Gmina Dziwnów
72-420 Dziwnów, ul. Szosowa 5
tel. 91 32 75 163, fax. 91 32 75 164
Godziny urzędowania: poniedziałek – piątek 7:30 – 15.30

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

DOTYCZY: Zwiększenie cyberbezpieczeństwa Gminy Dziwnów

NUMER POSTĘPOWANIA: WZP.271.5.2024

KATEGORIA ZAMÓWIENIA: DOSTAWY

(CPV: 48822000-6, 31682520-1, 32420000-3, 35120000-1, 48821000-9, 31214100-0, 51610000-1, 48900000-7, 80533100-0)

postępowanie o udzielenie zamówienia publicznego prowadzone w trybie podstawowym bez negocjacji, o wartości zamówienia nieprzekraczającej progów unijnych, zgodnie z art. 3 oraz art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – prawo zamówień publicznych (dz. u. 2023 r. poz 1605 ze zm.) – dalej: zwana: „p.z.p.”

ZATWIERDZAM:
Łukasz Dzioch
Elektronicznie podpisany przez Łukasz Dzioch
Data: 2024.05.29 12:59:28 +02'00'
.....
Zastępca Burmistrza Dziwnowa

Dziwnów, dnia 29 maja 2024 r.

Integralną część SWZ stanowią:

Załącznik nr 1. Formularz ofertowy.
Załącznik nr 2. Oświadczenie o braku podstaw do wykluczenia i o spełnianiu warunków udziału w postępowaniu.
Załącznik nr 3. Lista podmiotów należących do tej samej grupy kapitałowej/Informacja o nienależeniu do grupy kapitałowej.
Załącznik nr 4. Zobowiązanie podmiotu trzeciego do oddania do dyspozycji niezbędnych zasobów.
Załącznik nr 5. Wykaz dostaw.
Załącznik nr 6. Wykaz usług.
Załącznik nr 7. Projekt umowy.

Numer postępowania: WZP.271.5.2024

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)
INSTRUKCJA DLA WYKONAWCÓW

Nazwa zamówienia publicznego:
„Zwiększenie cyberbezpieczeństwa Gminy Dziwnów”

ROZDZIAŁ I.
POSTANOWIENIA OGÓLNE

1.1. NAZWA (FIRMA) ORAZ ADRES ZAMAWIAJĄCEGO

Gmina Dziwnów
72-420 Dziwnów, ul. Szosowa 5
tel. 91 32 75 163, fax. 91 32 75 164
NIP 986-01-56-976
REGON 811684918
e-mail: um@dziwnow.pl
adres strony internetowej: https://platformazakupowa.pl/pn/dziwnow
Elektroniczna Skrzynka Podawcza: na platformie ePUAP**:** /lt97ww13bx/SkrytkaESP
godziny urzędowania: 7:30 – 15:30
Konto bankowe: 18 1240 3868 1111 0000 4093 6541

1.2. INFORMACJE WSTĘPNE

1. Postępowanie prowadzone jest w języku polskim.
2. Wykonawcy zobowiązani są do dokładnego zapoznania się z całością niniejszej SWZ i ponoszą ryzyko niedostarczenia wszystkich wymaganych informacji i dokumentów lub oświadczeń, a także złożenia oferty nieodpowiadającej wymaganiom określonym przez Zamawiającego.
3. Wszystkie załączniki do niniejszej SWZ stanowią jej integralną część.

1.3. TRYB UDZIELENIA ZAMÓWIENIA

1. Niniejsze postępowanie prowadzone jest trybie podstawowym bez negocjacji, o którym mowa w art. 275 pkt 1 p.z.p. oraz niniejszej Specyfikacji Warunków Zamówienia (zwanej w dalszej części „SWZ”). Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
2. Wartość zamówienia nie przekracza progów unijnych, o którym mowa w art. 3 Pzp w odniesieniu do dostaw i usług.
3. W zakresie nieuregulowanym niniejszą SWZ, zastosowanie mają przepisy Pzp.
4. Wykonawca powinien dokładnie zapoznać się z niniejszą SWZ i złożyć ofertę zgodnie z jej wymaganiami

1.4 SŁOWNIK

Użyte w niniejszej SWZ (oraz w załącznikach) terminy mają następujące znaczenie:
1) **„Pzp"** - ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2023 r., poz. 1605 ze zm.),

2) **„SWZ"** - niniejsza Specyfikacja Warunków Zamówienia,

3) **„zamówienie"** - zamówienie publiczne, którego przedmiot został opisany w Rozdziale II niniejszej SWZ,

4) **„postępowanie"** - postępowanie o udzielenie zamówienia publicznego, którego dotyczy niniejsza SWZ,

5) **„Zamawiający"** – Gmina Dziwnów,
6) **„Wykonawca"** - należy przez to rozumieć osobę fizyczną, osobę prawną albo jednostkę organizacyjną nieposiadającą osobowości prawnej, która ubiega się o udzielenie zamówienia publicznego, złożyła ofertę lub zawarła umowę w sprawie zamówienia publicznego,

8) **„RODO"** - rozporządzenie 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. Urz. UE L 119 z 04.05.2016, str. 1),
9) **„platformazakupowa.pl "**- portal internetowy umożliwiający komunikację elektroniczną między Zamawiającym i Wykonawcami, w szczególności elektroniczne składanie ofert oraz oświadczeń, w tym JEDZ, w zgodzie z wymogami określonymi przez dyrektywy UE dostępne na stronie
Wykonawca zobowiązany jest do zapoznania się z instrukcjami korzystania z **platformazakupowa.pl** (https://platformazakupowa.pl/strona/45-instrukcje i postępowania zgodnie z jej postanowieniami z uwzględnieniem zapisów niniejszej SWZ.

1.4. OZNACZENIE POSTĘPOWANIA

1. Postępowanie oznaczone jest znakiem: **WZP.271.5.2024**
2. Wykonawcy powinni we wszelkich kontaktach z Zamawiającym powoływać się na wyżej podane oznaczenie.

1.5. ŹRÓDŁA FINANSOWANIA

Zamawiający informuje, iż zamówienie jest finansowane z budżetu Gminy Dziwnów w ramach programu Funduszu Europejskiego na Rozwój Cyfrowy (FERC) II Zaawansowane usługi cyfrowe działanie 2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa z Europejskiego Funduszu Rozwoju Regionalnego (EFRR).

1.6. OCHRONA DANYCH OSOBOWYCH

Zgodnie z art. 13 ust. 1 i 2 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. Urz. UE L 119 z 04.05.2016, str. 1), dalej *„RODO",* Zamawiający informuje, że:
1) Jest administratorem danych osobowych Wykonawcy oraz osób, których dane Wykonawca przekazał w niniejszym postępowaniu;

2) dane osobowe Wykonawcy przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na *„Zwiększenie cyberbezpieczeństwa Gminy Dziwnów”* prowadzonym w trybie przetargu nieograniczonego;

3) odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 Pzp;

4) dane osobowe Wykonawcy będą przechowywane, zgodnie z Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

5) obowiązek podania przez Wykonawcę danych osobowych bezpośrednio go dotyczących jest wymogiem ustawowym określonym w przepisach Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z Pzp;

6) w odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

7) Wykonawca posiada:
- na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Wykonawcy;

- na podstawie art. 16 RODO prawo do sprostowania danych osobowych, o ile ich zmiana nie skutkuje zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie narusza integralności protokołu oraz jego załączników;
- na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO;
- prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy Wykonawca uzna, że przetwarzanie jego danych osobowych narusza przepisy RODO

8) Wykonawcy nie przysługuje:

- w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych;
- prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO;
- na podstawie art. 21 RODO prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania danych osobowych Wykonawcy jest art. 6 ust. 1 lit. c RODO.

W przypadku, gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, wymagałoby niewspółmiernie dużego wysiłku, Zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego lub konkursu.
Skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 rozporządzenia 2016/679, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego lub konkursu ani zmianą postanowień umowy w zakresie niezgodnym z ustawą.
Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego lub konkursu.
W przypadku danych osobowych zamieszczonych przez zamawiającego w Biuletynie Zamówień Publicznych, prawa, o których mowa w art. 15 i art. 16 rozporządzenia 2016/679, są wykonywane w drodze żądania skierowanego do Zamawiającego.

1.7. INFORMACJE DODATKOWE

1. Zamawiający **nie przewiduje**:
   - zawarcia umowy ramowej,
   - rozliczania w walutach obcych,
   - aukcji elektronicznej,
   - zwrotu kosztów udziału w postępowaniu,
   - złożenia oferty w postaci katalogów elektronicznych.
2. Zgodnie z art. 139 Pzp Zamawiający może najpierw dokonać badania i oceny ofert, a następnie dokonać kwalifikacji podmiotowej wykonawcy, którego oferta została najwyżej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.
3. Zamawiający nie przewiduje udzielenia zamówień, o których mowa w art. 214 ust. 1 pkt 7 i 8 Pzp.
4. Zamawiający **dopuszcza** możliwości składania **ofert częściowych**.
5. Zamawiający **nie dopuszcza** możliwości złożenia **oferty wariantowej.**
6. Szacunkowa wartość przedmiotowego zamówienia nie przekracza progów unijnych, o których mowa w art. 3 p.z.p.
7. Zamawiający nie zastrzega możliwości ubiegania się o udzielenie zamówienia wyłącznie przez Wykonawców, o których mowa w art. 94 p.z.p.
8. Na podstawie art. 310 ustawy „Pzp" Zamawiający może unieważnić postępowanie o udzielenie zamówienia, jeżeli środki, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane, a możliwość unieważnienia postępowania na tej podstawie została przewidziana w ogłoszeniu o zamówieniu w postępowaniu prowadzonym w trybie podstawowym.

ROZDZIAŁ II.
OPIS PRZEDMIOTU ZAMÓWIENIA

2.1. PRZEDMIOT ZAMÓWIENIA

Przedmiotem zamówienia jest zakup i dostawa fabrycznie nowego sprzętu tj. :

- serwera i wdrożenie usługi Active Directory,
- macierz oraz dodatkowych dysków do posiadanej macierzy,
- oprogramowania zabezpieczające pocztę email urzędu (Email Secure Gateway),
- czterech przełączników sieciowych niezbędne do prawidłowej konfiguracji w tym zagregowania połączeń z serwerów oraz urządzeń pracujących w sieci,

oraz przeprowadzenie szkoleń zakresu cyberbezpieczeństwa dla pracowników Urzędu Miejskiego, jednostek podległych oraz kadry kierowniczej podnoszące świadomość cyberzagrożeń i bezpiecznego przetwarzania danych a także specjalistyczne szkolenia dla informatyka w zakresie zastosowanych (planowanych do zastosowania) środków bezpieczeństwa oraz wdrożonych rozwiązań.

Zamówienie podzielone jest na części:

CZĘŚĆ I. Zakup sprzętu zwiększającego cyberbezpieczeństwo.

Serwer wraz z konfiguracją Active Directory – 1 szt.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 1U wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa z możliwością wyposażenia w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania do dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. Na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać min. 1TB pamięci RAM.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. 16-rdzeniowy, min. 2.4GHz, klasy x86 dedykowane do pracy z zaoferowanym serwerem umożliwiające osiągnięcie wyniku min. 229 w teście SPECrate2017_int_base, dostępnym na stronie www.spec.org dla konfiguracji dwuprocesorowej.
RAM	Minimum 128GB DDR4 RDIMM 3200MT/s,
Funkcjonalność pamięci RAM	Advanced ECC, Memory Page Retire, Fault Resilient Memory, Memory Self-Healing lub PPR, Partial Cache Line Sparing
Gniazda PCI	- minimum jeden slot PCIe x16 generacji 4
Interfejsy sieciowe/FC/SAS	Wbudowane min. 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT oraz 4 interfejsy sieciowe 25Gb Ethernet w standardzie SFP28 obsadzone wkładkami 10Gb SFP+ (porty nie mogą być osiągnięte poprzez karty w slotach PCIe). Dodatkowa min. czteroportowa karta 12Gb SAS HBA. Serwer wyposażony w min. 8 światłowodów OM3 LC-LC oraz 2 kable UTP Kat 5e o długości minimum 3m.
Dyski twarde	Zainstalowane 2 dyski M.2 SATA o pojemności min. 480GB z możliwością konfiguracji RAID 1. Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde.
Kontroler RAID	Brak.
Wbudowane porty	Min. 4 x USB z czego nie mniej niż 1x USB 3.0, 2xVGA z czego jeden na panelu przednim.

Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200
Zasilacze	Redundantne, Hot-Plug min. 700W każdy.
Bezpieczeństwo	• Zatrzask górnej pokrywy oraz blokada na ramce panela zamykana na klucz służąca do ochrony nieautoryzowanego dostępu do dysków twardych, • Możliwość wyłączenia w BIOS funkcji przycisku zasilania, • BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła, • Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą, • Moduł TPM 2.0, • Możliwość dynamicznego włączania I wyłączania portów USB na obudowie – bez potrzeby restartu serwera, • Możliwość wymazania danych ze znajdujących się dysków wewnątrz serwera – niezależne od zainstalowanego systemu operacyjnego, uruchamiane z poziomu zarządzania serwerem.
Diagnostyka	Serwer wyposażony w panel LCD umieszczony na froncie obudowy, umożliwiający wyświetlenie informacji o stanie procesora, pamięci, dysków, BIOS'u, zasilaniu oraz temperaturze.
System operacyjny	Windows Server 2022 Standard 16 core oraz licencja na dodatkowe 16 core (Licencja musi umożliwiać uruchomienie 4 wirtualnych maszyn w ramach serwera).
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej; • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera; • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera.
Oprogramowanie do zarządzania	Zamawiający posiada oprogramowanie do zarzadzania OpenManage Enterprise i wymaga, aby serwer posiadał możliwość wyposażenia w taką licencję.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklarację CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2016, Microsoft Windows 2019, Microsoft Windows 2022.
Warunki gwarancji	5 lat gwarancji producenta, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość rozszerzenia gwarancji przez producenta do 7 lat. Możliwość sprawdzenia statusu gwarancji poprzez stronę producenta podając unikatowy numer urządzenia oraz pobieranie uaktualnień mikrokodu oraz sterowników nawet w przypadku wygaśnięcia gwarancji serwera

Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim. Możliwość zdalnego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.
Dodatki	Rozbudowa obecnego serwera Dell PowerEdge R440 o kartę sieciową 25Gb Ethernet w standardzie SFP28 obsadzoną wkładkami 10Gb SFP+. Rozbudowa obecnego serwera Dell PowerEdge R750xs o dwie kompatybilne wkładki 10Gb SFP+.

Macierz dyskowa

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa do montażu w szafie rack 19" za pomocą dostarczonych dedykowanych elementów.. Macierz musi umożliwiać instalację min 25 dysków SFF.
Zasilanie	Oferowane urządzenie musi być przystosowane do zasilania z sieci AC oraz wyposażone w kable zasilające PDU. Macierz musi być wyposażona w zdublowany, redundantny system zasilania, umożliwiający prawidłową, nieprzerwaną pracę urządzenia w przypadku awarii dowolnego pojedynczego źródła zasilania.
Kontrolery dyskowe	Macierz wyposażona w minimum 2 kontrolery pracujące w trybie active-active. Akceptowalna architektura to symmetric active-active, to znaczy pracę kontrolerów w trybie zapewniającym dostęp do wolumenów logicznych (LUN) utworzonych w macierzy, z wykorzystaniem wszystkich dostępnych ścieżek (path) i portów kontrolerów bez wymuszania preferowanej ścieżki dostępu oraz z zapewnieniem automatycznego równoważenia obciążenia (load balancing). Kontrolery nie mogą pracować w trybie active-passive.
Wymagana przestrzeń	Fizyczna przestrzeń dyskowa zbudowana tylko i wyłącznie za pomocą dysków SSD SAS. Przestrzeń użytkowa po zbudowaniu RAID 6 z 1 dyskiem hot-spare lub przestrzenią hot-spare równą pojemności 1 dysku musi wynosić min 15,37 TB. Ze względów wydajnościowych oraz niezawodnościowych rozmiar pojedynczego dysku nie może być większy niż 4 TB, co przełoży się na większą liczbę dysków. Wymagana pojemność użytkowa rozumiana jest jako pojemność dostępna po konfiguracji RAID i odliczeniu rezerwy na dyski/przestrzeń spare i dostępna dla hostów bez uwzględnienia jakichkolwiek mechanizmów kompresji, czy deduplikacji. Dyski muszą być wyposażone w podwójne interfejsy. Niedopuszczalne są dyski SSD zbudowane w oparciu o chipset QLC ze względu na skróconą żywotność.
Zabezpieczenia dyskami SPARE	Możliwość definiowania przez administratora dysków SPARE lub odpowiedniej zapasowej przestrzeni dyskowej.
Pamięć Cache	Rozbudowa oferowanej macierzy, do co najmniej 80 szt dysków SSD SAS, bez wymiany kontrolerów macierzowych oraz bez rozbudowy o dodatkowe kontrolery, tylko poprzez dodawanie półek i dysków SSD SAS. Macierz nie może obsługiwać dysków HDD.
Pamięć Cache	Co najmniej 64GB pamięci cache na całą macierz (dwa kontrolery). Zamawiający nie dopuszcza możliwości zastosowania dysków SSD/NVMe lub kart pamięci FLASH jako rozszerzenia pamięci cache. Pamięć cache musi być zabezpieczona przed utratą danych w przypadku awarii zasilania poprzez funkcję zapisu zawartości pamięci cache na nieulotną pamięć.
Dostępne interfejsy	Razem kontrolery muszą udostępnić minimum 12 porty 10Gb SFP+ Eth. Wymagana możliwość rozbudowy o dodatkowe 8 portów 10Gb Eth bez konieczności wymiany lub zakupu nowych kontrolerów i klastrowania z kontrolerami oferowanymi w tym postępowaniu. Wszystkie moduły muszą posiadać wkładki optyczne SFP+. Macierz musi posiadać wbudowane min 4 porty SAS 12Gb/s do podłączenia półek dyskowych.
Obsługiwane protokoły	Wymagane wsparcie dla iSCSI.
Obsługiwane typy zabezpieczenia RAID	Kontrolery wyposażone w funkcjonalność konfiguracji poziomu RAID 6 lub równoważnego tolerującego jednoczesną awarię 2 dysków bez utraty danych.
Prezentacja dysków logicznych o pojemności większej niż zajmowana	Wymagana funkcjonalność tworzenia i prezentacji dysków logicznych (LUN) o pojemności większej niż zajmowana fizyczna przestrzeń dyskowych (ang. ThinProvisioning). Wymagana funkcjonalność zwrotu skasowanej przestrzeni dyskowej do puli zasobów wspólnych (ang. Space Reclamation). Macierz musi wspierać nie mniej niż 1024 LUNów. Wymagana możliwość tworzenia grup wolumenów. Max liczba LUNów w grupie wolumenów nie może być mniejsza niż 100. Wymagane dostarczenie w/w funkcjonalności na zainstalowaną przestrzeń dyskową.

przestrzeń dyskowa (ang. Thin Provisioning)	
Zarządzanie	Zarządzanie macierzą (wszystkimi kontrolerami) z poziomu pojedynczego interfejsu graficznego. Wymagane jest stałe monitorowanie stanu macierzy w tym monitorowanie wydajności obiektów takich jak: - cała macierz - kontrolery - porty front-end - dyski - LUNy - hosty Pod kątem parametrów takich jak: - operacje wejścia/wyjścia IOPS - przepustowość (KB/s lub MB/s) - czas odpowiedzi (latency) Wymagana możliwość monitorowania stanu żywotności dysków SSD SAS. Wymagana możliwość dostępu do historycznych danych wydajnościowych z poziomu GUI macierzy do co najmniej 2 lat wstecz lub jako równoważne dostarczenie fizycznego serwera z oprogramowaniem umożliwiającym zbieranie i przeglądanie danych historycznych. Wymagana możliwość konfigurowania zasobów macierzy. Jeżeli do obsługi powyższej funkcjonalności wymagane są dodatkowe licencje, ich dostarczenie jest wymagane na tym etapie postępowania.
Kopie wewnątrz macierzy	Tworzenie na żądanie tzw. migawkowej kopii danych (ang. snapshot) w ramach macierzy do wykorzystania w celu np. wykonywania kopii zapasowych. Snapshoty muszą być wykonywanie w technologii ROW (Redirect On Write). Macierz musi obsługiwać min 2000 snapshotów. Wymagane wsparcie dla snapshotów kaskadowych. Wymagana możliwość tworzenia harmonogramu wykonywania snapshotów oraz zabezpieczenia migawek przed modyfikacją lub usunięciem pod kątem szybkiego przywrócenia danych w przypadku ataku ransomware. Dostarczenie powyższych funkcjonalności jest wymagane na tym etapie postępowania na całą przestrzeń dyskową i na maksymalną liczbę snapshotów obsługiwanych przez oferowany model macierzy. Tworzenie na żądanie kopii danych typu klon w ramach macierzy za pomocą wewnętrznych kontrolerów macierzowych. Funkcjonalność ta musi umożliwiać synchronizację danych z wolumenu źródłowego na docelowy oraz resynchronizację danych z wolumenu docelowego na źródłowy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Kompresja	Macierz musi wspierać funkcjonalności kompresji danych w trybie in-line (w locie). Musi być możliwe włączenie kompresji per wolumen (LUN). Musi istnieć możliwość wyłączenia tych funkcjonalności na wybranych wolumenach (LUN). Dostarczenie licencji na tą funkcjonalność jest wymagane na tym etapie postępowania.
Replikacja danych	Możliwość zdalnej replikacji danych typu on-line (bez przerywania prezentacji wolumenów dyskowych) do macierzy tej samej rodziny w trybie asynchronicznym oraz synchronicznym przy wykorzystaniu portów FC lub IP. Funkcjonalność ta nie może wpływać na obciążenie serwerów podłączonych do macierzy. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Klaster macierzowy	Wsparcie dla technologii klastrowania macierzy dyskowych (ang. Storage Metro Cluster). Macierz musi dostarczać funkcjonalność klastra klasy "wysokiej dostępności" tj. zapewnienia wysokiej dostępności zasobów dyskowych macierzy dla podłączonych platform oprogramowania i sprzętowych z wykorzystaniem synchronicznej replikacji danych po protokole FC lub IP pomiędzy 2 macierzami. Pod użytym pojęciem "wysoka dostępność zasobów dyskowych" należy rozumieć zapewnienie bezprzerwowego działania środowiska (aplikacja/system operacyjny/serwer) podłączonego do macierzy (macierz preferowana) w przypadku wystąpienia awarii logicznego połączenia z tą macierzą bądź awarii samej macierzy powodujących dla danego środowiska brak dostępu do zasobów macierzy preferowanej. Funkcjonalność klastra "wysokiej dostępności" pozwala na automatyczne przełączanie obsługi środowisk produkcyjnych z macierzy preferowanej na niepreferowaną w przypadku awarii macierzy preferowanej (tzw. automated failover). Wymagany jest również automatyczny failover z macierzy niepreferowanej na preferowaną. Dopuszczalne jest zastosowanie tzw arbitra (serwer quorum). Dostarczenie tej funkcjonalności nie jest wymagane na tym etapie postępowania.

Priorytety zadań	Macierz musi posiadać możliwość zapewnienia ciągłości biznesu na oczekiwanym poziomie usług (QoS) poprzez definicję polityk QoS w oparciu o maksymalne progi wydajności IOPS i MB/s. Musi istnieć możliwość określenia polityk QoS na poziomie wolumenów. Dostarczenie tej funkcjonalności jest wymagane na tym etapie postępowania.
Integralność danych	Macierz musi oferować wsparcie dla zachowania integralności danych na całej ścieżce transferu (ang. End-to-End) zgodnego ze standardem/specyfikacją T10 PI.
Wspierane systemy operacyjne	Wsparcie, dla co najmniej Microsoft Server Windows 2016/2019, VMware 6.x/7.x, Linux RedHat 7.x/8.x, CentOS 7.x/8.x
Serwisowalność	Wymagane uaktualnianie firmware-u kontrolerów macierzy bez przerywania dostępu do danych. Macierz przystosowana do napraw w miejscu zainstalowania oraz wymiany elementów bez konieczności jej wyłączania. Macierz musi umożliwiać zdalne zarządzanie. Urządzenie musi być fabrycznie nowe, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia do Zamawiającego i pochodzić z autoryzowanego kanału dystrybucji producenta, a także musi być objęte serwisem producenta lub autoryzowanego partnera serwisowego na terenie RP. Wymagana gwarancja 5 lata w trybie 9x5 NBD onsite. Zamawiający wymaga pozostawienie uszkodzonych dysków u Zamawiającego.

Wdrożenie:
- instalacja dostarczonego sprzętu (serwer, macierz) w miejscu wskazanym przez Zamawiającego,
- aktualizacja firmware serwerów oraz macierzy do najnowszej wersji,
- instalacja i konfiguracja systemu operacyjnego na dostarczonym serwerze,
- konfiguracja macierzy dyskowej. Udostępnienie zasobów macierzy do dostarczonego serwera,
- instalacja i konfiguracja Active Directory na dostarczonym serwerze,
- instalacja dysków do obecnej macierzy HPE,
- instalacja karty sieciowej do obecnego serwera Dell.

UWAGA
Do oferty należy załączyć certyfikaty:
- Data Center Virtualization 2023 (1szt)
- ISO 9001:2015 oraz 27001:2017 dla Wykonawcy w zakresie sprzedaży, montażu i wdrożenia sprzętu komputerowego oraz systemów informatycznych.

Dyski twarde do macierzy dyskowej

Rozbudowa macierzy o 8 dysków HPE MSA 2.4TB 12G SAS 10K 2.5in 512e HDD. Zamawiający wymaga dysków z oficjalnego kanału sprzedaży HPE świadczącego finalnie gwarancje dla całości produktu.

Przełączniki

Przełączniki typ 1 – 3 sztuki

1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy
2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).

8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)
11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.
13. Pobór mocy nie może być większy niż 70W.
14. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
15. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
16. Tablica adresów MAC o wielkości minimum 16000 pozycji
17. Obsługa Jumbo Frames
18. Obsługa sFlow lub Netflow
19. Obsługa skryptów w języku Python
20. Obsługa REST API
21. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
22. Obsługa RMON (minimum grupy 1,2,3 i 9)
23. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
24. Obsługa standardu 802.1v
25. Obsługa protokołu MVRP
26. Wsparcie dla VXLAN
27. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
28. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
29. Obsługa Secure FTP lub SCP
30. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
31. Obsługa SNTPv4 lub NTP
32. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
33. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3
34. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
35. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
36. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
37. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
38. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
39. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
40. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera
41. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie

42. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
43. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+
44. Wbudowany serwer DHCP
45. Obsługa blokowania nieautoryzowanych serwerów DHCP
46. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
47. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
48. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
49. Wbudowana sonda IP SLA
50. Zakres pracy od 0 do 45°C
51. Przełącznik w obudowie 19". Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm.
52. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
53. Wraz z każdym przełącznikiem należy dostarczyć:

a) 1 x kabel DAC SFP+ do SFP+ 10Gb/s minimum 1m
b) 2 x wkładka SFP+ 10Gb/s MM – zezwala się na stosowanie zamienników
c) 2 x kabel światłowodowy LC - LC multimode minimum OM3 1m
d) 2 x kabel światłowodowy LC - LC multimode minimum OM3 3m
e) 1 x organizer kabli do szafy rack 19" 1U

54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
55. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Załączyć do oferty oświadczenie producenta potwierdzające w/w wymogi.

Przełącznik typ 2 – 1 szt.

1. Minimum 48 portów 10/100/1000BASE-T umieszczonych z przodu obudowy ze wsparciem dla protokołu 802.3at (PoE+)
2. Minimum 4 porty 1/10gigabitowe SFP+ umieszczone z przodu obudowy
3. Przepustowość: minimum 176 Gb/s (pełna prędkość, tzw. wire-speed, na wszystkich portach przełącznika)
4. Wydajność: minimum 130 Mp/s
5. Bufor pakietów: minimum 7.5 MB
6. Minimum 8GB pamięci operacyjnej
7. Minimum 15GB wewnętrznej pamięci nieulotnej typu Flash (CF, SSD, SD, eUSB, SPI Flash).
8. Dedykowany port do zarządzania poza pasmowego (Ethernet, RJ-45), w pełni niezależny od portów liniowych
9. Dedykowany port konsoli USB
10. Port USB 2.0 (niezależny od portu konsoli USB)

11. Interfejs Bluetooth (dopuszcza się rozwiązanie w postaci adaptera Bluetooth, podłączanego do portu USB przełącznika, przsy czym adapter musi pochodzić od tego samego producenta co przełącznik)
12. Przełączniki tego samego typu muszą posiadać funkcję łączenia w stos (wirtualny przełącznik) złożony z minimum 8 urządzeń. Zarządzanie stosem musi odbywać się z jednego adresu IP. Z punktu widzenia zarządzania przełączniki muszą tworzyć jedno logiczne urządzenie (nie dopuszcza się rozwiązań typu klaster). Jeżeli łączenie w stos wymaga dodatkowych modułów lub licencji to dostarczenie ich jest wymagane w ramach tego postępowania. Dostępne metody łączenia przełączników muszą umożliwiać realizację stosów na odległość co najmniej 300m.
13. Wewnętrzny zasilacz 230V zapewniający budżet mocy PoE na poziomie nie niższym niż 740W. Pobór mocy (bez PoE) nie może być większy niż 80W.
14. Wielkość tablicy routingu: minimum 2000 wpisów IPv4, 1000 wpisów IPv6
15. Wielkość tablicy ARP co najmniej 8000 wpisów, wielkość tablicy ND co najmniej 8000 wpisów
16. Tablica adresów MAC o wielkości minimum 16000 pozycji
17. Obsługa Jumbo Frames
18. Obsługa sFlow lub Netflow
19. Obsługa skryptów w języku Python
20. Obsługa REST API
21. Wbudowany mechanizm monitoringu, analizy i troubleshootingu anomalii i problemów oraz zbierania danych sieciowych. Musi być możliwe podejmowanie akcji na podstawie zdefiniowanych polityk oraz wgrywanie i eksport skryptów pozwalających na indywidualizację monitorowanych danych. Musi być dostępna publicznie strona producenta zawierająca zatwierdzone przez niego, gotowe do użycia skrypty.
22. Obsługa RMON (minimum grupy 1,2,3 i 9)
23. Obsługa 4094 tagów IEEE 802.1Q oraz 2000 jednoczesnych sieci VLAN
24. Obsługa standardu 802.1v
25. Obsługa protokołu MVRP
26. Wsparcie dla VXLAN
27. Dostęp do urządzenia przez konsolę szeregową, HTTPS, SSHv2, SNMPv3, dedykowaną aplikację na urządzenia mobilne
28. Obsługa Rapid Spanning Tree (802.1w) i Multiple Spanning Tree (802.1s)
29. Obsługa Secure FTP lub SCP
30. Obsługa łączy agregowanych zgodnie ze standardem 802.3ad Link Aggregation Protocol (LACP)
31. Obsługa SNTPv4 lub NTP
32. Wsparcie dla IPv6 (IPv6 host, dual stack, MLD snooping, ND snooping)
33. Obsługa protokołów rutingu: ruting statyczny, OSPF, OSPFv3
34. Obsługa ruchu multicast: IGMPv1/v2/v3 (co najmniej 1000 grup), MLD (co najmniej 1000 grup)
35. Obsługa IEEE 802.1AB Link Layer Discovery Protocol (LLDP) i LLDP Media Endpoint Discovery (LLDP-MED)
36. Automatyczna konfiguracja VLAN dla urządzeń VoIP oparta co najmniej o: RADIUS VLAN (użycie atrybutów RADIUS i mechanizmu LLDP-MED)
37. Mechanizmy związane z zapewnieniem jakości usług w sieci: prioryteryzacja zgodna z 802.1p, ToS, TCP/UDP, DiffServ, wsparcie dla 8 kolejek sprzętowych, rate-limiting
38. Obsługa uwierzytelniania użytkowników zgodna z 802.1x
39. Obsługa uwierzytelniania użytkowników w oparciu o adres MAC i serwer RADIUS
40. Obsługa uwierzytelniania użytkowników w oparciu o stronę WWW z użyciem zewnętrznego serwera.
41. Obsługa uwierzytelniania wielu użytkowników na tym samym porcie w tym samym czasie
42. Obsługa autoryzacji logowania do urządzenia za pomocą serwerów RADIUS albo TACACS+
43. Obsługa autoryzacji komend wydawanych do urządzenia za pomocą serwerów RADIUS albo TACACS+

44. Wbudowany serwer DHCP
45. Obsługa blokowania nieautoryzowanych serwerów DHCP
46. Obsługa mechanizmu wykrywania łączy jednokierunkowych typu Device Link Detection Protocol (DLDP), Uni-Directional Link Detection (UDLD), lub równoważnego
47. Ochrona przed rekonfiguracją struktury topologii Spanning Tree (BPDU port protection)
48. Obsługa list kontroli dostępu (ACL) bazujących na porcie lub na VLAN z uwzględnieniem adresów, MAC, IP i portów TCP/UDP. Co najmniej 5000 wpisów typu ingress i 2000 wpisów typu egress dla IPv4 i MAC
49. Wbudowana sonda IP SLA
50. Zakres pracy od 0 do 45°C
51. Przełącznik w obudowie 19". Maksymalna wysokość obudowy 1U, maksymalna głębokość obudowy 35 cm.
52. Wraz z każdym przełącznikiem należy dostarczyć:

a) 1 x kabel DAC SFP+ do SFP+ 10Gb/s 3m
b) 2 x wkładka SFP+ 10Gb/s MM – zezwala się na stosowanie zamienników
c) 2 x kabel światłowodowy LC - LC multimode minimum OM3 1m
d) 2 x kabel światłowodowy LC - LC multimode minimum OM3 3m
e) 1 x organizer kabli do szafy rack 19" 1U

53. Jeżeli do działania któregokolwiek z wymienionych protokołów i funkcji wymagana jest dodatkowa licencja to należy ją dostarczyć w ramach tego postępowania
54. Wszystkie dostępne na przełączniku funkcje (tak wyspecyfikowane jak i nie wyspecyfikowane) muszą być dostępne przez cały okres jego użytkowania (permanentne), nie dopuszcza się licencji czasowych i subskrypcji.
55. Dożywotnia (minimum 5 lat po zakończeniu produkcji, przy czym, jeżeli data zakończenia produkcji jest ogłoszona to nie może być ona krótsza niż 2 lata po dostarczeniu sprzętu) gwarancja producenta obejmująca wszystkie elementy przełącznika (również zasilacze i wentylatory) zapewniająca wysyłkę sprzętu na podmianę maksymalnie na następny dzień roboczy. Serwis musi zapewniać również dostęp do poprawek i aktualizacji oprogramowania oraz wsparcia technicznego przez cały okres trwania gwarancji. Serwis musi być świadczony bezpośrednio przez producenta sprzętu w języku polskim. Cała komunikacja odbywać się musi bezpośrednio pomiędzy Zamawiającym i producentem sprzętu. Załączyć do oferty oświadczenie producenta potwierdzające w/w wymogi.

Wdrożenie:
• Instalacja w ustalonym z zamawiającym miejscu,
• Połączenie z istniejącymi elementami infrastruktury,
• Stworzenie stosu przełączników,
• Konfiguracja uzgodnionej funkcjonalności L2 (VLANy, agregacje, UDLD/DLDP, STP),
• Konfiguracja uzgodnionej funkcjonalności L3 (adresy, bramy, DNSy, NTP, syslog)
• Konfiguracja uzgodnionych funkcjonalności bezpieczeństwa (arp protect, dhcp snooping)
• Konfiguracja połączenia pomiędzy serwerowniami (po stronie Wykonawcy wymagane jest przygotowanie odpowiednich połączeń fizycznych)
• Szkolenie z obsługi

UWAGA
Do oferty należy załączyć certyfikaty:
• Routing i switching oferowanych przełączników (2 szt certyfikatów)
• ISO 9001:2015 oraz 27001:2017 dla Wykonawcy w zakresie sprzedaży, montażu i wdrożenia sprzętu komputerowego oraz systemów informatycznych.

System zabezpieczający pocztę elektroniczną - Email Secure Gateway.

Wymagania ogólne

System ochrony poczty musi zapewniać kompleksową ochronę antyspamową, antywirusową oraz antyspyware’ową bez limitu licencyjnego na ilość chronionych kont użytkowników.
System musi zapewniać integrację się z posiadanymi rozwiązaniami zabezpieczeń zamawiającego FortiGate. Dane IoC oraz inne dane telemetryczne muszą być udostępniane do zastosowanych już rozwiązań w celu zwiększenia bezpieczeństwa całej infrastruktury. System musi łączyć obecne rozwiązania by zidentyfikować wielowektorowe kampanie ataków. System musi zapewniać przepływ informacji by umożliwić automatyzację operacji bezpieczeństwa.
Dopuszcza się aby poszczególne elementy wchodzące w skład systemu ochrony były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia w środowisku wirtualnym. W przypadku implementacji programowej dostawca musi zapewnić platformę w postaci odpowiednio zabezpieczonego systememu operacyjnego, na którym będzie instalowane rozwiązanie. Platformy muszą mieć możliwość uruchomienia na co najmniej następujących hypervisorach: VMware vSphere Hypervisor ESX/ESXi 6.0, 6.7, 7.0 and higher, Microsoft Hyper-V Server 2008 R2, 2012 and 2012 R2, 2016, 2019, 2022, KVM qemu 2.12.1 and higher, Citrix XenServer v5.6sp2, 6.0 and higher; Open Source XenServer 7.4 and higher, Alibaba Cloud BYOL, AWS BYOL and On-Demand, Azure BYOL and On-Demand, Google Cloud Platform BYOL, Oracle Cloud Infrastructure BYOL. Dla zapewnienia wysokiej sprawności i skuteczności działania rozwiązanie musi pracować w oparciu o komercyjne bazy zabezpieczeń.

Dostarczone rozwiązanie musi mieć możliwość pracy w każdym trybów:

1. Tryb Gateway.
2. Tryb transparentny (nie wymaga rekonfiguracji istniejącego systemu poczty elektronicznej).

Parametry fizyczne systemu antyspamowego

System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności co najmniej 1 TB.

Ogólne funkcje systemu ochrony poczty:

Dostarczany system obsługi i ochrony poczty musi zapewniać poniższe funkcje:
1. Wsparcie dla co najmniej 20 domen pocztowych.
2. System musi realizować skanowanie antyspamowe i antywirusowe z wydajnością min. 25 tys. wiadomości/godzinę.
3. Polityki filtrowania poczty tworzone co najmniej w oparciu o: adresy mailowe, nazwy domenowe, adresy IP (w szczególności powinna być możliwość definiowania reguł all-all).
4. Email routing w oparciu o reguły lokalne lub w oparciu o zewnętrzny serwer LDAP.
5. Zarządzanie kolejkami wiadomości (np. reguły opóźniania dostarczenia wiadomości).
6. Możliwość ograniczenia ilości poczty wychodzącej do chronionych domen w oparciu o nie mniej niż: ilość jednoczesnych sesji, maksymalną liczbę wiadomości w ramach sesji, maksymalną liczbę odbiorców w zadanym czasie.
7. Ochrona i analiza zarówno poczty przychodzącej jak i wychodzącej.
8. Szczegółowe, wielowarstwowe polityki wykrywania spamu oraz wirusów.
9. Możliwość tworzenia polityk kontroli Antywirusowej oraz Antyspamowej w oparciu o użytkownika i atrybuty zwracane z zewnętrznego serwera LDAP.
10. Kwarantanna poczty z dziennym podsumowaniem dla użytkownika z możliwością samodzielnego zwalniania bądź usuwania wiadomości z kwarantanny przez użytkownika.
11. Możliwość poddania ponownemu skanowaniu (antywirus, sandbox) wiadomości w momencie uwalniania ich z kwarantanny użytkownika lub administratora.
12. Dostęp do kwarantanny użytkownika możliwy poprzez WebMail.
13. Archiwizacja poczty przychodzącej i wychodzącej w oparciu o polityki.

14. Możliwość przechowywania poczty oraz jej backup realizowany lokalnie na dysku systemu oraz na zewnętrznych zasobach, co najmniej: NFS, iSCSI.
15. Białe i czarne listy adresów mailowych definiowane globalnie oraz dla domen wskazanych przez administratora systemu.
16. Białe i czarne listy adresów mailowych dla poszczególnych użytkowników.
17. Skanowanie załączników zaszyfrowanych. Odszyfrowywanie ich w oparciu o nie mniej niż: słowa zawarte w wiadomości pocztowej, wbudowaną listę haseł, listę haseł zdefiniowaną przez użytkownika.

Kontrola antywirusowa i ochrona przed malware

W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1. Skanowanie antywirusowe wiadomości SMTP.
2. Kwarantannę dla zainfekowanych plików.
3. Skanowanie załączników skompresowanych.
4. Definiowanie komunikatów powiadomień w języku polskim.
5. Blokowanie załączników w oparciu o typ pliku.
6. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antywirusowej.
7. Moduł kontroli antywirusowej musi mieć możliwość współpracy z dedykowaną, komercyjną platformą (sprzętową lub wirtualną) lub usługą w chmurze typu Sandbox w celu rozpoznawania nieznanych dotąd zagrożeń. Rozwiązanie musi umożliwiać zatrzymanie poczty w dedykowanej kolejce wiadomości do momentu otrzymania werdyktu.
8. Definiowanie różnych akcji dla poszczególnych metod wykrywania wirusów i malware'u. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, zastąpienie podejrzanej treści lub załącznika, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
9. Ochronę typu wirus outbrake.
10. Ochronę przed zagrożeniami zawartymi wiadomościach pocztowych i w załącznikach (nie mniej niż: pliki MS Office, PDF, HTML, tekstowe) poprzez usuwanie treści będących zagrożeniem (makra, adresy URL zagnieżdżone w plikach, skrypty, ActiveX) i dostarczaniem oczyszczonych w ten sposób wiadomości.

Kontrola antyspamowa

System musi zapewniać poniższe funkcje i metody filtrowania spamu:
1. Reputacja adresów źródłowych IP oraz domen pocztowych w oparciu o bazy producenta.
2. Filtrowanie poczty w oparciu o sumy kontrolne wiadomości dostarczane przez producenta rozwiązania.
3. Szczegółowa kontrola nagłówka wiadomości.
4. Analiza Heurystyczna.
5. Współpraca z zewnętrznymi serwerami RBL, SURBL.
6. Filtrowanie w oparciu o filtry Bayes'a z możliwością uczenia przez administratora globalnie dla całego systemu lub dla poszczególnych chronionych domen.
7. Możliwością dostrajania filtrów Bayes'a przez poszczególnych użytkowników.
8. Wykrywanie spamu w oparciu o analizę plików graficznych oraz plików PDF.
9. Kontrola w oparciu o Greylisting oraz SPF.
10. Filtrowanie treści wiadomości i załączników.
11. Kwarantanna zarówno użytkowników jak i systemowa z możliwością edycji nagłówka wiadomości.
12. Możliwość zdefiniowania nie mniej niż 60 polityk kontroli antyspamowej.
13. Ochrona typu outbrake.
14. Filtrowanie poczty w oparciu o kategorie URL (co najmniej: malware, hacking).
15. Możliwość skanowania linków znajdujących się w przesyłkach pocztowych, w momencie ich kliknięcia przez adresata.

16. Możliwość wykrywania i ochrony przed podszywaniem się (spoofing) pod wiadomości wysyłane przez osoby na stanowiskach kierowniczych (C-level)
17. Definiowanie różnych akcji dla poszczególnych metod wykrywania spamu. Powinny one obejmować co najmniej: tagowanie wiadomości, dodanie nowego nagłówka, akcje discard lub reject, dostarczenie do innego serwera, powiadomienie administratora.
Ochrona przed atakami na usługę poczty
System musi zapewniać poniższe funkcje i metody filtrowania:
1. Ochrona przed atakami na adres odbiorcy (m.in. email bombing).
2. Definiowanie maksymalnej ilości wiadomości pocztowych otrzymywanych w jednostce czasu.
3. Definiowanie maksymalnej liczby jednoczesnych sesji SMTP w jednostce czasu.
4. Kontrola Reverse DNS (ochrona przed Anty-Spoofing).
5. Weryfikacja poprawności adresu e-mail nadawcy.

Funkcje logowania i raportowania

W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1 .Logowanie do zewnętrznego serwera SYSLOG.
2. Logowanie zmian konfiguracji oraz krytycznych zdarzeń systemowych np. w przypadku przepełnienia dysku.
3. Logowanie informacji na temat spamu oraz niedozwolonych załączników.
4. Możliwość podglądu logów w czasie rzeczywistym jak również danych historycznych.
5. Możliwość analizy przebiegu sesji SMTP.
6. Powiadamianie administratora systemu w przypadku wykrycia wirusów w przesyłanych wiadomościach pocztowych.
7. Predefiniowane szablony raportów oraz możliwość ich edycji przez administratora systemu.
8. Możliwość generowania raportów zgodnie z harmonogramem lub na żądanie administratora systemu.

Aktualizacje sygnatur, dostęp do bazy spamu

W tym zakresie dostarczony system ochrony poczty musi zapewniać:
1. Pracę w oparciu o bazę spamu oraz url uaktualniane w czasie rzeczywistym.
2. Planowanie aktualizacji szczepionek antywirusowych zgodnie z harmonogramem co najmniej raz na godzinę.

Zarządzanie

System ochrony poczty musi zapewniać poniższe funkcje:
1. System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH.
2. Możliwość modyfikowania wyglądu interfejsu zarządzania oraz interfejsu WebMail z opcją wstawienia własnego logo firmy.
3. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.
Wdrożenie:
- Dostawa oprogramowania
- Instalacja oprogramowania w środowisku zamawiającego
- Konfiguracja warstwy sieciowej
- Konfiguracja ustawień systemowych
- Konfiguracja profilów bezpieczeństwa
- Konfiguracja funkcji Sandbox
- Integracja z obecnym systemem pocztowym zamawiającego
- Konfiguracja logowania do FortiAnalyzera
- Szkolenie z obsługi

Serwisy i licencje

System musi być dostarczony w modelu „na własność" tj. Niewyku pienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.
W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować:

- Kontrola Antyspam,
- URL Filtering,
- kontrola antywirusowa,
- ochrona typu Virus Outbrake,
- Sandbox w chmurze,
- ochrona typu Click Protect,
- Content Disarm & Reconstruction,
- Business Email Compromise na okres 24 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

Opisy do wymagań ogólnych

W przypadku istnienia takiego wymogu w stosunku do technologii objętej przedmiotem niniejszego postępowania (tzw. produkty podwójnego zastosowania), Dostawca 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.

CZĘŚĆ II. Szkolenia z zakresu cyberbezpieczeństwa

Przedmiotem jest kompleksowa usługa „Podnoszenia Świadomości Bezpieczeństwa" (Security Awareness), umożliwiająca przeprowadzenie kampanii edukacyjnej z zakresu podstaw bezpieczeństwa w internecie. Dedykowana jest użytkownikom Zamawiającego i świadczona przez okres 6 miesięcy w uzgodnieniu z Zamawiającym.

Usługa musi zawierać:
I. Moduł szkolenia pracowników:
1. Platformę szkoleniową zawierającą minimum 45 szkoleń, dostępnych w języku polskim, w postaci filmów i prezentacji, zakończonych testami lub quizami sprawdzającymi przyswojenie przedstawianego materiału merytorycznego.
a) Szkolenia muszą zapewniać zakres tematyczny co najmniej w ujęciu:

- ✓ Podstawy bezpiecznego internetu
- ✓ Bezpieczeństwo poczty
- ✓ Załączniki w poczcie elektronicznej
- ✓ Phishing
- ✓ Spyware/malware
- ✓ Bezpieczeństwo danych osobowych RODO/GDRP
- ✓ Bezpieczne hasła

- ✓ Menedżery haseł
- ✓ Bezpieczeństwo urządzeń mobilnych
- ✓ Uwierzytelnianie wieloskładnikowe (MFA)
- ✓ Bezpieczna praca zdalna
- ✓ Bezpieczna praca w biurze
- ✓ Sieci społeczne
- ✓ Socjotechnika stosowana
- ✓ Zakupy w internecie

b) Użytkownicy powinni być podzieleni na grupy, dla których będą przygotowane indywidualne harmonogramy szkoleń oraz dedykowane kampanie phishingowe.
c) Łączny czas trwania wszystkich materiałów szkoleniowych powinien wynosić co najmniej 8 godzin.

2. Dedykowaną platformę phishingową pozwalającą na generowanie i wysyłanie spreparowanych maili phishingowych do wszystkich użytkowników usługi oraz na generowanie, co najmniej, poniższych typów wiadomości e-mail:

a) z linkiem prowadzącym do stronnym internetowej,
b) z linkiem do portalu podszywającego się pod usługodawcę i pozwalającego na logowanie (weryfikację, czy użytkownicy są gotowi na fałszywej stronie portalu zalogować się swoim loginem i hasłem); platforma musi zapewniać bezpieczeństwo takiej operacji,
c) z załącznikiem (szyfrowanym i niezaszyfrowanym) zawierającym potencjalnie niebezpieczny kod,
d) z załącznikiem w postaci dokumentu Word lub Excel zawierającym potencjalnie niebezpieczny kod.

W przypadku, gdy użytkownik pozwoli się oszukać, platforma musi posiadać możliwość automatycznego skierowania takiego użytkownika na dodatkowe szkolenie lub ponowne wykonanie jednego z wcześniej ukończonych szkoleń.

3. Dedykowaną platformę dostarczającą raporty obejmujące minimum:

a) status wykonania szkoleń przez użytkowników, z podziałem na grupy i uwzględnieniem terminu wykonania szkoleń oraz wyniku quizów i testów,
b) status kampanii, wraz z raportem o liczbie wysłanych e-maili oraz szczegółach zwierających informację: kto otworzył wiadomość, kto i kiedy pozwolił się oszukać, kto otworzył załącznik, jaka była platforma z jakiej wykonał tę akację oraz szczegółowe daty wykonania tych operacji.

W ramach świadczonej usługi usługodawca musi:

- przygotować platformę do świadczenia usługi, założyć konta dla użytkowników oraz sprawdzić techniczne elementy związane z zapewnieniem dostarczenia wiadomości phishingowych z platformy do użytkowników,
- zaproponować do akceptacji Zamawiającego szczegółowy harmonogram szkoleń dopasowany do okresu świadczenia usługi,
- zaplanować na podstawie harmonogramu całą kampanię szkoleniową i dostarczyć ją użytkownikom za pośrednictwem dedykowanych wiadomości e-mail,
- dostarczać pełny raport z realizacji szkoleń dla użytkowników oraz przeprowadzonych kampanii po zakończeniu każdego modułu szkoleniowego oraz zbiorcze raporty końcowe,
- wprowadzić zmiany w harmonogramie i zakresie szkoleń w przypadku potrzeby modyfikacji, zmian kolejności szkoleń lub liczby użytkowników (nie więcej niż 6 zmian w okresie trwania usługi).

Wymagania dodatkowe:
Usługa ma być świadczona z centrum danych znajdującym się na terenie Unii Europejskiej. Dostawca platformy musi zapewnić całkowite usunięcie danych użytkowników po zakończeniu realizacji usługi.

Wszystkie moduły (platforma szkoleniowa, platforma phishingowa i moduł raportowania) muszą pochodzić od jednego producenta.
Dla zapewnienia wysokiego poziomu usług, podmiot świadczący usługę musi posiadać certyfikat ISO 9001 w zakresie świadczenia usług. Zgłoszenia i komunikacja z usługodawcą będą przyjmowane w języku polskim w trybie 8x5, przez dedykowany portal serwisowy dostępny w sieci internet oraz infolinię w języku polskim 8x5. Czas reakcji usługodawcy nie może być dłuższy niż 1 godzina – reakcja w postaci połączenia telefonicznego lub odpowiedzi w portalu serwisowym.
Do oferty należy załączyć oświadczenie usługodawcy o gotowości świadczenia takiej usługi wraz z certyfikatem ISO 9001.

II. Moduł szkolenia specjalisty.

1. Szkolenie na terenie województwa zachodniopomorskiego min. 21 roboczogodzin przeprowadzone przez pracownika Wykonawcy z certyfikatem minimum NSE8 w zakresie:

- Konfiguracja sieć FortiGate przy użyciu domyślnych ustawień fabrycznych
- Konfiguracja dostęp administratora do FortiGate
- Omówienie używania GUI i CLI
- Kontrola dostępu sieciowych do skonfigurowanych sieci za pomocą zasad zapory sieciowej
- Zastosowanie przekierowań portów, źródłowy NAT i docelowy NAT
- Analizy tabeli tras FortiGate
- Trasowanie pakietów przy użyciu tras statycznych i opartych na zasadach w przypadku wdrożeń wielościeżkowych i z równoważeniem obciążenia
- Uwierzytelnianie użytkowników, korzystając z zasad zapory sieciowej
- Monitorowanie użytkowników zapory sieciowej z poziomu interfejsu graficznego FortiGate
- Konfiguracja dostępów Fortinet Single Sign-On (FSSO) do usług sieciowych, zintegrowany z Microsoft Active Directory (AD)
- Omówienie funkcji szyfrowania i certyfikatów
- Weryfikacja ruchu zabezpieczonego protokołem SSL/TLS, aby zapobiec szyfrowaniu używanemu do omijania zasad bezpieczeństwa
- Konfiguracja profili zabezpieczeń, aby neutralizować zagrożenia i nadużycia, w tym wirusy, torrenty i nieodpowiednie strony internetowe
- Zastosowanie techniki kontroli aplikacji do monitorowania i kontrolowania aplikacji sieciowych, które mogą korzystać ze standardowych lub niestandardowych protokołów i portów
- Analiza SSL VPN, aby zapewnić bezpieczny dostęp do swojej sieci prywatnej
- Omówienie konfiguracji tuneli IPsec VPN pomiędzy dwoma urządzeniami FortiGate
- Konfiguracja routingu statycznego
- Omówienie konfiguracji zastosowań SD-WAN
- Identyfikacja cech sieci Fortinet Security Fabric
- Uruchomienie urządzenia FortiGate jako klaster HA, aby zapewnić odporność na awarie i wysoką wydajność
- Diagnoza i rozwiązania dla typowych problemów Fortinet.

2. Szkolenie na terenie województwa zachodniopomorskiego przeprowadzone przez pracownika Wykonawcy min. 21 roboczogodzin w zakresie:

- Instalacja i konfiguracja kontrolerów domeny.
- Zarządzanie obiektami w usługach AD DS za pomocą narzędzi graficznych i programu Windows PowerShell.

- Wdrażanie usługi AD DS w złożonych środowiskach.
- Wdrażanie administracja usługami zarządzania prawami dostępu w usłudze Active Directory (AD RMS).
- Implementacja witryny AD DS oraz konfiguracja replikacji i zarządzaj nią.
- Wdrażanie i zarządzanie obiektami zasad grupy (GPO).
- Zarządzanie ustawieniami użytkowników za pomocą obiektów GPO.
- Bezpieczeństwo AD DS i konta użytkowników.
- Wdrożenie organizacji urzędów certyfikacji (CA) i zarządzanie nią za pomocą usług AD CS.
- Wdrożenie certyfikatów wraz z zarządzaniem.
- Wdrożenie i administracja usługami AD FS.
- Wdrożenie synchronizacji między usługami AD DS i usługą Azure AD.
- Monitoring, rozwiązywanie problemów i zapewnienie ciągłość biznesową usług AD DS.

3. Szkolenie na terenie województwa zachodniopomorskiego min. 21 roboczogodzin przeprowadzone przez pracownika Wykonawcy z certyfikatem VMware Professional min. 6.5 w zakresie:

- Opis komponentów vSphere i ich funkcję w infrastrukturze
- Instalacja i skonfiguruj hosty VMware ESXi
- Wdrozenie i konfiguracja VMware vCenter Server Appliance
- Używanie VMware vSphere Client do zarządzania zasobami vCenter Server i konfiguracją vCenter Server
- Zarządzanie, monitoring, tworzenie kopi zapasowych i ochrona urządzenie vCenter Server
- Tworzenie sieci witalnych za pomocą standardowych przełączników vSphere
- Opis technologi pamięci masowej obsługiwane przez vSphere
- Konofiguracja pamięć wirtualną przy użyciu pamięci masowej iSCSI i NFS
- Tworzenie i zarządzanie magazynami danych VMware vSphere VMFS
- Wykorzystanie vSphere do tworzenia maszyn wirtualnych, szablonów, klonów i migawek
- Tworzenie zawartości i wdrażaj maszyny wirtualne na podstawie szablonów w bibliotece
- Zarządzanie wykorzystaniem zasobów maszyny wirtualnej
- Migracja maszyn wirtualnych za pomocą VMware vSphere vMotion i VMware vSphere Storage vMotion
- Tworzenie klastra vSphere i zarządzanie nim z obsługą VMware vSphere High Availability i VMware vSphere Distributed Resource Scheduler
- Omówienie rozwiązania do zarządzania cyklem życia vSphere
- Wykorzystanie VMware vSphere Update Manager, aby zastosować poprawki i przeprowadzić aktualizacje na hostach ESXi i maszynach wirtualnych

Rozwiązania równoważne.

W przypadku użycia w dokumentacji opisującej przedmiot zamówienia odniesień do norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych Zamawiający dopuszcza rozwiązania równoważne opisywanym. Wykonawca analizując dokumentację projektową powinien założyć, że każdemu odniesieniu użytemu w dokumentacji projektowej towarzyszy wyraz „lub równoważne".

W przypadku, gdy w dokumentacji opisującej przedmiot zamówienia zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować materiały lub urządzenia równoważne, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie negatywnie na prawidłowe funkcjonowanie rozwiązań przyjętych w dokumentacji projektowej. Wykonawca, który

zastosuje urządzenia lub materiały równoważne będzie obowiązany wykazać w trakcie realizacji zamówienia, że zastosowane przez niego urządzenia i materiały spełniają wymagania określone przez Zamawiającego. Użycie w dokumentacji opisującej przedmiot zamówienia etykiety oznacza, że Zamawiający akceptuje wszystkie etykiety potwierdzające, że dane dostawy spełniają równoważne wymagania określonej przez zamawiającego etykiety. W przypadku gdy wykonawca z przyczyn od niego niezależnych nie może uzyskać określonej przez zamawiającego etykiety lub równoważnej etykiety, zamawiający, w terminie, przez siebie wyznaczonym akceptuje inne odpowiednie przedmiotowe środki dowodowe, w szczególności dokumentację techniczną producenta, o ile dany wykonawca udowodni, że dostawy, które mają zostać przez niego wykonane, spełniają wymagania określonej etykiety lub określone wymagania wskazane przez zamawiającego. Użycie w dokumentacji opisującej przedmiot zamówienia wymogu posiadania certyfikatu wydanego przez jednostkę oceniającą zgodność lub sprawozdania z badań przeprowadzonych przez tę jednostkę jako środka dowodowego potwierdzającego zgodność z wymaganiami lub cechami określonymi w opisie przedmiotu zamówienia, kryteriach oceny ofert lub warunkach realizacji zamówienia oznacza, że zamawiający akceptuje również certyfikaty wydane przez inne równoważne jednostki oceniające zgodność. Zamawiający akceptuje także inne odpowiednie środki dowodowe, w szczególności dokumentację techniczną producenta, w przypadku, gdy dany Wykonawca nie ma ani dostępu do certyfikatów lub sprawozdań z badań, ani możliwości ich uzyskania w odpowiednim terminie, o ile ten brak dostępu nie może być przypisany danemu Wykonawcy, oraz pod warunkiem że dany Wykonawca udowodni, że wykonywane przez niego dostawa spełniają wymogi lub kryteria określone w opisie przedmiotu zamówienia, kryteriach oceny ofert lub wymagania związane z realizacją zamówienia. Jeżeli w opisie przedmiotu zamówienia ujęto zapis wynikający z KNR lub KNNR wskazujący na konieczność wykorzystywania przy realizacji zamówienia konkretnego sprzętu o konkretnych parametrach Zamawiający dopuszcza używanie innego sprzętu o ile zapewni to osiągnięcie zakładanych parametrów projektowych i nie spowoduje ryzyka niezgodności wykonanych prac z dokumentacją techniczną.
Wykonawca, który powołuje się na rozwiązania równoważne, jest zobowiązany wykazać, że oferowane przez niego rozwiązanie spełnia wymagania określone przez zamawiającego. W takim przypadku, wykonawca załącza do oferty wykaz rozwiązań równoważnych wraz z jego opisem lub normami.

2.1. NAZWY I KODY WSPÓLNEGO SŁOWNIKA ZAMÓWIEŃ (CPV):

48822000-6 Serwery komputerowe
32420000-3 Urządzenia sieciowe
35120000-1 Systemy i urządzenia nadzoru i bezpieczeństwa
48821000-9 Serwery sieciowe
31214100-0 Przełączniki
51610000-1 Usługi instalowania urządzeń komputerowych i przetwarzania informacji
48900000-7 Różne pakiety oprogramowania i systemy komputerowe
80533100-0 Usługi szkolenia komputerowego

2.2. PODWYKONAWCY

1. Zamawiający **dopuszcza powierzenie części zamówienia podwykonawcom**.
   Wykonawca:
   1) jest zobowiązany wskazać w formularzu ofertowym **(Załącznik nr 1 do SWZ)** części zamówienia, których wykonanie zamierza powierzyć podwykonawcom i podać firmy **(oznaczenie przedsiębiorstwa)** podwykonawców;

2) jeżeli późniejsza zmiana albo rezygnacja z podwykonawcy dotyczy podmiotu, na którego zasoby Wykonawca powoływał się, na zasadach określonych w art. 118 Pzp w celu wskazania spełnienia warunków udziału w postępowaniu Wykonawca jest zobowiązany wskazać Zamawiającemu, iż proponowany inny Podwykonawca lub Wykonawca samodzielnie spełniają je w stopniu nie mniejszym niż Podwykonawca, na którego zasoby wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia. Kary umowne za nieprawidłowe zgłaszanie Podwykonawców oraz realizowanie na ich rzecz płatności określone są w projekcie umowy.

2. Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia w zakresie przedmiotu zamówienia.

ROZDZIAŁ III
TERMIN WYKONANIA ZAMÓWIENIA

Termin realizacji zamówienia: **sześć miesięcy od dnia zawarcia umowy.**

ROZDZIAŁ IV
WARUNKI UDZIAŁU W POSTĘPOWANIU

4.1.O udzielenie zamówienia publicznego mogą ubiegać się Wykonawcy, o których mowa w art. 57 Pzp, którzy nie podlegają wykluczeniu, na podstawie art. 108 ust. 1 Pzp, art. 109 ust. 1 pkt. 4, 5, 7 Pzp oraz spełniają warunki udziału w postępowaniu dotyczące:

1) **zdolności do występowania w obrocie gospodarczym:**
   Zamawiający nie stawia warunku w powyższym zakresie.
2) **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów** - Zamawiający odstępuje od określenia warunku,
3) **sytuacji ekonomicznej lub finansowej** - Zamawiający odstępuje od określenia warunku,
4) **zdolności technicznej** - Zamawiający odstępuje od określenia warunku,
5) **zdolności zawodowej:**
   dla Części I: Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał co najmniej 1 (jedną) dostawę sprzętu komputerowego, serwerów o łącznej wartości nie mniejszej niż 200 000,00 zł.
   dla Części II: Zamawiający uzna warunek za spełniony jeżeli Wykonawca wykaże, że w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował co najmniej 2 szkolenia z zakresu cyberbezpieczeństwa lub cyberzagrożeń.

2. Wykluczenie Wykonawcy, o którym mowa w ust. 1, następuje na podstawie przepisu art. 111 Pzp. Ofertę Wykonawcy wykluczonego uznaje się za odrzuconą.

3. Ocena spełniania wyżej opisanych warunków udziału w postępowaniu dokonywana będzie zgodnie z zasadą „spełnia – nie spełnia”, w oparciu o złożone przez Wykonawcę w niniejszym postępowaniu dokumenty oraz oświadczenia. Wskazane warunki udziału w postępowaniu są minimalnymi wymaganiami, jakie stawiane są Wykonawcy przez Zamawiającego.

4. Zamawiający może, na każdym etapie postępowania uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizacje zamówienia.

5. Zamawiający w stosunku do Wykonawców wspólnie ubiegających się o udzielenie zamówienia, w odniesieniu do warunku zdolności technicznej lub zawodowej – dopuszcza łączne spełnienie warunku przez Wykonawców.

4. Wykonawcy w celu potwierdzenia spełnienia warunków udziału mogą polegać na zdolnościach technicznych lub zawodowych podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go nimi stosunków prawnych.

5. W odniesieniu do warunków dotyczących doświadczenia, Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby, jeżeli podmioty te wykonują świadczenia do realizacji którego te zdolności są wymagane.
6. Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą zobowiązanie podmiotu udostępniającego mu do dyspozycji niezbędne zasoby na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów – wzór odwidzenie stanowi załącznik nr 5 lub załącznik nr 6 do niniejszej SWZ.
7. Zamawiający ocenia, czy udostępniane Wykonawcy przez podmioty udostępniające zasoby zdolności techniczne lub zawodowe, pozwalają na wykazanie przez Wykonawcę spełnienia warunków udziału w postępowaniu, a także bada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
8. Jeżeli zdolności techniczne lub zawodowe podmiotu udostępniającego zasoby nie potwierdzają spełnienia przez Wykonawcę warunków udziału w postępowaniu lub zachodzą wobec tego podmiotu podstawy wykluczenia, Zamawiający żąda, aby Wykonawca w terminie wskazanym przez Zamawiającego zastąpił ten podmiot innym podmiotem lub podmiotami albo wskazał, że samodzielnie spełnia warunek udziału w postępowaniu.
9. Wykonawca nie może po upływie terminu składania ofert, powoływać się mną zdolności lub sytuację podmiotów udostępniających zasoby, jeżeli na etapie składania ofert nie polegał on w danym zakresie na zdolnościach lub sytuacji podmiotów udostępniających zasoby.
10. Wykonawca w przypadku polegania na zdolnościach lub sytuacji podmiotów udostępniających zasoby przedstawia wraz z oświadczeniem, o którym mowa rozdziale V ust. 1 SWZ, także oświadczeniem podmiotu udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnienie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby, zgodnie z wykazem dokumentów określonym w Rozdziale V.
11. Zamawiający może na każdym etapie postępowania, uznać, że Wykonawca nie posiada wymaganych zdolności, jeżeli posiadanie przez Wykonawcę sprzecznych interesów w szczególności zaangażowanie zasobów technicznych lub zawodowych Wykonawcy w inne przedsięwzięcia gospodarcze Wykonawcy może mieć negatywny wpływ na realizację zamówienia.
12. **Dodatkowe informacje dla Wykonawców wspólnie ubiegających się o dzielenie zamówienia np. konsorcjum, spółka cywilna.** W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia Wykonawcy tacy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i w zawarciu umowy w sprawie zamówienia publicznego. Pełnomocnictwo winno być załączone do oferty. W przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia, oświadczenia, o których mowa w Rozdziale V ust. 1 SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw do wykluczenia oraz spełnienie warunków udziału w postępowaniu. Wykonawcy wspólnie ubiegający się o zamówienia dołączają do oferty oświadczenie, z którego treści wynikać będzie, które roboty usługi wykonają poszczególni Wykonawcy. Oświadczenia i dokumenty potwierdzające brak podstaw do wykluczenia z postępowania składa każdy z Wykonawców wspólnie ubiegający się o zamówienie.

ROZDZIAŁ V.
WYKAZ OŚWIADCZEŃ I DOKUMENTÓW, POTWIERDZAJĄCYCH SPEŁNIANIE WARUNKÓW UDZIAŁU W POSTĘPOWANIU ORAZ BRAK PODSTAW WYKLUCZENIA (PODMIOTOWE ŚRODKI DOWODOWE)

1. Dokumenty, które należy załączyć do oferty:

Wraz z ofertą (formularzem ofertowym – zgodnie z załącznikiem nr 1 do SWZ) Wykonawca zobowiązany jest złożyć:

1) aktualne na dzień składania ofert, oświadczenie o spełnieniu warunków udziału w postępowaniu oraz braku podstaw do wykluczenia z postępowania – zgodnie z załącznikiem nr 2 do SWZ,

2) oraz podmiotowe środki dowodowe aktualne na dzień złożenia podmiotowych środków dowodowych:
    1. Odpis lub informacje z Krajowego Rejestru sądowego lub z Centralnej Ewidencji Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 p.z.p., sporządzonych nie wcześniej niż 3 miesiące przed złożeniem oferty jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
    2. Zobowiązanie podmiotu udostępniającego swoje zasoby na potrzeby Wykonawcy składającego ofertę – jeżeli dotyczy, zgodnie z załącznikiem nr 4 do SWZ,
    3. Wykaz dostaw zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał co najmniej 1 (jedną) dostawę sprzętu komputerowego o łącznej wartości nie mniejszej niż 200 000,00 zł.– załącznik nr 5 do SWZ.
    4. Wykaz usług zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował co najmniej 2 szkolenia z zakresu cyberbezpieczeństwa lub cyberzagrożeń – załącznik nr 6 do SWZ,
3) Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza terytorium Rzeczypospolitej Polskiej, zamiast dokumentu, o którym mowa w ust. 2 pkt 2 składa dokument lub dokumenty wystawione w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji ani nie ogłoszono upadłości. Dokument, o którym mowa powyżej powinien być wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert.
4) Jeżeli w kraju, w którym Wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w ust. 2 pkt 2, zastępuje się je w całości lub w części dokumentem zawierającym odpowiednio oświadczenie Wykonawcy, ze wskazaniem osoby albo osób uprawnianych do jego reprezentacji, złożone przed notariuszem lub przed organem sądowym, administracyjnym albo organem samorządu zawodowego lub gospodarczego właściwym ze względu na siedzibę lub miejsce zamieszkania Wykonawcy. Przepis ust. 3 stosuje się odpowiednio.
5) Zgodnie z art. 274 ust. 1 ustawy Pzp, Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta została najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni, aktualnych na dzień złożenia, oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 p.z.p., o braku przynależności do tej samej grupy kapitałowej, w rozumieniu ustawy z dnia 16 lutego 2007 roku o ochronie konkurencji i konsumentów z innym Wykonawcą, który złożył odrębną ofertę lub ofertę częściową albo oświadczenie o przynależności do grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty lub oferty częściowej niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej – załącznik nr 3 do SWZ.
6) Zamawiający nie wzywa do złożenia podmiotowych środków dowodowych jeżeli:
    1) może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 roku o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile Wykonawca wskazała w oświadczeniu, o którym mowa w art. 125 ust. 1 p.z.p. dane uniemożliwiające dostęp do tych środków;
    2) podmiotowym środkiem dowodowym jest oświadczenie, którego treść odpowiada zakresowo oświadczenia, o którym mowa w art. 125 ust. 1 p.z.p.
7) Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które Zamawiający posiada, jeżeli Wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
8) W zakresie nieuregulowanym p.z.p. lub niniejszą SWZ do oświadczeń i dokumentów składanych przez Wykonawcę w postępowaniu zastosowanie mają w szczególności przepisy rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 roku w sprawie podmiotowych środków dowodowych oraz innych dokumentów i oświadczeń, jakich może

żądać Zamawiający od Wykonawcy (Dz. U. poz. 2415) oraz rozporządzenie Prezesa Rady Ministrów z dnia 20 grudnia 2020 roku w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. poz. 2452).

ROZDZIAŁ VI.
INFORMACJE O SPOSOBIE POROZUMIEWANIA SIĘ ZAMAWIAJĄCEGO Z WYKONAWCAMI ORAZ PRZEKAZYWANIA OŚWIADCZEŃ I DOKUMENTÓW, A TAKŻE WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

1. W toku postępowania dopuszczalne jest kontaktowanie się Wykonawców z Zamawiającym na zasadach określonych w niniejszym Rozdziale.
2. Zamawiający urzęduje od poniedziałku do piątku w godzinach od 07:30 do 15:30, oprócz świąt i dni ustawowo wolnych od pracy.
3. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami odbywa się za pośrednictwem platformazakupowa.pl pod adresem https://platformazakupowa.pl/pn/dziwnow.
4. Osoby upoważnione do kontaktów z Wykonawcami:
   Osobą ze strony Zamawiającego upoważnioną do kontaktowania się z Wykonawcami w zakresie merytorycznym jest:
   stanowisko: Informatyk
   imię i nazwisko: Jarosław Pociask
   tel. 91 32 75 188
   w terminach: poniedziałek – piątek w godz. 8:00 – 15:00
   Osobą ze strony Zamawiającego upoważnioną do kontaktowania się w zakresie proceduralnym oraz do potwierdzenia wpływu oświadczeń, wniosków, zawiadomień oraz innych informacji przekazywanych za pomocą faksu lub drogą elektroniczną jest:
   stanowisko: Warunki zabudowy i zamówienia publiczne
   imię i nazwisko: Anna Korwin-Szymanowska
   tel. 91 32 75 169
   fax. 91 32 75 164
   w terminach: poniedziałek – piątek w godz. pomiędzy 8:00 – 15:00
5. W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między zamawiającym a wykonawcami w zakresie:
   a) przesyłania Zamawiającemu pytań do treści SWZ;
   b) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
   c) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
   d) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
   e) przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;
   f) przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;

g) przesyłania wniosków, informacji, oświadczeń Wykonawcy;
h) przesyłania odwołania/inne odbywa się za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego”.
Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego” po których pojawi się komunikat, że wiadomość została wysłana do zamawiającego.

6. Zamawiający będzie przekazywał wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji “Komunikaty”. Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego wykonawcy.
7. Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
8. Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:
   a) stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
   b) komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
   c) zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
   d) włączona obsługa JavaScript,
   e) zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
   f) szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3,
   g) oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.
9. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
   a) akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
   b) zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej pod linkiem.
10. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego”).
    Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu ponieważ nie został spełniony obowiązek narzucony w art. 221 Ustawy Prawo Zamówień Publicznych.
11. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
12. Formaty plików wykorzystywanych przez Wykonawców powinny być zgodne z “obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram

Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".

13. Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf
14. W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów:
    a) .zip
    b) .7Z
15. Wśród formatów powszechnych a NIE występujących w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.
16. Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.
17. Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.
18. Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
19. Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
20. Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
21. Zaleca się, aby komunikacja z wykonawcami odbywała się tylko za pośrednictwem platformazakupowa.pl przy użyciu formularza "Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
22. Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
23. Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
24. Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
25. Jeśli wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
26. Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
27. Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.

ROZDZIAŁ VII.
WYMAGANIA DOTYCZĄCE WADIUM

1. Zamawiający żąda od Wykonawców wniesienia wadium.
2. Kwota wadium wynosi: 3 000,00 PLN (słownie: trzy tysiące złotych 00/100)
3. Wadium wnosi się przed upływem terminu składania ofert.
4. Wadium może być wnoszone w jednej lub w kilku formach określonych w art. 97 ust. 7 Pzp.
5. W przypadku wniesienia wadium w pieniądzu, do oferty należy dołączyć kopię dokumentu przelewu potwierdzoną za zgodność z oryginałem przez Wykonawcę.
6. Wadium zostanie zwrócone w sytuacji i na zasadach określonych w art. 98 Pzp.
7. W ofercie należy wpisać nr konta, na które Zamawiający ma zwrócić wadium lub dołączyć do oferty upoważnienie do odbioru wadium przez wskazaną osobę.
8. Zamawiający zatrzyma wadium, gdy zajdą przesłanki, o których mowa w art. 98 ust. 6 Pzp.

9. Zamawiający będzie żądał ponownego wniesienia wadium przez Wykonawcę, któremu zwrócono wadium, jeżeli w wyniku rozstrzygnięcia odwołania jego oferta została wybrana jako najkorzystniejsza. Wykonawca będzie zobowiązany wnieść wadium w terminie określonym przez Zamawiającego jednak nie krótszym jak 7 dni.
10. Jeżeli wadium wnoszone jest w formie gwarancji lub poręczeń Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej. Gwarancja lub poręczenie musi obejmować cały okres związania z ofertą i spełniać co najmniej poniższe wymagania:
    a) musi obejmować odpowiedzialność za wszystkie przypadki powodujące utratę wadium przez Wykonawcę określone w Pzp,
    b) z jej treści powinno wynikać jednoznacznie zobowiązanie gwaranta do zapłaty całej kwoty wadium,
    c) powinno być nieodwołane i bezwarunkowe oraz płatne na pierwsze żądanie;
    d) termin obowiązania poręczenia lub gwarancji nie może być krótszy niż termin związania ofertą (z zastrzeżeniem, iż pierwszym dniem związania ofertą jest dzień składania ofert);
    e) w treści poręczenia lub gwarancji powinna znaleźć się nazwa oraz numer przedmiotowego postępowania;
    f) beneficjentem poręczenia lub gwarancji jest Gmina Dziwnów z siedzibą w Dziwnowie przy ul. Szosowej 5;
    g) w przypadku Wykonawców wspólnie ubiegających się o udzielenie zamówienia (art. 58 Pzp), Zamawiający wymaga, aby poręczenie i gwarancja obejmowały swą treścią wszystkich Wykonawców (tj. zobowiązanych z tytułu poręczenia lub gwarancji) lub aby z jej treści wynikało, że zabezpiecza ofertę Wykonawców wspólnie ubiegających się o udzielenie zamówienia (konsorcjum).
11. W przypadku wniesienia wadium w formie gwarancji lub poręczenia koniecznym, jest aby formy te obejmowały odpowiedzialność za wszystkie przypadki powodujące utratę wadium, muszą zawierać w swojej treści nieodwołalne i bezwarunkowe zobowiązanie wystawcy dokumentu do zapłaty na rzecz Zamawiającego kwoty wadium. Wadium wniesione w formie gwarancji (bankowej lub ubezpieczeniowej) musi mieć taką samą płynność jak wadium wniesione w pieniądzu – dochodzenie roszczenia z tytułu wadium wniesionego w tej formie nie może być utrudnione. Dlatego w treści gwarancji powinna znaleźć się klauzula stanowiąca, iż wszelkie spory odnośnie gwarancji będą rozstrzygane zgodnie z prawem polskim i poddane jurysdykcji sądów polskich chyba, że coś innego wnika z przepisów prawa.
12. Oferta Wykonawcy, który nie wniesie wadium, wniesie w sposób nieprawidłowy lub nie utrzyma wadium nieprzerwanie do upływu terminu związania ofertą lub złoży wniosek o zwrot wadium w przypadku, o którym mowa w art. 98 ust. 2 pkt 3 Pzp zostanie odrzucona.
13. Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy Zamawiającego:

    Bank Pekao S.A. I/O w Kamieniu Pomorskim
    nr konta 18 1240 3868 1111 0000 4093 6541.

    Na poleceniu przelewu należy zamieścić adnotację: **„Przetarg nr WZP.271.5.2024 na zwiększenie cyberbezpieczeństwa Gminy Dziwnów”.**
14. W przypadku wniesienia wadium w pieniądzu, do oferty należy dołączyć kopię dokumentu przelewu potwierdzoną za zgodność z oryginałem przez Wykonawcę.

ROZDZIAŁ VIII.
TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca pozostaje związany ofertą przez okres **30** dni (tj do dnia 06.07.2024 r.).
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem ostatecznego terminu składania ofert.
3. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu składania ofert termin związania ofertą wskazany w ust. 1 niniejszego rozdziału Zamawiający przed upływem terminu związania ofertę zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie terminu o wskazany przez niego okres, nie dłuższy niż 30 dni. Przedłużenie

terminu związania ofertą wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą. Odmowa wyrażenia zgody na przedłużenie terminu związania ofertą nie powoduje utraty wadium.

4. W przypadku gdy Zamawiający żąda wniesienia wadium, przedłużenie terminu związania ofertą, o którym mowa w ust. 3, następuje wraz z przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.

ROZDZIAŁ IX.
OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Na ofertę składają się: oferta cenowa oraz wszystkie pozostałe wymagane dokumenty (w tym oświadczenia, załączniki itp.) zgodnie z rozdziałem V SWZ.
2. Wykonawca sporządza jedną ofertę zgodnie z wymaganiami SWZ.
3. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem.
4. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny Wykonawca składa bezpośrednio na dokumencie, który następnie przesyła do systemu.
5. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem.
6. Oferta powinna być:
   a) sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
   b) złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
   c) podpisana kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną/upoważnione
7. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać “Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.
8. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny. Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.
9. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Jeżeli wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
10. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu składania ofert wycofać ofertę lub wniosek za pośrednictwem Formularza składania oferty lub wniosku. Z uwagi na to, że oferta lub wniosek wykonawcy są zaszyfrowane nie można ich edytować. Przez zmianę oferty lub wniosku rozumie się złożenie nowej oferty i wycofanie poprzedniej, jednak należy to zrobić przed upływem terminu zakończenia składania ofert w postępowaniu.
11. Sposób dokonywania wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
12. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe podlegać będą odrzuceniu.

13. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
14. Dokumenty i oświadczenia składane przez wykonawcę powinny być w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
15. Zgodnie z definicją dokumentu elektronicznego z art.3 ustęp 2 Ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca, albo przez podwykonawcę.
16. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
17. **Na ofertę składają się następujące dokumenty:**
    a) Formularz ofertowy przygotowany wg wzoru stanowiącego załącznik nr 1 do SWZ podpisany kwalifikowanym podpisem elektronicznym lub opatrzony podpisem zaufanym czy podpisem osobistym,
    b) Oświadczenie o braku podstaw do wykluczenia oraz spełnianiu warunków udziału w postępowaniu, wg wzoru stanowiącego załącznik nr 2 do SWZ podpisany kwalifikowanym podpisem elektronicznym lub opatrzony podpisem zaufanym czy podpisem osobistym,
    c) Zobowiązanie podmiotu udostępniającego swoje zasoby na potrzeby Wykonawcy składającego ofertę – jeżeli dotyczy, zgodnie z załącznikiem nr 4 do SWZ,
    d) Odpis lub informacje z Krajowego Rejestru sądowego lub z Centralnej Ewidencji Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 p.z.p., sporządzonych nie wcześniej niż 3 miesiące przed złożeniem oferty jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji;
    e) Wykaz dostaw zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie wykonał co najmniej 1 (jedną) dostawę sprzętu komputerowego o łącznej wartości nie mniejszej niż 200 000,00 zł.– załącznik nr 5 do SWZ,
    f) Wykaz usług zrealizowanych w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie zrealizował co najmniej 2 szkolenia z zakresu cyberbezpieczeństwa lub cyberzagrożeń – załącznik nr 6 do SWZ,
    g) W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia – pełnomocnictwo do reprezentowania wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, ewentualnie umowę o współdziałaniu, z której będzie wynikać przedmiotowe pełnomocnictwo. Pełnomocnik może być ustanowiony do reprezentowania Wykonawców w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

ROZDZIAŁ X.
TERMIN SKŁADANIA I OTWARCIA OFERT

Miejsce i termin składania ofert

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na platformazakupowa.pl pod adresem: https://platformazakupowa.pl/pn/dziwnow w myśl Ustawy Pzp na stronie internetowej prowadzonego postępowania do dnia **07 czerwca 2024 roku do godziny 10:00.**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
3. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania".
4. Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty

za pośrednictwem platformazakupowa.pl, wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust 1 oraz ust.2 Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust.1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.

5. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

Otwarcie ofert

1. Otwarcie ofert następuje niezwłocznie po upływie terminu składania ofert.
2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
   1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   2) cenach lub kosztach zawartych w ofertach.

   Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji „Komunikaty” .
6. W przypadku ofert, które podlegają negocjacjom, zamawiający udostępnia informacje, o których mowa w ust. 5 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.

   Zgodnie z Ustawą Pzp Zamawiający nie ma obowiązku przeprowadzania jawnej sesji otwarcia ofert w sposób jawny z udziałem wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line a ma jedynie takie uprawnienie.

ROZDZIAŁ XI
OPIS SPOSOBU OBLICZENIA CENY

1. Cena za wykonanie zamówienia jest ceną ryczałtową.
2. Cena ofertowa winna być obliczona przy zachowaniu zasad staranności, wiedzy technicznej, w oparciu o niniejszą SWZ.
3. Cena powinna być podana za cały okres realizacji zamówienia.
4. Cena oferty uwzględnia wszystkie zobowiązania, musi być podana cyfrowo i słownie w polskich złotych, z wyodrębnieniem obowiązującego podatku VAT – jeżeli występuje.
5. Cena podana w ofercie powinna obejmować wszystkie koszty i składniki związane z wykonaniem przedmiotu zamówienia oraz warunkami stawianymi przez Zamawiającego.
6. Cena powinna być tylko jedna za wykonanie przedmiotu zamówienia, nie dopuszcza się wariantowości cen.

ROZDZIAŁ XII.
OPIS KRYTERIÓW, KTÓRYMI ZAMAWIAJĄCY BĘDZIE SIĘ KIEROWAŁ PRZY WYBORZE OFERTY, WRAZ Z PODANIEM ZNACZENIA TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

Zamawiający uzna ofertę za spełniającą wymagania i przyjmie do oceny jeżeli:
1) oferta spełnia wymagania określone niniejszym SWZ,
2) oferta została złożona, w określonym przez Zamawiającego terminie,
3) wniesiono poprawnie wadium.

2. Kryteria oceny ofert - stosowanie matematycznych obliczeń przy ocenie ofert, stanowi podstawową zasadę oceny ofert, które oceniane będą w odniesieniu do najkorzystniejszych warunków przedstawionych przez Wykonawców w zakresie każdego kryterium.

3. Za parametry najkorzystniejsze w danym kryterium, oferta otrzyma maksymalną ilość punktów ustaloną w poniższym opisie, pozostałe będą oceniane odpowiednio - proporcjonalnie do parametru najkorzystniejszego, wybór oferty dokonany zostanie na podstawie opisanych kryteriów i ustaloną punktację: punktacja 0-100 (100%=100pkt). Za najkorzystniejszą zostanie uznana oferta, która uzyska najwyższą liczbę punktów obliczonych w oparciu o ustalone kryteria przedstawione w tabeli:

Nazwa kryterium	**Waga**
CENA	100%

Przez **CENĘ** rozumie się zaoferowaną przez Wykonawcę cenę brutto, podaną w formularzu ofertowym.

W kryterium „CENA” ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$\frac{\textbf{najniższa cena ofertowa brutto}}{\textbf{cena brutto oferty ocenianej}} \textbf{ x 100 pkt x 100\% = liczba punktów}$$

4. Zgodnie z art. 248 p.z.p. jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny lub kosztu i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybiera ofertę z najniższą ceną lub najniższym kosztem, a jeżeli zostały złożone oferty o takiej samej cenie lub koszcie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych, które zawierają nową cena lub koszt.
5. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen lub kosztów wyższych niż zaoferowane w złożonych ofertach – art. 251 p.z.p.
6. Zamawiający odrzuci ofertę, jeżeli zaistnieją przesłanki określone w art. 226 ust. 1 p.z.p.
7. Zamawiający zawiadomi o wyniku postępowania wszystkich Wykonawców, którzy złożyli oferty. Powiadomienie odpowiadać będzie wymogom określonym w art. 253 Pzp.

ROZDZIAŁ XIII.
INFORMACJE O FORMALNOŚCIACH, JAKIE POWINNY ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą.

2. Jeżeli termin związania ofertą upłynął przed wyborem najkorzystniejszej oferty, Zamawiający wzywa Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.

3. Stosownie do art. 253 ust. 1 Pzp, Zamawiający informuje niezwłocznie wszystkich Wykonawców o:

1) wyborze najkorzystniejszej oferty, podając nazwę albo imię i nazwisko, siedzibę albo miejsce zamieszkania, jeżeli jest miejscem wykonywania działalności Wykonawcy, którego ofertę wybrano, oraz nazwy albo imiona i nazwiska, siedziby albo miejsca zamieszkania, jeżeli są miejscami wykonywania działalności Wykonawców, którzy złożyli oferty, a także punktację przyznaną ofertom w każdym kryterium oceny ofert i łączną punktację,

2) Wykonawcach, których oferty zostały odrzucone, podając uzasadnienie faktyczne i prawne.

4. Informacje o których mowa w pkt 3 Zamawiający opublikuje na swojej stronie internetowej: https://platformazakupowa.pl/pn/dziwnow.

5. W przypadku, gdy zostanie wybrana jako najkorzystniejsza oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Wykonawca przed podpisaniem umowy na wezwanie Zamawiającego przedłoży umowę regulującą współpracę Wykonawców, w której m.in. zostanie określony pełnomocnik uprawniony do kontaktów z Zamawiającym oraz do wystawiania dokumentów związanych z płatnościami.

6. Osoby reprezentujące Wykonawcę przy podpisywaniu umowy powinny posiadać dokumenty potwierdzające ich umocowanie do reprezentowania Wykonawcy, o ile umocowanie to nie będzie wynikać z dokumentów załączonych do oferty.

7. O terminie złożenia dokumentu, o którym mowa w pkt 5. Zamawiający powiadomi Wykonawcę odrębnym pismem.

ROZDZIAŁ XIV
WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie przewiduje wniesienia zabezpieczenia należytego wykonania umowy.

ROZDZIAŁ XV
ISTOTNE DLA STRON POSTANOWIENIA, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI ZAWIERANEJ UMOWY – OGÓLNE WARUNKI UMOWY

1. Istotne postanowienia, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego zostały przedstawione w załączniku nr 7 do SWZ - Projekt umowy.
2. Zamawiający przewiduje możliwość zmiany postanowień treści zawartej umowy w sprawie zamówienia publicznego. Szczegółowy opis warunków dokonania takich zmian znajduje się w Projekcie Umowy stanowiącym załącznik nr 7 do SWZ.
3. O terminie i miejscu zawarcia umowy Zamawiający zawiadomi wybranego Wykonawcę odrębnym pismem.

ROZDZIAŁ XVI
POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY W TOKU POSTĘPOWANIA O UDZIELENIE ZAMÓWIENIA

Wykonawcom, a także innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Pzp, przysługują środki ochrony prawnej na zasadach przewidzianych w dziale IX Pzp (art. 505–590).