS Jarosławska Maria, ul. Wolności 1, 39-300 Mielec. Bezpośrednio przed otwarciem ofert Wykonawcy zostaną poinformowani o kwocie jaką Zamawiający przeznaczył na sfinansowanie zamówienia.

Wykonawcy zostaną poinformowani w trakcie spotkania o ilości złożonych ofert, nazwach i adresach Wykonawców, cenach poszczególnych, a także i informacjach dotyczących pozostałych kryteriów oceny ofert.
W razie jakichkolwiek dodatkowych pytań prosimy o kontakt z Panią Anną Pelc, e-mail: anna.pelc@confly.pl.

IX. TERMIN WAŻNOŚCI OFERTY

Wykonawca jest związany ofertą przez okres 40 dni kalendarzowych od dnia upływu terminu składania ofert.

X. WYKLUCZENIE

1. Z postępowania wyklucza się ponadto Wykonawcę, który:
   a. nie wykazał spełniania warunków udziału w postępowaniu, określonych w punkcie IV Zapytania ofertowego,
   b. z innymi Wykonawcami zawarł porozumienie mające na celu zakłócenie konkurencji między Wykonawcami w postępowaniu o udzielenie zamówienia, co zamawiający jest w stanie wykazać za pomocą stosownych środków dowodowych.
2. Z postępowania wyklucza się Wykonawców, którzy należąc do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, 1571, 1667), złożyli odrębne oferty, chyba, że wykażą, że istniejące między nimi powiązania nie prowadzą do zakłócenia konkurencji w postępowaniu o udzielenie zamówienia.
3. Zamówienie może być udzielone wyłącznie podmiotom, które nie są powiązane z Zamawiającym osobowo lub kapitałowo, tzn. nie występują 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:
   - Uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
   - Posiadaniu co najmniej 10% udziałów lub akcji,
   - Pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
   - Pozostawaniu 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.

XI. WARUNKI ZMIANY UMOWY

Zamawiający przewiduje możliwość wprowadzenia istotnych zmian postanowień zawartej umowy z wybranym Wykonawcą w stosunku do treści oferty, na podstawie której dokonano

wyboru Wykonawcy. Zmiany muszą być dokonywane w formie pisemnych aneksów do umowy podpisanej przez obie strony, pod rygorem nieważności.
Zamawiający przewiduje możliwość zmiany umowy, m.in. w przypadku:

- Gdy nastąpi zmiana powszechnie obowiązujących przepisów prawa w zakresie mającym wpływ na realizację przedmiotu umowy – w zakresie niezbędnym do dostosowania się do zaistniałych zmian,
- Wystąpienia okoliczności niezależnych od Wykonawcy na uzasadniony wniosek Wykonawcy, pod warunkiem, że zmiana ta wynika z okoliczności, których Wykonawca nie mógł przewidzieć na etapie składania oferty i nie jest przez niego zawiniona, przypadków siły wyższej, uznanej przez Zamawiającego jako zdarzenie nadzwyczajne, zewnętrzne, niemożliwe do zapobieżenia (np. decyzje administracyjne, państwowe).

Wszelkie zmiany, jakie strony chciałaby wprowadzić do postanowień zawartej umowy, wymagają pod rygorem nieważności formy pisemnej i zgody obu stron (w drodze pisemnego aneksu).

XII. ZAŁĄCZNIKI

1. Formularz ofertowy – Załącznik nr 1,
2. Oświadczenie o braku powiązań osobowych lub kapitałowych pomiędzy Oferentem a Zamawiającym – Załącznik nr 2,
3. Zestawienie potwierdzające, iż Oferenci posiadają udokumentowane doświadczenie – Załącznik nr 3.
4. Oświadczenie o zachowaniu poufności – załącznik nr 4.

Projekt realizowany w ramach Programu Operacyjnego Polska Wschodnia na lata 2014-2020

Tytuł projektu: *„Wzmocnienie konkurencyjności firmy WDM Computers dzięki wdrożeniu strategii wzorniczej”*