NIKiDW
NARODOWY INSTYTUT KULTURY
I DZIEDZICTWA WSI

NIKIDW.SSZ.26.23.2023.EG.1 Warszawa, 29 listopada 2023 r.

ZAPROSZENIE DO ZŁOŻENIA OFERTY

Zamawiający, Narodowy Instytut Kultury i Dziedzictwa Wsi, zaprasza do składania ofert na: **„Zakup 2 serwerów oraz niezbędnego oprogramowania”**.

1. **Zamawiający:**
   Narodowy Instytut Kultury i Dziedzictwa Wsi
   ul. Krakowskie Przedmieście 66
   00-322 Warszawa
   NIP: 5252804887
   REGON: 384655657

2. **Określenie przedmiotu zamówienia:**
   Przedmiotem zamówienia jest sprzedaż oraz dostawa infrastruktury informatycznej na potrzeby Narodowego Instytutu Kultury i Dziedzictwa Wsi. Szczegółowy opis przedmiotu zamówienia zawiera załącznik nr 1 do zaproszenia. Warunki realizacji zamówienia określa wzór umowy stanowiący załącznik nr 4 do zaproszenia.

3. **Termin realizacji zamówienia:**
   Zamówienie musi zostać zrealizowane do dnia 18 grudnia 2023 r.

4. **Miejsce realizacji zamówienia:**
   Wykonawca dostarcza przedmiot zamówienia do siedziby Narodowego Instytutu Kultury i Dziedzictwa Wsi (dalej: NIKiDW).

5. **Oferty częściowe**
   Zamawiający nie dopuszcza możliwości składania ofert częściowych. W przypadku złożenia oferty na część zamówienia oferta zostanie odrzucona.

6. **Wymagania wobec Wykonawcy**
   1) W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Wykonawca winien przedłożyć dokument pochodzący od importera tej technologii stwierdzający, iż przy jej wprowadzeniu na terytorium Polski, zostały dochowane wymogi właściwych przepisów prawa, w tym ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa

państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz.U. z 2004, Nr 229, poz. 2315 z późn zm.) oraz dokument potwierdzający, że importer posiada certyfikowany przez właściwą jednostkę system zarządzania jakością tzw. wewnętrzny system kontroli wymagany dla wspólnotowego systemu kontroli wywozu, transferu, pośrednictwa i tranzytu w odniesieniu do produktów podwójnego zastosowania.

2) Wykonawca winien przedłożyć oświadczenie producenta lub autoryzowanego dystrybutora producenta na terenie Polski, iż oferent posiada autoryzację producenta w zakresie sprzedaży oferowanych rozwiązań.

7. Opis sposobu przygotowania i złożenia oferty:

Do oferty należy dołączyć:

1. Formularz ofertowy – Załącznik nr 2 do Zaproszenia do złożenia oferty;
2. Formularz asortymentowo – cenowy – Załącznik nr 3 do Zaproszenia do złożenia oferty.
3. Dokumenty wskazane w Opisie przedmiotu zamówienia.
4. Szczegółową specyfikację techniczną oferowanego sprzętu (dotyczy zadania 1 i 2) oraz firewallu (zadanie 3).
5. Pełnomocnictwo do reprezentowania Wykonawcy – jeśli oferta zostanie podpisana przez osobę nie umocowaną jako reprezentant Wykonawcy w stosownym rejestrze (KRS, CEiDG, RIK itp.).

UWAGA: złożona oferta powinna być podpisana przez osobę upoważnioną do reprezentacji Wykonawcy. Jeśli oferta zostanie podpisana przez pełnomocnika, do oferty winno być dołączone Pełnomocnictwo podpisane przez osoby upoważnione do jego udzielenia.
Kompletną ofertę należy przesłać za pośrednictwem platformy zakupowej.

8. Termin składania ofert

Ofertę należy złożyć do dnia 07.12.2023 r. do godz.: 11:00 .

9. Opis sposobu obliczania ceny

1) Wykonawca jest zobowiązany skalkulować cenę oferty tak, aby obejmowała wszystkie koszty, jakie Wykonawca poniesie przy realizacji zamówienia.
2) Wykonawca zobowiązuje się do podania wartości cenowych zgodnie z Formularzem ofertowym oraz Formularzem asortymentowo – cenowym.
3) Ceny należy podać w polskich złotych z dokładnością do jednego grosza (dwóch miejsc po przecinku). Rozliczenia będą prowadzone w PLN.
4) Cena podana w Formularzu ofertowym – Załącznik nr 1 do Zaproszenia do złożenia oferty jest ceną ostateczną, niepodlegającą negocjacji.
5) Wyliczona cena oferty brutto będzie służyć do porównania złożonych ofert.
6) Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.

10. Opis Kryteriów oceny ofert, ich waga i sposób oceny:

Przy wyborze najkorzystniejszej oferty zamawiający będzie kierować się kryterium ceny.

11. Badanie i wyjaśnienie ofert.

1) W toku badania i oceny ofert Zamawiający może żądać od Wykonawcy wyjaśnień dotyczących treści złożonej oferty.
2) Zamawiający zastrzega sobie możliwość poprawy w ofercie:
   a. oczywistych pomyłek pisarskich,
   b. oczywistych pomyłek rachunkowych,
   c. innych omyłek, polegających na niezgodności oferty z dokumentami zamówienia, niepowodujących istotnych zmian w treści oferty.
3) W przypadku stwierdzenia ww. omyłek Zamawiający poprawi je we własnym zakresie, z uwzględnieniem konsekwencji dokonanych poprawek.
4) W toku badania złożonych ofert Zamawiający wezwie Wykonawcę do uzupełnienia dokumentów. Uzupełnieniu nie podlega Formularz ofertowy – Załącznik nr 1 do Zaproszenia do złożenia oferty oraz Formularz asortymentowo – cenowy – Załącznik nr 2 do Zaproszenia do złożenia oferty.

12. Informacje dotyczące wyboru najkorzystniejszej oferty.

Niniejsze zaproszenie do składania ofert nie stanowi zobowiązania Zamawiającego do udzielenia zamówienia. Zamawiający dokona wyboru oferty najkorzystniejszej na warunkach określonych w Zaproszeniu i przekaże oświadczenie o przyjęciu oferty wybranemu oferentowi za pośrednictwem poczty elektronicznej.

13. Informacje dotyczące unieważnienia postępowania.

Zamawiający unieważnia postępowanie w sytuacji:

1) gdy nie złożono żadnej oferty niepodlegającej odrzuceniu,
2) cena najkorzystniejszej oferty przewyższa kwotę jaką Zamawiający zamierza przeznaczyć na sfinansowanie zamówienia,
3) w trakcie procedury nastąpiło istotne naruszenie Regulaminu planowania, zasad organizacji i udzielania zamówień publicznych o wartości poniżej kwoty 130 000 zł netto w Narodowym Instytucie Kultury i Dziedzictwa Wsi, które miało lub mogło mieć wpływ na wynik postępowania,
4) wystąpiła istotna zmiana okoliczności powodująca, że prowadzenie postępowania lub wykonanie zamówienia nie leży w interesie Zamawiającego,
5) udzielenie zamówienia na oferowanych warunkach nie leży w interesie Zamawiającego.

14. Osoby wskazane do kontaktu:

Osobą upoważnioną do kontaktów ze strony Zamawiającego jest: Eliza Gajowczyk. Korespondencja będzie prowadzona przez Platformę zakupową.

15. Informacja dotycząca przetwarzania danych osobowych

Wypełniając obowiązek informacyjny wynikający z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego

przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r., Nr 119, str. 1) – dalej RODO, informujemy że:

1) Administratorem Państwa danych osobowych jest Narodowy Instytut Kultury i Dziedzictwa Wsi (NIKiDW) z siedzibą przy ul. Krakowskie Przedmieście 66, 00-322 Warszawa.
2) W sprawach związanych z przetwarzaniem danych przez Administratora można kontaktować się z wykorzystaniem powyższych danych adresowych.
3) Dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b i c RODO – w celu związanym z rozpatrzeniem Państwa oferty, w związku z ewentualnym zawarciem i wykonywaniem umowy na wykonanie zadania stanowiącego przedmiot zapytania ofertowego oraz ewentualnej kontroli uprawnionych organów.
4) W trakcie przetwarzania dane osobowe mogą być ujawnione osobom upoważnionym oraz podmiotom, które wykażą prawnie uzasadnione interesy.
5) W odniesieniu do danych osobowych nie będą podejmowane decyzje w sposób zautomatyzowany w myśl art. 22 RODO oraz nie będą profilowane.
6) Dane osobowe nie będą przekazywane do państw trzecich.
7) Dane osobowe będą przechowywane przez okres niezbędny do realizacji obowiązku prawnego ciążącego na administratorze, realizacji przedmiotu objętego zapytaniem ofertowym oraz realizacji i wykonania ewentualnej umowy.
8) Posiadają Państwo prawo do żądania dostępu do swoich danych osobowych, ich sprostowania, wniesienia sprzeciwu wobec przetwarzania danych osobowych oraz prawo do ich przeniesienia.
9) Przysługuje Państwu prawo wniesienia skargi do organu nadzorczego.

16. Załączniki:

1) Opis przedmiotu zamówienia
2) Formularz ofertowy
3) Formularz asortymentowo - cenowy
4) Projekt umowy

…….

Sporządził:

……
Data i podpis

Załącznik nr 1 do Zaproszenia do złożenia oferty

OPIS PRZEDMIOTU ZAMÓWIENIA

„Zakup 2 serwerów oraz niezbędnego oprogramowania”

Zadanie nr 1: Zakup oraz dostawa serwera wraz z niezbędnymi licencjami.

1) Parametry techniczne i wymagania:
   1) Obudowa wysokości 2U:
      a) obudowa serwerowa do montażu w szafie RACK 19" wraz z wysuwanymi szynami dedykowanymi do tego urządzenia przez producenta serwera;
      b) obudowa powinna posiadać dodatkowy przedni panel zamykany na klucz chroniący dyski twarde przed nieuprawnionym wyjęciem z serwera;
      c) obudowa powinna posiadać możliwość opcjonalnego dodania panelu z wyświetlaczem pozwalającym na wyświetlenie co najmniej adresu IP serwera;
      d) w obudowie powinien być zainstalowany zestaw redundantnych zasilaczy Hot Plug co najmniej 1100W o sprawności Titanium każdy oraz zestaw redundantnych wentylatorów; wentylatory powinny mieć możliwość wymiany podczas pracy serwera;
      e) obudowa powinna posiadać wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą;
      f) obudowa powinna posiadać możliwość instalacji interfejsu NFC do połączenia z aplikacją zarządzającą serwerem na telefonie; aplikacja zarządzająca powinna być dostępna na Android i iOS.
   2) Płyta główna:
      a) obsługująca co najmniej dwa procesory i co najmniej 24 sloty na pamięć taktowaną przynajmniej z częstotliwością 3200MT/s przy użyciu odpowiednich procesorów;
      b) musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym;
      c) musi posiadać zintegrowany z płytą główną moduł TPM w wersji co najmniej 2.0.
   3) Procesor – dwa procesory typu skalowalnego posiadające co najmniej po 8 rdzeni działające co najmniej z częstotliwością 2.8GHz i dające w teście Passmark dostępnym na stronie https://www.cpubenchmark.net/ wynik nie mniejszy niż 19200.
   4) Pamięć RAM – 128 GB pamięci RAM w modułach 32GB RDIMM przygotowanych na działanie z częstotliwością co najmniej 3200MT/s.
   5) Dyski:
      a) serwer powinien mieć możliwość instalacji co najmniej 12 dysków 3.5";
      b) w serwerze powinny być zainstalowane dwa dyski 480GB SSD skonfigurowane fabrycznie w RAID1 oraz cztery dyski 4TB i cztery dyski 8TB SAS.
   6) Kontrolery:
      a) serwer powinien posiadać kontroler RAID umożliwiający konfigurację RAID 0,1,5,10,50,6 posiadający co najmniej 8GB pamięci cache zabezpieczonej przed awarią prądu;
      b) serwer powinien posiadać przewidzianą przez producenta możliwość dodania modułu pozwalającego na startowanie systemu z kart SD lub dysków M.2 skonfigurowanych w RAID1.
   7) Sieć:
      a) na płycie głównej powinna być zainstalowana karta sieciowa 1GB BT oraz dwuportowa karta 10GB w standardzie Base-T;
      b) karty nie mogą zajmować slotu PCIe.

8) Karta zarządzająca – niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet, umożliwiająca:
   a) zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
   b) szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
   c) podmontowanie zdalnych wirtualnych napędów;
   d) wirtualną konsolę z dostępem do myszy, klawiatury;
   e) wsparcie dla IPv6 - wsparcie dla SNMP; IPMI2.0, VLAN tagging, SSH;
   f) zdalne monitorowanie w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz;
   g) zdalne ustawienia limitu poboru prądu przez konkretny serwer;
   h) integrację z Active Directory;
   i) obsługę przez ośmiu administratorów jednocześnie;
   j) wsparcie dla automatycznej rejestracji DNS - wsparcie dla LLDP;
   k) wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej;
   l) podłączenie lokalne poprzez złącze RS-232;
   m) zarządzanie bezpośrednie poprzez złącze microUSB umieszczone na froncie obudowy;
   n) monitorowanie zużycia dysków SSD;
   o) monitorowanie z jednej konsoli min. 100 serwerami fizycznymi;
   p) automatyczne zgłaszanie alertów do centrum serwisowego producenta;
   q) automatyczny update firmware dla wszystkich komponentów serwera;
   r) przywrócenie poprzednich wersji firmware;
   s) eksport/import konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON;
   t) zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych;
   u) automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.

2) Certyfikaty:
   1) Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001.
   2) Serwer musi posiadać deklarację CE.
   3) Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” Microsoft Windows 2019 i Windows 2022.

3) Warunki gwarancji:
   1) 3 lata gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia – zgłoszenia przyjmowane 7 dni w tygodniu w trybie 24/7.
   2) Gwarancja musi obejmować całość rozwiązania, Zamawiający nie dopuszcza aby jakaś część przedmiotu zamówienia nie podlegała gwarancji.
   3) Możliwość zgłaszania awarii poprzez ogólnopolską linię telefoniczną producenta.
   4) Wymagana jest możliwość rozszerzenia gwarancji do 7-miu lat.
   5) W przypadku naprawy dysku – uszkodzony dysk zostaje u klienta.
   6) Podczas trwania gwarancji producent powinien zapewnić narzędzia i procesy do proaktywnej oceny stanu technicznego oraz automatycznego zgłaszania usterek bez ingerencji człowieka.
   7) Wymagana jest możliwość skorzystania z pomocy wsparcia producenta za pomocą komunikatora np. Messenger, Teams, WhatsApp.
   8) Firma serwisująca musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.

9) Wymagana jest możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera.
10) Wymagana jest możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

4) Z uwagi na kompatybilność z już istniejącymi systemami, na serwerze powinien być zainstalowany system Microsoft Windows Server standard w najnowszej wersji z licencjami pozwalającymi na uruchomienie czterech maszyn wirtualnych.

Zadanie nr 2: Zakup oraz dostawa serwera NAS wraz z niezbędnymi licencjami.

1) Parametry techniczne i wymagania:
    1) Procesor:
        a) procesor 64 bit Intel x86 o takowaniu nie mniejszym niż 2.8 GHz;
        b) nie mniej niż 8 rdzeni;
    2) Pamięć RAM:
        a) nie mniej niż 8GB;
        b) minimum 2 sloty;
        c) możliwość rozszerzenia do minimum 64G.
    3) Pamięć Flash – nie mniej niż 5GB.
    4) Gniazdo M.2 – minimum 2;
    5) Liczba zatok na dyski twarde – minimum 8;
    6) Obsługiwane dyski twarde – 3.5" HDD SATA oraz 2.5" HDD SATA oraz 2.5" SSD SATA;
    7) Możliwość podłączenia modułu rozszerzającego – tak, co najmniej 1;
    8) Porty LAN 2,5 GbE – minimum 2;
    9) Diody LED – minimum Stan, LAN, HDD, USB;
    10) Porty USB 3.2 Gen 1 – minimum 4;
    11) Port PCiE – tak, minimum 2 Gen3;
    12) Przyciski – reset, zasilanie;
    13) Typ obudowy – RACK, 2U;
    14) Dopuszczalna temperatura pracy – od 0 do 40˚C;
    15) Wilgotność względna podczas pracy – 5-95% R.H;
    16) Zasilanie – redundantne, pojedynczy zasilacz do 250W, 100-240 V;
    17) Zainstalowane dyski – 6 szt. dysków 6Gb/s dedykowanych do pracy ciągłej w urządzeniach NAS.
2) Specyfikacja oprogramowania:
    1) Wymagana agregacja łączy.
    2) Obsługiwane systemy plików:
        a) dyski wewnętrzne EXT4;
        b) dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+.
    3) Szyfrowanie wolumenów – tak, min AES 256.
    4) Zarządzanie dyskami:
        a) pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD;
        b) obsługa Hot Spare per grupa RAID oraz global hot spare;
        c) rozszerzanie pojemności Online RAID;
        d) migracja poziomów Online RAID;
        e) HDD S.M.A.R.T.;
        f) skanowanie uszkodzonych bloków (pliku);
        g) przywracanie macierzy RAID;

h) obsługa map bitowych;
i) pula pamięci masowej;
j) obsługa migawek;
k) obsługa replikacji migawek.

5) Wbudowana obsługa iSCSI:
   a) obsługa LUN Mapping & Masking;
   b) obsługa MPIO;
   c) migawka LUN;
   d) kopia zapasowa iSCSI LUN.
6) Zarządzanie prawami dostępu:
   a) ograniczenie dostępnej pojemności dysku dla użytkownika;
   b) importowanie listy użytkowników;
   c) zarządzanie kontami użytkowników;
   d) zarządzanie grupą użytkowników;
   e) zarządzanie współdzieleniem w sieci;
   f) tworzenie użytkowników za pomocą makr;
   g) obsługa zaawansowanych uprawnień dla podfolderów, Windows ACL.
7) Obsługa Windows AD:
   a) logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web;
   b) funkcja serwera LDAP.
8) Funkcje backup:
   a) oprogramowanie do tworzenia kopii plików, opracowane przez producenta urządzenia dla systemów Windows;
   b) backup na zewnętrzne dyski twarde.
9) Współpraca z zewnętrznymi dostawcami usług chmury – przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box.
10) Darmowe aplikacje na urządzenia mobilne:
   a) monitoring / zarządzanie / współdzielenie plików / obsługa kamer / odtwarzacz muzyki;
   b) dostępne na systemy iOS oraz Android.
11) Minimum obsługiwane serwery:
   a) serwer plików;
   b) serwer FTP;
   c) serwer WEB;
   d) serwer kopii zapasowych;
   e) serwer multimediów UPnP;
   f) serwer pobierania (Bittorrent / HTTP / FTP);
   g) serwer monitoringu.
12) VPN:
   a) VPN client/VPN server;
   b) obsługa PPTP, OpenVPN;
13) Administracja systemu:
   a) połączenia HTTP/HTTPS;
   b) powiadamianie przez e-mail (uwierzytelnianie SMTP);
   c) powiadamianie przez SMS;
   d) ustawienia inteligentnego chłodzenia;
   e) DDNS oraz zdalny dostęp w chmurze;
   f) SNMP (v2 & v3);
   g) obsługa UPS z zarządzaniem SNMP (USB);

h) obsługa sieciowej jednostki UPS;
i) monitor zasobów;
j) kosz sieciowy dla CIFS/SMB oraz AFP;
k) monitor zasobów systemu w czasie rzeczywistym;
l) rejestr zdarzeń;
m) system plików dziennika;
n) całkowity rejestr systemowy (poziom pliku);
o) zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line;
p) aktualizacja oprogramowania;
q) kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu.

14) Wirtualizacja:
a) wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android;
b) dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5;
c) funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.

15) Konteneryzacja – możliwość uruchomienia wirtualnych kontenerów dla LXD i Docker.

16) Zabezpieczenia:
a) filtracja IP;
b) ochrona dostępu do sieci z automatycznym blokowaniem;
c) połączenie HTTPS;
d) FTP z SSL/TLS (Explicit);
e) obsługa SFTP;
f) szyfrowanie AES 256-bit;
g) szyfrowana zdalna replikacja (Rsync poprzez SSH);
h) import certyfikatu SSL;
i) powiadomienia o zdarzeniach za pośrednictwem Email i SMS.

17) Możliwość instalacji dodatkowego oprogramowania:
a) tak, sklep z aplikacjami;
b) możliwość instalacji z paczek.

3) Gwarancja – co najmniej 3 lata gwarancji.

Zadanie nr 3: Zakup oraz dostawa firewallu do rozdzielenia VPN od sieci.

1. Wymagania ogólne:
1) System bezpieczeństwa realizuje wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Poszczególne elementy wchodzące w skład systemu bezpieczeństwa mogą być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej muszą być zapewnione niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. Dla wszystkich funkcji systemu musi być dostarczony dokument potwierdzony przez producenta lub autoryzowanego dystrybutora o gotowości świadczenia usług wsparcia w języku polskim oraz bezpłatnej obsługi procesu wymiany uszkodzonego urządzenia.
2) System realizujący funkcję Firewall zapewnia pracę w jednym z trzech trybów:
a) routera z funkcją NAT;
b) transparentnym;
c) monitorowania na porcie SPAN.

3) System umożliwia budowę minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie:
   a) Routingu;
   b) Firewall'a;
   c) IPSec VPN;
   d) antywirus;
   e) IPS;
   f) kontroli aplikacji.
4) Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
5) System wspiera protokoły IPv4 oraz IPv6 w zakresie:
   a) Firewall;
   b) ochrony w warstwie aplikacji;
   c) protokołów routingu dynamicznego.

2. Redundancja, monitoring i wykrywanie awarii
   1) W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – istnieje możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach system firewall zapewnia funkcję synchronizacji sesji.
   2) Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
   3) Monitoring stanu realizowanych połączeń VPN.
   4) System umożliwia agregację linków statyczną oraz w oparciu o protokół LACP. Ponadto daje możliwość tworzenia interfejsów redundantnych.
3. Interfejsy, dysk, zasilanie:
   1) System realizujący funkcję Firewall dysponuje co najmniej 10 portami Gigabit Ethernet RJ-45.
   2) System Firewall posiada wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
   3) System Firewall pozwala skonfigurować co najmniej 200 interfejsów wirtualnych, definiowanych jako VLAN'y w oparciu o standard 802.1Q.
   4) System jest wyposażony w zasilanie AC.

4) Parametry wydajnościowe:
   1) W zakresie Firewall'a obsługa nie mniej niż 700 tys. jednoczesnych połączeń oraz 32 tys. nowych połączeń na sekundę.
   2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
   3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
   4) Wydajność szyfrowania IPSec VPN protokołem AES z kluczem 128 nie mniej niż 6 Gbps.
   5) 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 1.3 Gbps.
   6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 650 Mbps.
   7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 600 Mbps.
4. Funkcje Systemu Bezpieczeństwa – w ramach systemu ochrony są realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:
   1) Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.

2) Kontrola Aplikacji.
3) Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4) Ochrona przed malware.
5) Ochrona przed atakami - Intrusion Prevention System.
6) Kontrola stron WWW.
7) Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8) Zarządzanie pasmem (QoS, Traffic shaping).
9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. Konieczne są co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11) Inspekcja (minimum: IPS) ruchu szyfrowanego protokołem SSL/TLS, minimum dla następujących typów ruchu: HTTP (w tym HTTP/2), SMTP, FTP, POP3.
12) Funkcja lokalnego serwera DNS z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.
13) Rozwiązanie posiada wbudowane mechanizmy automatyzacji polegające na wykonaniu określonej sekwencji akcji (takich jak zmiana konfiguracji, wysłanie powiadomień do administratora) po wystąpieniu wybranego zdarzenia (np. naruszenie polityki bezpieczeństwa).

5. Polityki, Firewall:
   1) Polityka Firewall uwzględnia:
      a) adresy IP;
      b) użytkowników;
      c) protokoły;
      d) usługi sieciowe;
      e) aplikacje lub zbiory aplikacji;
      f) reakcje zabezpieczeń;
      g) rejestrowanie zdarzeń.
   2) System realizuje translację adresów NAT:
      a) źródłowego i docelowego;
      b) translację PAT;
      c) translację jeden do jeden oraz jeden do wielu;
      d) dedykowany ALG (Application Level Gateway) dla protokołu SIP.
   3) W ramach systemu istnieje możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
   4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie URL, adresy IP.
   5) Polityka firewall umożliwia filtrowanie ruchu w zależności od kraju, do którego przypisane są adresy IP źródłowe lub docelowe.
   6) Możliwość ustawienia przedziału czasu, w którym dana reguła w politykach firewall jest aktywna.
   7) Element systemu realizujący funkcję Firewall integruje się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to, aby użyć ich przy budowaniu polityk kontroli dostępu.
      a) Amazon Web Services (AWS);
      b) Microsoft Azure;
      c) Cisco ACI;
      d) Google Cloud Platform (GCP);
      e) OpenStack;

f) VMware NSX;
g) Kubernetes.

6. Połączenia VPN:
   1) System umożliwia konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji zapewnia:
      a) wsparcie dla IKE v1 oraz v2;
      b) obsługę szyfrowania protokołem minimum AES z kluczem 128 oraz 256 bitów w trybie pracy Galois/Counter Mode(GCM);
      c) obsługę protokołu Diffie-Hellman grup 19, 20;
      d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh;
      e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site;
      f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności;
      g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego;
      h) wsparcie dla następujących typów uwierzytelniania: pre-shared key, certyfikat.
      i) możliwość ustawienia maksymalnej liczby tuneli IPSec negocjowanych (nawiązywanych) jednocześnie w celu ochrony zasobów systemu;
      j) możliwość monitorowania wybranego tunelu IPSec site-to-site i w przypadku jego niedostępności automatycznego aktywowania zapasowego tunelu;
      k) obsługę mechanizmów: IPSec NAT Traversal, DPD, Xauth;
      l) mechanizm „Split tunneling" dla połączeń Client-to-Site.
   2) System umożliwia konfigurację połączeń typu SSL VPN. W zakresie tej funkcji zapewnia:
      a) pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki; w tym zakresie system zapewnia stronę komunikacyjną działającą w oparciu o HTML 5.0;
      b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta;
      c) producent rozwiązania posiada w ofercie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN. Oprogramowanie klienckie vpn jest dostępne jako opcja i nie jest wymagane w implementacji.
7. Routing i obsługa łączy WAN – w zakresie routingu rozwiązanie zapewnia obsługę:
   1) Routingu statycznego.
   2) Policy Based Routingu (w tym: wybór trasy w zależności od adresu źródłowego, protokołu sieciowego, oznaczeń Type of Service w nagłówkach IP).
   3) Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2 (w tym RIPng), OSPF (w tym OSPFv3), BGP oraz PIM.
   4) Możliwość filtrowania tras rozgłaszanych w protokołach dynamicznego routingu.
   5) ECMP (Equal cost multi-path) – wybór wielu równoważnych tras w tablicy routingu.
   6) BFD (Bidirectional Forwarding Detection).
   7) Monitoringu dostępności wybranego adresu IP z danego interfejsu urządzenia i w przypadku jego niedostępności automatyczne usunięcie wybranych tras z tablicy routingu.
8. Funkcje SD-WAN:
   1) System umożliwia wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
   2) SD-WAN wspiera zarówno interfejsy fizyczne jak i wirtualne (w tym VLAN, IPSec).
9. Zarządzanie pasmem:
   1) System Firewall umożliwia zarządzanie pasmem poprzez określenie: maksymalnej i gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.

2) System daje możliwość określania pasma dla poszczególnych aplikacji.
3) System pozwala zdefiniować pasmo dla wybranych użytkowników niezależnie od ich adresu IP.
4) System zapewnia możliwość zarządzania pasmem dla wybranych kategorii URL.

10. Ochrona przed malware:
    1) Silnik antywirusowy umożliwia skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
    2) Silnik antywirusowy zapewnia skanowanie następujących protokołów: HTTP, HTTPS, FTP, POP3, IMAP, SMTP, CIFS.
    3) System umożliwia skanowanie archiwów, w tym co najmniej: Zip, RAR. W przypadku archiwów zagnieżdżonych istnieje możliwość określenia, ile zagnieżdżeń kompresji system będzie próbował zdekompresować w celu przeskanowania zawartości.
    4) System umożliwia blokowanie i logowanie archiwów, które nie mogą zostać przeskanowane, ponieważ są zaszyfrowane, uszkodzone lub system nie wspiera inspekcji tego typu archiwów.
    5) System dysponuje sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
    6) Baza sygnatur musi być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    7) System współpracuje z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. Konieczne jest zastosowanie platformy typu Sandbox wraz z niezbędnymi serwisami lub licencjami upoważniającymi do korzystania z usługi typu Sandbox w chmurze.
    8) System zapewnia usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
    9) Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.
    10) Możliwość uruchomienia ochrony przed malware dla wybranego zakresu ruchu.
11. Ochrona przed atakami:
    1) Ochrona IPS opiera się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych.
    2) System chroni przed atakami na aplikacje pracujące na niestandardowych portach.
    3) Baza sygnatur ataków zawiera minimum 5000 wpisów i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
    4) Administrator systemu ma możliwość definiowania własnych wyjątków oraz własnych sygnatur.
    5) System zapewnia wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS.
    6) Mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty).
    7) Możliwość kontrolowania długości nagłówka, ilości parametrów URL oraz Cookies dla protokołu http.
    8) Wykrywanie i blokowanie komunikacji C&C do sieci botnet.
    9) Możliwość uruchomienia ochrony przed atakami dla wybranych zakresów komunikacji sieciowej. Mechanizmy ochrony IPS nie mogą działać globalnie.
12. Kontrola aplikacji:
    1) Funkcja Kontroli Aplikacji umożliwia kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
    2) Baza Kontroli Aplikacji zawiera minimum 2000 sygnatur i jest aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.

3) Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) są kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.
4) Baza sygnatur zawiera kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5) Administrator systemu ma możliwość definiowania wyjątków oraz własnych sygnatur.
6) Istnieje możliwość blokowania aplikacji działających na niestandardowych portach (np. FTP na porcie 2021).
7) System daje możliwość określenia dopuszczalnych protokołów na danym porcie TCP/UDP i blokowania pozostałych protokołów korzystających z tego portu (np. dopuszczenie tylko HTTP na porcie 80).

13. Kontrola WWW:
1) Moduł kontroli WWW korzysta z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2) W ramach filtra WWW są dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3) Filtr WWW dostarcza kategorii stron zabronionych prawem np.: Hazard.
4) Administrator ma możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5) Filtr WWW umożliwia statyczne dopuszczanie lub blokowanie ruchu do wybranych stron WWW, w tym pozwala definiować strony z zastosowaniem wyrażeń regularnych (Regex).
6) Filtr WWW daje możliwość wykonania akcji typu „Warning" – ostrzeżenie użytkownika wymagające od niego potwierdzenia przed otwarciem żądanej strony.
7) Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
8) Administrator ma możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania WWW.
9) System pozwala określić, dla których kategorii URL lub wskazanych URL nie będzie realizowana inspekcja szyfrowanej komunikacji.

14. Uwierzytelnianie użytkowników w ramach sesji:
1) System Firewall umożliwia weryfikację tożsamości użytkowników za pomocą:
   a) haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu;
   b) haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP;
   c) haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2) System daje możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego.
3) System umożliwia budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS, API lub SYSLOG w tym procesie.
4) Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

15. Zarządzanie:
1) Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i mogą współpracować z dedykowanymi platformami centralnego zarządzania i monitorowania.

2) Komunikacja elementów systemu zabezpieczeń z platformami centralnego zarządzania jest realizowana z wykorzystaniem szyfrowanych protokołów.
3) Istnieje możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4) System współpracuje z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwia przekazywanie statystyk ruchu za pomocą protokołów Netflow lub sFlow.
5) System daje możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewall posiada wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7) Element systemu realizujący funkcję Firewall umożliwia wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.
8) Możliwość przypisywania administratorom praw do zarządzania określonymi częściami systemu (RBM).
9) Możliwość zarządzania systemem tylko z określonych adresów źródłowych IP.

16. Logowanie:
    1) Elementy systemu bezpieczeństwa realizują logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub konieczne jest zastosowanie komercyjnego systemu logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
    2) W ramach logowania element systemu pełniący funkcję Firewall zapewnia przekazywanie danych o: zaakceptowanym ruchu, blokowanym ruchu, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Ponadto zapewnia możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
    3) Logowanie obejmuje zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa.
    4) Możliwość włączenia logowania per reguła w polityce firewall.
    5) System zapewnia możliwość logowania do serwera SYSLOG.
    6) Przesyłanie SYSLOG do zewnętrznych systemów jest możliwe z wykorzystaniem protokołu TCP oraz szyfrowania SSL/TLS.
17. Serwisy i licencje – do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów wymagane są licencje:
    1) Kontrola Aplikacji.
    2) IPS.
    3) Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android).
    4) Analiza typu Sandbox cloud.
    5) Antyspam.
    6) Web Filtering.
    7) Bazy reputacyjne adresów IP/domen na okres 12 miesięcy.
18. Gwarancja oraz wsparcie:
    1) Dostarczone rozwiązanie musi być objęte rozszerzonym wsparciem technicznym gwarantującym - w przypadku awarii - odbiór i zwrot urządzenia do producenta bez dodatkowych kosztów, realizowanym przez producenta rozwiązania lub autoryzowanego dystrybutora przez okres wymaganej gwarancji, przez okres 12 miesięcy.

2) Do zamawianego sprzętu Wykonawca zapewni: usługi wsparcia technicznego świadczone przez producenta lub Autoryzowanego Dystrybutora Producenta świadczona w języku polskim w zakresie:
   a) obsługa procesu RMA u producenta;
   b) zdalna pomoc w skonfigurowaniu urządzenia do współpracy z aktualnymi bazami funkcji ochronnych i serwisów producenta;
   c) jednorazowa podstawowa konfiguracja platformy realizowana przez inżyniera z najwyższym dostępnym poziomem certyfikacji technicznej oferowanego producenta system realizującego funkcję Firewall;
   d) dostęp do szkolenia wideo prezentującego najlepsze praktyki współpracy z suportem producenta systemu realizującego funkcję Firewall.

   Dostęp do usługi musi być świadczony przez dedykowaną infolinię (należy podać numer telefonu) oraz przez dedykowany moduł internetowy (należy podać adres).
   Usługa ta ma być świadczona prze podmiot posiadający certyfikat ISO 9001 w zakresie świadczenia usług serwisowych.

Do oferty należy załączyć oświadczenie producenta lub Autoryzowanego Dystrybutora o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001 oraz co najmniej 4 certyfikaty inżynierów producenta lub Autoryzowanego Dystrybutora producenta systemu realizującego funkcję Firewall.

Załącznik nr 2 do Zaproszenia do złożenia oferty

Wykonawca:

……

(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)

reprezentowany przez:

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

FORMULARZ OFERTOWY

Zamawiający:
Narodowy Instytut Kultury i Dziedzictwa Wsi
ul. Krakowskie Przedmieście 66
00-322 Warszawa

Odpowiadając na Zaproszenie do złożenia oferty na: **„Zakup 2 serwerów oraz niezbędnego oprogramowania”:**

1. **SKŁADAM OFERTĘ** na dostawę infrastruktury informatycznej, na łączną kwotę: ……..... zł brutto (słownie: ……..…….…….…. zł), w tym podatek VAT ……..… zł, kwota …….……..zł netto, obliczoną zgodnie z załączonym Formularzem asortymentowo – cenowym.

2. **AKCEPTUJĘ** termin realizacji zamówienia do dnia 18 grudnia 2023 r.

3. **OŚWIADCZAM**, że zapoznałem/zapoznałam się z Zaproszeniem do złożenia oferty, opisem przedmiotu zamówienia oraz projektem Umowy i uznaję się za związanego/związaną określonymi w nich postanowieniami i zasadami postępowania.

4. **AKCEPTUJĘ** warunki płatności, tj. 14 dni od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury, wraz z protokołem odbioru.

5. **UWAŻAM SIĘ** za związanego/związaną niniejszą ofertą przez okres 30 dni od upływu terminu składania ofert.

6. **OŚWIADCZAM**, iż niniejsza oferta oraz wszelkie załączniki do niej są jawne i nie zawierają informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

7. **WSZELKĄ KORESPONDENCJĘ** w sprawie niniejszego postępowania należy kierować do ……, e-mail: .....

8. **W PRZYPADKU** wyboru mojej oferty osobą umocowaną do podpisania umowy jest ……...……...……

9. **W PRZYPADKU** wyboru mojej oferty osobą odpowiedzialną za realizację przedmiotu zamówienia jest ……..……., tel.: ……..… e-mail …….

10. Załączniki do oferty:
   1) ……
   2) ……

……., dnia …….. r. ……..

(podpis Wykonawcy)

Załącznik nr 4 do Zaproszenia do złożenia oferty

UMOWA NR xxx/2023/NIKiDW

Umowa zawarta jest w Warszawie w dniu ……. grudnia 2023 r. pomiędzy:

Narodowym Instytutem Kultury i Dziedzictwa Wsi z siedzibą w Warszawie (00-322), przy ul. Krakowskie Przedmieście 66, wpisanym do Rejestru Instytucji Kultury, dla których organizatorem jest Minister Rolnictwa i Rozwoju Wsi, pod numerem 3, NIP: 525-280-48-87, Regon: 384655657, zwanym dalej **Zamawiającym**, reprezentowanym przez:
Katarzynę Saks - Dyrektor,
a
……
……
zwanym dalej **Wykonawcą.**
W wyniku postępowania o udzielenie zamówienia publicznego prowadzonego na podstawie Regulaminu planowania zasad organizacji i udzielania zamówień publicznych o wartości poniżej kwoty 130 000,00 zł netto w NIKiDW, została sporządzona umowa o następującej treści:

§ 1
Przedmiot Umowy

1. Zamawiający powierza, a Wykonawca przyjmuje do wykonania zamówienie pn.: „Zakup 2 serwerów oraz niezbędnego oprogramowania”, w zakresie i na warunkach wskazanych w Umowie, w szczególności zgodnie z Opisem Przedmiotu Zamówienia, stanowiącym Załącznik nr 1 do Umowy (dalej: Przedmiot Umowy).
2. Wykonawca zrealizuje Przedmiot Umowy z użyciem własnych pracowników, własnego sprzętu i materiałów oraz innych niezbędnych środków.
3. Wykonanie Przedmiotu Umowy polega w szczególności na:
   1) dostarczeniu i rozładunku wszystkich urządzeń;
   2) należytym zabezpieczeniu dostarczonych urządzeń przed kradzieżą, uszkodzeniem lub innymi czynnikami mogącymi wpłynąć na jakość dostarczonych materiałów i urządzeń;
   3) przedłożeniu kompletnej dokumentacji i certyfikatów dla wszystkich zastosowanych urządzeń, osprzętu czy innych rozwiązań systemowych.

   Wszystkie dostarczone urządzenia muszą być fabrycznie nowe (nieużywane), wyprodukowane nie wcześniej niż w roku poprzedzającym zawarcie Umowy, zapakowane w oryginalne opakowania producenta, kompletne, posiadać w szczególności niezbędne okablowanie, certyfikaty i instrukcje. Każde urządzenie winno mieć odrębną wypełnioną i podstemplowaną kartę gwarancyjną. Wszystkie dokumenty będą sporządzone w języku polskim lub w języku angielskim wraz z tłumaczeniem na język polski.
4. Wykonawca oświadcza, że każde urządzenie dostarczane w ramach realizacji Umowy jest zakupione w oficjalnym, autoryzowanym kanale sprzedaży producenta, posiadającym stosowny pakiet usług gwarancyjnych, kierowanych do użytkowników z obszaru RP.

§ 2
Termin wykonania Przedmiotu Umowy

1. Przedmiot Umowy zostanie wykonany w terminie do 18 grudnia 2023 r.
2. Wszystkie prace wykonywane będą w dni robocze (poniedziałek – piątek) w godzinach: od 8.00 do 16.00.
3. Na potrzeby Umowy, pod pojęciem „dzień roboczy", Strony rozumieją wszystkie dni kalendarzowe w roku, za wyjątkiem dni uznanych ustawowo za dzień wolny od pracy, zgodnie z ustawą z dnia 18 stycznia 1951 r. o dniach wolnych od pracy (Dz. U. z 2020 r., poz. 1920, t.j. z dnia 2 listopada 2020 r.) lub soboty, zgodnie z art. 115 ustawy z dnia 23 kwietnia 1964 r. Kodeks Cywilny (Dz. U z 2022 r., poz.1360, t.j. z dnia 29 czerwca 2022 r.).
4. Dostawa urządzeń realizowana będzie transportem Wykonawcy, na jego koszt i ryzyko, do siedziby Zamawiającego.
5. Wykonawca zobowiązuje się we własnym zakresie dokonywać wyładunku i wniesienia urządzeń do wskazanych przez Zamawiającego pomieszczeń.
6. Wykonawca zobowiązuje się powiadomić Zamawiającego o terminach realizacji Przedmiotu Umowy co najmniej z jednodniowym wyprzedzeniem.

§ 3
Obowiązki Stron

1. Zamawiający zobowiązany jest do:
   1) zapewnienia nadzoru nad realizacją Przedmiotu Umowy,
   2) odbioru należycie wykonanego Przedmiotu Umowy, wolnego od wad,
   3) zapłaty wynagrodzenia Wykonawcy za należycie wykonany Przedmiot Umowy, wolny od wad.
2. Wykonawca zobowiązany jest do:
   1) Należytego wykonania Przedmiotu Umowy, w szczególności zgodnie z:
      a. zasadami rzetelnej wiedzy technicznej,
      b. obowiązującymi przepisami prawa,
      c. obowiązującymi normami technicznymi i technologicznymi,
      d. obowiązującymi standardami zabezpieczenia i bezpieczeństwa,
      e. najwyższą starannością.
   3) Stosowania wyrobów posiadających odpowiednie atesty, certyfikaty i aprobaty, deklaracje zgodności, , Wykonawca zobowiązany będzie do przedstawienia przedstawicielowi Zamawiającego dokumentów (atestów, kart technicznych, aprobat technicznych, certyfikatów i wszelkich innych wymaganych przepisami prawa dokumentów), które pozwolą na ocenę zgodności wyrobów z dokumentacją oraz ofertą Wykonawcy.
   4) Zawarcia lub posiadania umowy ubezpieczenia od odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim w związku z realizacją Przedmiotu Umowy, tj.: ubezpieczenie od odpowiedzialności cywilnej deliktowej i kontraktowej (obejmujące roboty związane z Przedmiotem Umowy), o wartości nie mniejszej niż cena oferty brutto Wykonawcy (Załącznik nr 2). Wykonawca jest zobowiązany do posiadania ww. umowy ubezpieczenia przez cały okres realizacji Przedmiotu Umowy. W przypadku gdy termin ważności przedłożonej umowy ubezpieczenia będzie upływał w trakcie realizacji Przedmiotu Umowy, Wykonawca jest zobowiązany do wydłużenia terminu

obowiązywania posiadanej umowy ubezpieczenia lub do zawarcia nowej umowy ubezpieczenia o wartości nie mniejszej niż cena ofertowa brutto oraz przekazania kopii tych dokumentów Zamawiającemu najpóźniej z datą upływu ważności poprzedniej umowy ubezpieczenia. W trakcie realizacji umowy na każde żądanie Zamawiającego Wykonawca zobowiązany jest przedłożyć kopię aktualnej umowy ubezpieczenia (lub polisy). Sankcję niewykonania obowiązków, o których mowa powyżej stanowi uprawnienie Zamawiającego do zastosowania kary umownej, o której mowa w § 10 ust.1 pkt 5) Umowy.

5) Dokonywania w okresie objętym udzieloną gwarancją, w ramach wynagrodzenia umownego, wymaganych przeglądów i kompletnych czynności konserwacyjnych (serwisowych), wymaganych do utrzymania gwarancji na dostarczonych, w ramach niniejszej Umowy urządzeniach i systemach, bez wezwania Zamawiającego.
6) Umożliwienia Zamawiającemu w każdym czasie przeprowadzenia kontroli dokumentów dotyczących urządzeń i realizowanych dostaw, stosowanych w ich toku wyrobów oraz wszelkich okoliczności dotyczących realizacji Przedmiotu Umowy.
7) Zgłoszenia Przedmiotu Umowy do odbioru końcowego.
8) Przekazania Zamawiającemu dokumentów pozwalających na ocenę prawidłowego wykonania prac zgłaszanych do odbioru oraz innych dokumentów potwierdzających, że spełniają wszelkie normy i wymagania przewidziane prawem.
9) Nieodpłatnego uczestniczenia w czynnościach odbioru końcowego, przeglądach gwarancyjnych i w ramach rękojmi w okresie gwarancji i w okresie rękojmi za wady na wezwanie Zamawiającego.
10) Usunięcia stwierdzonych wad, nadających się do usunięcia, ujawnionych w okresie odbioru końcowego oraz w okresie i w ramach gwarancji i rękojmi za wady – w terminach wyznaczonych w Umowie i protokołach przeglądów gwarancyjnych i w ramach rękojmi.

§ 4
Przedstawiciele Stron

1. Strony zgodnie postanawiają, iż do osobami uprawnionymi do kontaktu w ramach realizacji niniejszej Umowy, nadto w ramach realizacji praw wynikających z udzielonej gwarancji i rękojmi oraz podpisania protokołu odbioru, o którym mowa w § 7 ust. 2, są:
   1) ze strony Zamawiającego: Daniel Staroń tel. , daniel.staroń@nikidw.edu.pl,
   2) ze strony Wykonawcy: ……, tel. …….., e-mail: ……
2. Zmiana osób wskazanych w ust. 1 nie stanowi zmiany niniejszej Umowy oraz dokonywana będzie w formie pisemnego powiadomienia drugiej Strony.

§ 5
Podwykonawcy

1. Wykonawca zrealizuje zamówienie *bez udziału/ z udziałem** podwykonawców.
2. Za działanie lub zaniechanie Podwykonawcy/ów Wykonawca ponosi odpowiedzialność jak za swoje własne.
3. W przypadku realizacji Przedmiotu Umowy z udziałem Podwykonawców, Wykonawca zobowiązany jest do zawarcia pisemnych umów o podwykonawstwo.

4. Wykonawca nie może zwolnić się od odpowiedzialności względem Zamawiającego z tego powodu, że niewykonanie lub nienależyte wykonanie umowy przez Wykonawcę było następstwem niewykonania lub nienależytego wykonania zobowiązań wobec Wykonawcy przez jego Podwykonawców.
5. W przypadku wykonywania Przedmiotu Umowy, w miejscu podlegającym bezpośredniemu nadzorowi Zamawiającego, Zamawiający żąda, aby przed przystąpieniem do wykonania zamówienia Wykonawca, o ile są już znani, podał nazwy albo imiona i nazwiska oraz dane kontaktowe podwykonawców i osób do kontaktu z nimi, zaangażowanych w takie zamówienie. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach danych, o których mowa w zdaniu pierwszym, w trakcie realizacji zamówienia, a także przekazuje informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację części Przedmiotu Umowy.
6. Wykonawca odpowiada za działania i zaniechania Podwykonawców na zasadzie ryzyka.
7. Do zawarcia umowy przez Wykonawcę z podwykonawcą, a także na dokonanie zmian w takiej umowie jest wymagana uprzednia zgoda Zamawiającego. Wykonawca jest zobowiązany do ukształtowania umowy z własnym podwykonawcą, zgodnie z żądaniem Zamawiającego, w szczególności w zakresie wymagań umownych określonych w niniejszej Umowie.
8. Podwykonawca jest zobowiązany przedstawić Zamawiającemu za pośrednictwem Wykonawcy projekt umowy lub zmianę projektu umowy o podwykonawstwo w zakresie powierzonej części Przedmiotu Umowy. Jeżeli Zamawiający zgłosi na piśmie zastrzeżenia do treści projektu umowy lub zmiany projektu umowy – Podwykonawca obowiązany jest uwzględnić zgłoszone zastrzeżenia i przedstawić projekt lub jego zmianę do ponownej akceptacji.
9. Wykonawca zobowiązany jest w terminie 3 dni od dnia zawarcia umowy z Podwykonawcą lub od dnia zamiany takiej umowy, przedłożyć Zamawiającemu poświadczoną za zgodność z oryginałem kopię zawartej umowy lub zawartego aneksu.
10. Jeżeli zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się w celu wykazania spełniania warunków udziału w postępowaniu lub kryteriów selekcji, Wykonawca jest obowiązany wykazać Zamawiającemu, że proponowany inny Podwykonawca lub Wykonawca samodzielnie spełnia je w stopniu nie mniejszym niż podwykonawca, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia.
11. Jeżeli powierzenie Podwykonawcy wykonania części Przedmiotu Umowy, następuje w trakcie jego realizacji, Wykonawca na żądanie Zamawiającego przedstawia oświadczenie lub oświadczenia lub dokumenty potwierdzające brak podstaw wykluczenia, wobec tego Podwykonawcy.
12. Jeżeli Zamawiający stwierdzi, że wobec danego Podwykonawcy zachodzą podstawy wykluczenia, Wykonawca obowiązany jest zastąpić tego Podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia Podwykonawcy.
13. Wykonawca obowiązany jest informować Zamawiającego o wysokości wynagrodzenia należnego Podwykonawcom lub dalszym Podwykonawcom oraz o wysokości kwot im zapłaconych za wykonanie prac, objętych przedłożoną Zamawiającemu umową o podwykonawstwo.

14. Przepisy niniejszego paragrafu mają zastosowanie również do umów z dalszymi podwykonawcami.

§ 6
Przygotowania odbioru końcowego

1. Wykonawca zgłasza pisemnie Zamawiającemu gotowość do odbioru końcowego Przedmiotu Umowy, nie później niż 3 dni przed planowanym odbiorem.
2. Razem z wnioskiem o dokonanie odbioru końcowego Przedmiotu Umowy Wykonawca przekaże Zamawiającemu dokumenty pozwalające na ocenę prawidłowego wykonania Przedmiotu Umowy, w tym:
   1) dokument/y stwierdzający/e udzielenie przez Wykonawcę gwarancji na cały wykonany Przedmiot Umowy wraz z warunkami gwarancji i serwisu gwarancyjnego (które nie mogą być sprzeczne z postanowieniami niniejszej Umowy);
   2) dokument/y (w języku polskim) stwierdzający/e udzielenie przez producenta/ów gwarancji na dostarczone urządzenia i produkty wraz z warunkami gwarancji i serwisu gwarancyjnego wraz z dokonaniem przeniesienia na Zamawiającego wszystkich uprawnień wynikających z tych gwarancji;
   3) instrukcje obsługi technicznej i eksploatacji zamontowanych urządzeń i produktów wraz z danymi technicznymi oraz prospektami. Dokumentacja dostarczona przez Wykonawcę (w języku polskim) wraz z urządzeniami i sprzętem powinna obejmować następujące elementy: dane dotyczące identyfikacji urządzenia (nazwa, typ, producent), informacje dotyczące przechowywania i transportu, informacje dotyczące uruchomienia sprzętu, informacje dotyczące samego wyposażenia i sprzętu (warunki pracy, opis techniczny), instrukcje obsługi, informacje dotyczące utrzymania ruchu, w tym także wymagań w zakresie konserwacji, informacje dotyczące postępowania w sytuacjach awaryjnych, wszelkie wymagane prawem atesty, oświadczenia, certyfikaty i aprobaty, związane z realizacją Przedmiotu Umowy.

§ 7
Odbiór końcowy

1. Zamawiający przystąpi do czynności odbioru końcowego najpóźniej w terminie 3 dni, licząc od daty otrzymania pisemnego zgłoszenia przez Wykonawcę gotowości do odbioru końcowego.
2. Poprzez zakończenie pełnego zakresu Przedmiotu Umowy należy rozumieć dokonanie ostatecznego odbioru Przedmiotu Umowy bez usterek za protokołem zatwierdzonym przez przedstawicieli Zamawiającego i Wykonawcy, najpóźniej w terminie określonym w § 2 ust. 1 umowy, którego wzór stanowi Załącznik nr 3 do Umowy.
3. Jeżeli w toku czynności odbioru zostaną stwierdzone wady, Zamawiającemu przysługują następujące uprawnienia:
   1) jeżeli wady nadają się do usunięcia – może odmówić odbioru do czasu usunięcia wad,
   2) jeżeli wady nie nadają się do usunięcia, lecz:
      a. umożliwiają użytkowanie Przedmiotu Umowy, zgodnie z przeznaczeniem – Zamawiający może obniżyć wynagrodzenie przysługujące Wykonawcy o taki procent, o jaki wada obniża wartość Przedmiotu Umowy,

b. uniemożliwiają użytkowanie zgodnie z przeznaczeniem – Zamawiający może odstąpić od Umowy lub żądać wykonania Przedmiotu Umowy po raz drugi.

5. W przypadku, o którym mowa w ust. 3, Zamawiający sporządza protokół zawierający przyczyny odmowy odbioru.
6. Żądając usunięcia stwierdzonych wad, Zamawiający wyznaczy Wykonawcy termin pozwalający na ich usunięcie. Wykonawca nie może odmówić usunięcia wad bez względu na wysokość związanych z tym kosztów.
7. Gdy wady zostaną usunięte, procedura odbioru zostanie powtórzona.
8. W przypadku nieusunięcia przez Wykonawcę zgłoszonej wady w wyznaczonym terminie, Zamawiający może usunąć wadę lub zlecić jej usunięcie w zastępstwie Wykonawcy i na jego koszt i ryzyko po uprzednim pisemnym powiadomieniu Wykonawcy.
9. W przypadku gdy dostarczane na etapie realizacji i odbioru Przedmiotu Umowy produkty nie będą zgodne z treścią oferty Wykonawcy, Zamawiający ma prawo do żądania wymiany produktu/ów na spełniające wymogi jakościowe (techniczne i użytkowe) określone w OPZ i w ofercie Wykonawcy, na koszt i ryzyko Wykonawcy.

§ 8
Wynagrodzenie

1. Z tytułu wykonania Przedmiotu Umowy, Wykonawcy przysługuje ryczałtowe wynagrodzenie, zgodnie ze złożoną ofertą i wynosi …….. zł netto, (słownie: ……), co stanowi **……. zł brutto** (słownie: ……. złotych 00/100).
2. Podstawą wypłaty wynagrodzenia będzie zaakceptowana przez Zamawiającego faktura VAT wystawiona przez Wykonawcę po wykonaniu i przyjęciu Przedmiotu Umowy oraz przedstawieniu podpisanego protokołu odbioru (Załącznik nr 3).
3. Zapłata za wykonany Przedmiot Umowy nastąpi przelewem bankowym w ciągu 14 dni od daty wpływu faktury do siedziby Zamawiającego, na rachunek bankowy Wykonawcy wskazany na fakturze.
4. Kwota, o której mowa w ust. 1 jest ostateczna i obejmuje wszelkie koszty, jakie powstaną w związku z realizacją Przedmiotu Umowy, w tym opłaty celne, podatkowe, koszty transportu, ubezpieczenia podczas transportu do Zamawiającego, gwarancji, rękojmi, a także wartość opłat licencyjnych na korzystanie z oprogramowania na wszelkich polach eksploatacji niezbędnych do prawidłowego korzystania z oprogramowania i zgodnych z oczekiwaniami Zamawiającego
5. Za datę płatności Strony uznają dzień obciążenia rachunku bankowego Zamawiającego poleceniem zapłaty.
6. W przypadku zawarcia umowy o podwykonawstwo, Wykonawca zobowiązany jest do dokonania we własnym zakresie wypłaty wynagrodzenia należnego Podwykonawcy z zachowaniem terminów płatności określonych w umowie o podwykonawstwo.

§ 9
Gwarancja i rękojmia

1. Na wykonany Przedmiot Umowy (w tym na urządzenia, produkty, materiały) Wykonawca udziela Zamawiającemu gwarancji na okres **60** miesięcy, niezależnie od rękojmi, licząc od

daty podpisania protokołu ostatecznego odbioru Przedmiotu Umowy, o którym mowa w § 7 ust. 2.

2. Za dokument gwarancyjny zostanie uznana podpisana przez obie strony niniejsza Umowa, w przypadku, gdy Wykonawca nie dostarczy Zamawiającemu dokumentów wymaganych w § 6 ust. 2.
3. Jeżeli okres gwarancji udzielony przez Producenta jest dłuższy niż okres gwarancji udzielony przez Wykonawcę, wszelkie prawa wynikające z gwarancji producenta przejmuje Zamawiający. Na tą okoliczność wykonawca przekaże Zamawiającemu stosowne oświadczenie i dokumenty konieczne do korzystania z gwarancji producenta.
4. W okresie udzielonej gwarancji Wykonawca zobowiązany będzie do świadczenia serwisu gwarancyjnego na swój koszt (obejmującego również dojazd i transport), polegającego na wymianie Przedmiotu Umowy na wolny od wad lub usunięciu wad w drodze naprawy, na warunkach opisanych w niniejszej Umowie.
5. Gwarancja obejmuje zakres Przedmiotu Umowy wynikający z Umowy:
   1) w przypadku gdy wady ujawnią się w terminie trwania gwarancji określonym w § 9 ust. 1 Wykonawca zobowiązuje się do bezpłatnego usunięcia wad fizycznych lub do dostarczenia i zamontowania wolnego od wad Przedmiotu Umowy;
   2) w przypadku zaistnienia wad Wykonawca zobowiązuje się do usunięcia wady na miejscu jej wystąpienia, a jeżeli to nie będzie możliwe do odebrania wadliwego Przedmiotu Umowy i jego naprawy oraz dostarczenia i ponownego zamontowania po usunięciu wad na swój koszt;
   3) Wykonawca zobowiązuje się wykonać obowiązki wynikające z gwarancji w terminie 14 dni od dnia zgłoszenia wystąpienia wady. W przypadku nie usunięcia wady Zamawiający zleci jej usunięcie innemu podmiotowi na koszt i ryzyko Wykonawcy;
   4) każda naprawa wydłuża czas gwarancji na każdą naprawianą część Przedmiotu Umowy o okres od wystąpienia wady do czasu jej usunięcia i potwierdzenia naprawy przez Zamawiającego;
   5) jedynie w przypadku stwierdzenia, że przyczyną była dewastacja lub wandalizm koszty usunięcia szkody nie będą obciążały Wykonawcy, a naprawa takiej usterki nie wydłuża okresu gwarancji. W pozostałych przypadkach Wykonawca wykonuje naprawy na swój koszt;
   6) wszelkie koszty związane z realizacją gwarancji, w szczególności: dojazdów lub dostarczenia Przedmiotu Umowy, robocizny, ponosi Wykonawca.
6. Gwarancja nie wyłącza, nie ogranicza ani nie zawiesza uprawnień nabywcy wynikających z rękojmi za wady Przedmiotu Umowy.
7. Uprawnienia Zamawiającego z tytułu rękojmi za wady wygasają nie wcześniej niż 3 miesiące po upływie okresu gwarancji, przewidzianego w ust. 1

§ 10
Kary umowne

1. Wykonawca zapłaci Zamawiającemu kary umowne w niżej określonych wysokościach, w następujących przypadkach:
   1) za każdy dzień opóźnienia w wykonaniu Przedmiotu Umowy, w wysokości 1 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1;

2) za opóźnienie w usunięciu wad stwierdzonych przez Zamawiającego przy odbiorze lub w ramach rękojmi i gwarancji za wady w wysokości 1 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1, za każdy dzień opóźnienia licząc od następnego dnia po upływie terminu określonego przez Zamawiającego do usunięcia wad;
3) za niezgłoszenie Przedmiotu Umowy do odbioru w terminie określonym w § 6 ust. 1, w wysokości 1 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1;
4) za odstąpienie od Umowy przez którąkolwiek ze stron z przyczyn, za które ponosi odpowiedzialność Wykonawca – w wysokości 20 % wynagrodzenia brutto, o którym mowa w § 8 ust. 1;
5) za nieposiadanie umowy ubezpieczenia z tytułu odpowiedzialności cywilnej za szkody wyrządzone osobom trzecim w zakresie prowadzonej działalności gospodarczej w zakresie, o którym mowa w § 3 ust. 2 pkt 3) Umowy, w wysokości 1 % wynagrodzenia brutto określonego w § 8 ust. 1, za każdy dzień braku obowiązywania umowy ubezpieczenia.

2. Wykonawca jest uprawniony do dochodzenia odszkodowania w wysokości przewyższającej zastrzeżone kary umowne na zasadach ogólnych.
3. Odstąpienie od Umowy wymaga formy pisemnej pod rygorem nieważności, poprzez złożenie oświadczenia drugiej stronie umowy.
4. Zamawiający zastrzega sobie prawo do potrącenia kar umownych z dowolnej należności Wykonawcy, na co niniejszym Wykonawca wyraża zgodę.

§ 11
Odstąpienie od Umowy

1. W przypadku zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o tych okolicznościach.
2. W przypadku, o którym mowa w ust. 1, Wykonawca może żądać wyłącznie wynagrodzenia należnego mu z tytułu wykonania części Umowy.
3. Niezależnie od ust. 1 i 2, Zamawiający może odstąpić od Umowy, jeżeli:
   1) Wykonawca nie podjął się realizacji Przedmiotu Umowy lub przerwał realizację Umowy, a opóźnienie (przerwa) przekracza 7 dni;
   2) Wykonawca nie dostarczył Przedmiotu Umowy w terminie, określonym w § 2 ust. 1;
   3) Wykonawca pomimo uprzednich pisemnych zastrzeżeń Zamawiającego nie wykonuje Przedmiotu Umowy, zgodnie z warunkami Umowy.

§ 12
Zmiana Umowy

1. Zakazana jest istotna zmiana postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, z zastrzeżeniem ust. 2.
2. Strony przewidują następujące rodzaje i warunki zmiany treści Umowy:
   1) zmniejszenie zakresu Przedmiotu Umowy, gdy jego wykonanie w pierwotnym zakresie nie leży w interesie publicznym,

2) zmniejszenie wynagrodzenia za wykonanie Przedmiotu Umowy w przypadku zmniejszenia jego zakresu w razie zaistnienia sytuacji, o której mowa w ust. 1,
3) zmiana terminu realizacji Przedmiotu Umowy, w przypadku:
   a. gdy zachowanie pierwotnie określonego terminu nie leży w interesie publicznym,
   b. działania siły wyższej, uniemożliwiającego wykonanie prac w określonym pierwotnie terminie,
   c. konieczności zmiany finansowania,
   d. realizacji prac powiązanych z Przedmiotem Umowy zleconych na podstawie aneksu do niniejszej Umowy lub na podstawie odrębnej umowy,
   e. wymuszających konieczność koordynacji tych prac z pracami realizowanym na podstawie niniejszej Umowy i uwzględnienia wzajemnych powiązań,
   f. zmiany Podwykonawcy, o którym mowa w § 5 Umowy,
   g. gdy z przyczyn obiektywnych Wykonawca nie mógł zrealizować Przedmiotu Umowy w terminie.

3. Zmiany Umowy przewidziane w ust. 2 dopuszczalne są na następujących warunkach:
   1) zmniejszenie zakresu Przedmiotu Umowy w granicach uzasadnionego interesu publicznego lub w zakresie wynikającym z cofnięcia środków pochodzących z zewnętrznych źródeł finansowania, które miały być przeznaczone na dofinansowanie Przedmiotu Umowy;
   2) zmniejszenie wynagrodzenia Wykonawcy określonego kwotą ryczałtową brutto (§ 8 ust. 1 Umowy), odpowiednio do wartości zmniejszonego zakresu Przedmiotu Umowy;
   3) zmiana terminu realizacji Przedmiotu Umowy:
      a. o okres umożliwiający osiągnięcie uzasadnionego interesu publicznego,
      b. o okres działania siły wyższej oraz potrzebny do usunięcia skutków tego działania,
      c. o okres proporcjonalny do zmniejszonego zakresu,
      d. o okres niezbędny na wykonanie prac powiązanych z przedmiotem niniejszej Umowy (zleconych na podstawie aneksu do niniejszej Umowy lub odrębną umową),
      e. o okres niezbędny na wykonanie prac, gdy z przyczyn obiektywnych Wykonawca nie mógł zrealizować Przedmiotu Umowy w terminie – na uzasadniony wniosek Wnioskodawcy;
   4) zmiana postanowień zawartej Umowy może nastąpić wyłącznie za zgodą Stron wyrażoną w formie pisemnego aneksu pod rygorem nieważności.

§ 13
RODO

1. W przypadku udostępnienia Wykonawcy na mocy Umowy przez Zamawiającego danych osobowych pracowników i współpracowników Zamawiającego w zakresie niezbędnym do realizacji Umowy, Wykonawca zobowiązuje się przetwarzać udostępnione przez Zamawiającego dane osobowe w zakresie: imię, nazwisko, numer telefonu, adres e-mail wyłącznie w celu należytego wykonania Umowy zgodnie z postanowieniami Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781, tj. z dnia 19 września 2019 r.) oraz aktami wykonawczymi do Ustawy i Rozporządzenia Parlamentu

Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. U. UE. L. z 2016 r. Nr 119, str. 1 z późn. zm.) (dalej: RODO) oraz innymi powszechnie obowiązującymi przepisami prawa.

2. Wykonawca zobowiązuje się do zabezpieczenia danych osobowych przed ujawnieniem lub udostępnieniem ich osobom nieupoważnionym. W celu zapewnienia realizacji Umowy Wykonawca zobowiązuje się ujawniać dane osobowe wyłącznie pisemnie upoważnionym osobom będącym pracownikami lub zleceniobiorcami Zamawiającego.
3. Wykonawca ponosi wszelką odpowiedzialność za szkody wyrządzone Zamawiającemu, jego pracownikom lub zleceniobiorcom oraz osobom trzecim w związku z przetwarzaniem danych osobowych.
4. W przypadku wygaśnięcia Umowy z jakiegokolwiek powodu Wykonawca w ciągu 7 dni od dnia zakończenia obowiązywania Umowy, trwale usunie wszelkie sporządzone w związku lub przy okazji wykonywania Umowy zapisy zawierające dane osobowe pracowników lub współpracowników Zamawiającego w sposób przewidziany w przepisach prawa. Wykonawca ma prawo do zachowania kopii informacji zawierających dane osobowe udostępnione przez Zamawiającego jedynie, gdy jest to wymagane przepisami prawa lub decyzją/orzeczeniem uprawnionego organu. Dane takie muszą zostać zniszczone/usunięte/zanonimizowane przez Wykonawcę po ustaniu celu, w jakim są przechowywane.
5. W przypadku udostępnienia Zamawiającego przez Wykonawcę danych osobowych swojego pracownika Wykonawca zobowiązuje się do poinformowania tego pracownika o przetwarzaniu przez Zamawiającego jego danych osobowych w zakresie: imię, nazwisko, numer telefonu, adres e-mail wyłącznie w celu należytego wykonania Umowy zgodnie z postanowieniami Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781, tj. z dnia 19 września 2019 r.) oraz RODO. Podstawą do przetwarzania danych jest art. 6 ust. 1 lit. b) RODO. Wykonawca zobowiązuje się także do poinformowana tego pracownika, że jego dane osobowe będą przetwarzane przez cały czas trwania Umowy oraz przez okres przedawnienia ewentualnych roszczeń z Umowy. Dane pracownika Wykonawcy nie będą przekazywane innym podmiotom. Pracownik Wykonawcy ma prawo dostępu do treści danych osobowych oraz ich poprawiania, sprostowania oraz do usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec ich przetwarzania. Ponadto pracownikowi Wykonawcy przysługuje prawo do wniesienia skargi do organu nadzorczego właściwego dla przetwarzania danych. W przypadku zmiany pracownika, Wykonawca zobowiązuje się do poinformowania nowo wskazanej osoby o treści niniejszego ustępu.

§ 14
Postanowienia końcowe

1. Wykonawca gwarantuje Zamawiającemu, że uzyskał wszystkie niezbędne prawa własności przemysłowej i intelektualnej na dostarczone urządzenia i oprogramowanie objęte Umową, oraz że urządzenia i to oprogramowanie, nie naruszają żadnych praw, w tym praw własności przemysłowej i intelektualnej osób trzecich ani ich dóbr osobistych.

2. Zamawiający otrzymuje niewyłączne, nieprzenoszalne licencje na korzystanie z oprogramowania, umożliwiające jego wykorzystanie, na zasadach i w granicach (pola eksploatacji) wskazanych w dokumencie licencyjnym załączonym do ww. oprogramowania - przez cały czas trwania autorskich praw majątkowych do tego oprogramowania.
3. Wykonawca ponosi odpowiedzialność z tytułu ewentualnego naruszenia praw (w tym praw, o których mowa w ust. 1 lub dóbr osobistych osób trzecich, mogącego ewentualnie wyniknąć z tytułu eksploatacji urządzeń i dostarczonego wraz z nimi oprogramowania, zgodnej z zakresem przewidzianym w Umowie i załącznikach. W przypadku skierowania roszczeń z tego tytułu przeciwko Zamawiającemu, Wykonawca zobowiązuje się do:
   1) zwolnienia Zamawiającego z obowiązku świadczeń z tego tytułu na zasadzie art. 392 Kodeksu cywilnego, w tym pokrycia kosztów zastępstwa prawnego i całkowitego zaspokojenia słusznych roszczeń osób trzecich z tytułu naruszenia w/w praw;
   2) wstąpienia do toczącego się przeciwko Zamawiającemu postępowania w charakterze strony bądź interwenienta ubocznego po stronie Zamawiającego (w zależności od sytuacji procesowej).
4. W przypadku skierowania przez osoby trzecie jakichkolwiek roszczeń wobec Zamawiającego związanych z niewykonaniem lub nienależytym wykonaniem umowy przez Wykonawcę, Wykonawca zobowiązany jest niezwłocznie przystąpić do sporu lub wstąpić w miejsce Zamawiającego w takim sporze, chyba że roszczenia uznane zostały za bezzasadne prawomocnym orzeczeniem Sądu.
5. Prawa i obowiązki oraz wierzytelności Wykonawcy wynikające z umowy nie mogą być w okresie realizacji oraz po zakończeniu umowy przenoszone na rzecz osób trzecich bez uprzedniej zgody Zamawiającego, wyrażonej na piśmie pod rygorem nieważności.
6. W sprawach nie uregulowanych niniejszą Umową mają zastosowanie przepisy Kodeksu Cywilnego oraz ustawy Prawo zamówień publicznych.
7. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
8. Wszelkie spory mogące powstać w związku z realizacją niniejszej Umowy podlegają rozpoznaniu przez sąd powszechny, właściwy dla Zamawiającego.
9. Umowa niniejsza została sporządzona i zawarta w formie pisemnej.

Załączniki:
Załącznik nr 1 – Opis Przedmiotu Zamówienia;
Załącznik nr 2 – Oferta Wykonawcy;
Załącznik nr 3 – Protokół odbioru.

....
(podpis Wykonawcy) (podpis Zamawiającego)

Załącznik nr 1 do Umowy nr xxx/2023/NIKiDW

OPIS PRZEDMIOTU ZAMÓWIENIA

Załącznik nr 3 do Umowy nr xxx/2023/NIKiDW

PROTOKÓŁ ODBIORU

sporządzony w Warszawie, w dniu …… grudnia 2023 r., pomiędzy:

Narodowym Instytutem Kultury i Dziedzictwa Wsi z siedzibą w Warszawie (00-322), przy ul. Krakowskie Przedmieście 66, wpisanym do Rejestru Instytucji Kultury, dla których organizatorem jest Minister Rolnictwa i Rozwoju Wsi, pod numerem 3, NIP: 525-28-04-887, Regon: 384655657, reprezentowanym przez:

……. - pracownika NIKiDW,

zwanym dalej: **Zamawiającym,**
a
……
……
…….
zwanym w dalej **Wykonawcą**.

Zamawiający potwierdza odbiór Przedmiotu Umowy nr xxx/2023/NIKiDW (dalej: Umowa) dostarczonego i zamontowanego przez Wykonawcę w dniu/dniach ....., zgodnie z poniższą specyfikacją

Miejsce dostawy: NIKiDW, ul. Krakowskie Przedmieście 66, 00-322 Warszawa

☐ Zamawiający potwierdza zgodność dostarczonych urządzeń z Umową.

☐ Zamawiający składa następujące uwagi:
……
……
Data usunięcia wad lub usterek: …….

ZAMAWIAJĄCY **WYKONAWCA**