Numer sprawy: ZP.272.4/2021

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

/SWZ/

w postępowaniu o udzielenie zamówienia publicznego prowadzonym w trybie podstawowym

na

„dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19"

Rodzaj zamówienia:

☒ dostawy

Wartość zamówienia jest mniejsza niż progi unijne określone na podstawie art. 3 ustawy z dnia 11 września 2019 r. – *Prawo zamówień publicznych* (t. j. z 2021 r., poz. 1129, ze zm.) – dalej jako „ustawa Pzp", „ustawa" lub „Prawo zamówień publicznych".

I INFORMACJE O ZAMAWIAJĄCYM

Nazwa zamawiającego:
Muzeum Niepodległości w Warszawie
Adres:
al. Solidarności 62, 00-240 Warszawa
Kod pocztowy, miejscowość, województwo:
00-240 Warszawa, woj. mazowieckie
Adres poczty elektronicznej:
it@muzeumniepodleglosci.art.pl
Adres strony internetowej prowadzonego postępowania:
https://muzeum-niepodleglosci.pl
https://miniportal.uzp.gov.pl
adres skrzynki ePuap: https://epuap.gov.pl/wps/portal

Na wyżej wskazanej stronie internetowej będą udostępniane zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia.

II TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie jest prowadzone w trybie podstawowym bez negocjacji, o którym mowa w art. 275 pkt 1 ustawy Pzp. W odpowiedzi na ogłoszenie o zamówieniu oferty mogą składać wszyscy zainteresowani wykonawcy, a następnie zamawiający wybiera najkorzystniejszą ofertę bez przeprowadzenia negocjacji.

2. Zgodnie z art. 310 pkt 1) ustawy PZP Zamawiający zastrzega sobie prawo do unieważnienia przedmiotowego postępowania, jeżeli środki publiczne, które zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostaną mu przyznane, a możliwość unieważnienia postępowania na tej podstawie została przewidziana w ogłoszeniu o zamówieniu.

3. Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 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", informuję, że:

a. administratorem danych osobowych wskazanych w złożonych ofertach jest Muzeum Niepodległości w Warszawie, al. Solidarności 62, 00-240 Warszawa;
b. administrator wyznaczył inspektora ochrony danych. Z inspektorem ochrony danych osobowych można się skontaktować poprzez e-mail: iod@muzeumniepodleglosci.art.pl
c. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przedmiotowym postępowaniem o udzielenie zamówienia publicznego;
d. odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o przepisy ustawy;
e. Pani/Pana dane osobowe będą przechowywane, zgodnie z przepisami ustawy, 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;
f. obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy, związanym z udziałem

w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy;

g. w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;

h. posiada Pani/Pan:
   – na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   – na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych (przy czym skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą oraz nie może naruszać 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 (przy czym prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego);
   – prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

i. nie przysługuje Pani/Panu:
   – 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 Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c RODO.

4. Wykonawca ubiegając się o udzielenie zamówienia publicznego jest zobowiązany do wypełnienia wszystkich obowiązków formalno-prawnych związanych z udziałem w postępowaniu. Do obowiązków tych należą m.in. obowiązki wynikające z RODO, w szczególności obowiązek informacyjny przewidziany w art. 13 RODO względem osób fizycznych, których dane osobowe dotyczą i od których dane te wykonawca bezpośrednio pozyskał. Jednakże obowiązek informacyjny wynikający z art. 13 RODO nie będzie miał zastosowania, gdy i w zakresie, w jakim osoba fizyczna, której dane dotyczą, dysponuje już tymi informacjami (vide: art. 13 ust. 4). Ponadto wykonawca będzie musiał wypełnić obowiązek informacyjny wynikający z art. 14 RODO względem osób fizycznych, których dane przekazuje zamawiającemu i których dane pośrednio pozyskał, chyba że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO.

5. W celu zapewnienia, że wykonawca wypełnił ww. obowiązki informacyjne oraz ochrony prawnie uzasadnionych interesów osoby trzeciej, której dane zostały przekazane w związku z udziałem wykonawcy w postępowaniu, Zamawiający wymaga złożenia w treści formularza oferty oświadczenia o wypełnieniu przez niego obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO.

6. Do spraw nieuregulowanych w SWZ mają zastosowanie przepisy ustawy z 11 września 2019 r. – Prawo zamówień publicznych (Dz.U. z 2021 r. poz. 1129) oraz przepisy RODO.

III OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiot zamówienia stanowi dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19. Szczegółowy opis przedmiotu zamówienia określony został w załączniku nr 1 do SWZ – opis przedmiotu zamówienia.
2. Kod CPV: 30200000-1 - Urządzenia komputerowe.
3. Podwykonawstwo.
Zamawiający nie zastrzega obowiązku osobistego wykonania przez wykonawcę kluczowych zadań składających się na przedmiot zamówienia. Wykonawca jest zobowiązany wskazać w formularzu ofertowym – załącznik nr 2 do SWZ, części zamówienia których wykonanie zamierza powierzyć podwykonawcom i podać firmy podwykonawców, o ile są już znane.
4. Wizja lokalna
Zamawiający nie przewiduje obowiązku odbycia przez wykonawcę wizji lokalnej miejsca dostawy i instalacji przedmiotu zamówienia.
5. W formularzu cenowym wypełnionym zgodnie ze wzorem stanowiącym załącznik nr 7 do SWZ wykonawcy zobowiązani są podać w szczególności nazwę modelu oraz producenta oferowanego urządzenia. W przypadku braku podania ww. informacji oferta zostanie odrzucona.

IV OPIS CZĘŚCI ZAMÓWIENIA

Przedmiot zamówienia podzielony jest na trzy części:
Część 1 - dostawa systemu ochrony styku z Internetem, przełącznika oraz UPS.
- 32420000-3: urządzenia sieciowe (do firewall),
- 35100000-5: UPS.
Część 2 - dostawa serwera wraz z oprogramowaniem.
- 48820000-2 serwer.
Część 3 - dostawa komputerów przenośnych oraz serwera NAS.
- 30213100-6 komputery przenośne,
- 30233000-1 urządzenia do przechowywania i odczytu danych.
Wykonawca może złożyć ofertę na jedno, kilka lub wszystkie części przedmiotu zamówienia.

V INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

1. Zamawiający żąda, aby wykonawca **złożył wraz z ofertą** następujące, przedmiotowe środki dowodowe potwierdzające, że oferowane dostawy spełniają określone w SWZ wymagania:
- opisy techniczne, katalogi lub foldery producenta urządzeń zaoferowanych w formularzu cenowym.
2. Zamawiający akceptuje równoważne przedmiotowe środki dowodowe, jeśli potwierdzają, że oferowane świadczenia spełniają określone przez zamawiającego wymagania, cechy lub kryteria.
3. Zamawiający przewiduje uzupełnianie przedmiotowych środków dowodowych. Jeżeli wykonawca nie złożył przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe są niekompletne, zamawiający wzywa do ich złożenia lub uzupełnienia w wyznaczonym terminie.
4. Zamawiający nie dopuszcza możliwości złożenia dokumentów określonych w pkt 1 w języku angielskim bez tłumaczenia ich na język polski. Wszelkie dokumenty sporządzone w języku obcym wykonawca składa wraz z tłumaczeniem na język polski.

VI TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest do realizacji przedmiotu zamówienia, określonego w rozdz. III SWZ w następujących terminach:

– **część 1** – maksymalnie 90 dni licząc od dnia podpisania umowy,

- **część 2** – maksymalnie 90 dni licząc od dnia podpisania umowy,

- **część 3** – maksymalnie 60 dni licząc od dnia podpisania umowy.

VII INFORMACJA O PRZEWIDYWANYCH ZAMÓWIENIACH, O KTÓRYCH MOWA W ART. 214 UST. 1 PKT 7 i 8 USTAWY PZP

Zamawiający **nie przewiduje** udzielania zamówień na podstawie art. 214 ust. 1 pkt 8 ustawy Pzp tj. zamówienia polegającego na powtórzeniu zamówienia na dodatkowe dostawy.

VIII INFORMACJE O OFERTACH WARIANTOWYCH

Zamawiający nie dopuszcza złożenia oferty wariantowej.

IX INFORMACJE O WARUNKACH UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się wykonawcy, którzy spełniają niżej określone warunku udziału w postępowaniu.

1) zdolność do występowania w obrocie gospodarczym:

Zamawiający nie stawia szczegółowego warunku w tym zakresie.

2) uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów:

Zamawiający nie stawia szczegółowego warunku w tym zakresie.

3) sytuacja ekonomiczna lub finansowa:

Zamawiający nie stawia szczegółowego warunku w tym zakresie.

4) zdolność techniczna lub zawodowa:

Zamawiający nie stawia szczegółowego warunku w tym zakresie.

3. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia zgodnie z art. 58 ustawy. W takim przypadku, wykonawcy ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.

4. Jeżeli oferta wykonawców, o której mowa w zdaniu poprzedzającym, została wybrana, zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego, kopii umowy regulującej współpracę tych wykonawców.

X PODSTAWY WYKLUCZENIA

Zamawiający **wykluczy** z postępowania wykonawców, wobec których zachodzą następujące podstawy wykluczenia:

1) wykonawcę będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

   a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,

b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,

c) o którym mowa w art. 228-230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,

d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,

e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,

f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769 oraz z 2020 r. poz. 2023),

g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,

h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

- lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;

3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

XI WYKAZ PODMIOTOWYCH ŚRODKÓW DOWODOWYCH

1. Wykonawca dołącza **do oferty oświadczenie o niepodleganiu wykluczeniu z postępowania** w zakresie wskazanym w rozdziale X SWZ – sporządzone zgodnie ze wzorem określonym w załączniku nr 3 do SWZ.

2. Oświadczenie, o którym mowa w ust. 1, składane jest pod rygorem nieważności **w formie elektronicznej (tj. postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym (przy użyciu dowodu osobistego z warstwą elektroniczną).**

3. Oświadczenie składa **odrębnie** każdy spośród Wykonawców wspólnie ubiegających się o udzielenie zamówienia.

4. Samooczyszczenie – w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2, 5 wykonawca nie podlega wykluczeniu jeżeli udowodni Zamawiającemu, że spełnił łącznie następujące przesłanki:

   1) naprawił lub zobowiązał się do naprawienia szkody wyrządzonej przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem, w tym poprzez zadośćuczynienie pieniężne;

   2) wyczerpująco wyjaśnił fakty i okoliczności związane z przestępstwem, wykroczeniem lub swoim nieprawidłowym postępowaniem oraz spowodowanymi przez nie szkodami, aktywnie współpracując odpowiednio z właściwymi organami, w tym organami ścigania lub zamawiającym;

   3) podjął konkretne środki techniczne, organizacyjne i kadrowe, odpowiednie dla zapobiegania dalszym przestępstwom, wykroczeniom lub nieprawidłowemu postępowaniu, w szczególności:

   a) zerwał wszelkie powiązania z osobami lub podmiotami odpowiedzialnymi za nieprawidłowe postępowanie wykonawcy,

   b) zreorganizował personel,

   c) wdrożył system sprawozdawczości i kontroli,

   d) utworzył struktury audytu wewnętrznego do monitorowania przestrzegania przepisów, wewnętrznych regulacji lub standardów,

   e) wprowadził wewnętrzne regulacje dotyczące odpowiedzialności i odszkodowań za nieprzestrzeganie przepisów, wewnętrznych regulacji lub standardów.

   Zamawiający ocenia, czy podjęte przez wykonawcę czynności są wystarczające do wykazania jego rzetelności, uwzględniając wagę i szczególne okoliczności czynu wykonawcy, a jeżeli uzna, że nie są wystarczające, wyklucza wykonawcę.

5. Oświadczenie o niepodleganiu wykluczeniu z postępowania, składa się pisemnie w formie elektronicznej, w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym, w zakresie i w sposób określony w przepisach wydanych na podstawie art. 70 ustawy tj. w Rozporządzeniu 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). Szczegółowe informacje zostały zawarte w rozdziale XII SWZ.

6. Oświadczenia i inne dokumenty, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
7. Jeżeli wykonawca nie złożył oświadczenia o niepodleganiu wykluczeniu z postępowania lub innych dokumentów składanych w postępowaniu lub są one niekompletne lub zawierają błędy, Zamawiający wzywa Wykonawcę odpowiednio do ich złożenia, poprawienia lub uzupełnienia w wyznaczonym terminie, chyba że:

   1) oferta Wykonawcy podlega odrzuceniu bez względu na ich złożenie, uzupełnienie lub poprawienie lub

   2) zachodzą przesłanki unieważnienia postępowania.
8. Niezależnie od powyższych wymagań, na Wykonawcach jako administratorach danych osobowych w rozumieniu RODO, ciąży obowiązek dołączenia oświadczenia potwierdzającego stosowanie przez nich przepisów RODO, według wzoru stanowiącego załącznik nr 4 i 5 do SWZ.

XII INFORMACJE O ŚRODKACH KOMUNIKACJI ELEKTRONICZNEJ, PRZY UŻYCIU KTÓRYCH ZAMAWIAJĄCY BĘDZIE KOMUNIKOWAŁ SIĘ Z WYKONAWCAMI ORAZ INFORMACJE O WYMAGANIACH TECHNICZNYCH I ORGANIZACYJNYCH SPORZĄDZANIA, WYSYŁANIA I ODBIERANIA KORESPONDENCJI ELEKTRONICZNEJ

1. Komunikacja w postępowaniu o udzielenie zamówienia, w tym składanie ofert, wymiana informacji oraz przekazywanie dokumentów lub oświadczeń odbywa się przy użyciu środków komunikacji elektronicznej.
2. Komunikacja ustna dopuszczalna jest wyłącznie w odniesieniu do informacji, które nie są istotne, w szczególności nie dotyczą ogłoszenia o zamówieniu lub dokumentów zamówienia, ofert, o ile jej treść jest udokumentowana.
3. W niniejszym postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym, a Wykonawcami odbywa się przy użyciu miniPortalu https://miniportal.uzp.gov.pl/, ePUAPu https://epuap.gov.pl/wps/portal.
4. Zamawiający nie przewiduje komunikowania się z Wykonawcami za pomocą poczty elektronicznej.
5. Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, musi posiadać konto na ePUAP. Wykonawca posiadający konto na ePUAP ma dostęp do formularzy: złożenia, zmiany, wycofania oferty lub wniosku oraz do formularza do komunikacji.
6. Wymagania techniczne i organizacyjne wysyłania i odbierania dokumentów elektronicznych, elektronicznych kopii dokumentów i oświadczeń oraz informacji przekazywanych przy ich użyciu opisane zostały w Regulaminie korzystania z miniPortalu oraz Regulaminie ePUAP.
7. Za datę przekazania oferty, wniosków, zawiadomień, dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń oraz innych informacji przyjmuje się datę ich przekazania na ePUAP.
8. Identyfikator postępowania dla danego postępowania o udzielenie zamówienia dostępne są na Liście wszystkich postępowań na miniPortalu.
9. Poza składaniem ofert, komunikacja Zamawiającego z Wykonawcami, w szczególności składanie oświadczeń, wniosków, zawiadomień oraz przekazywanie informacji odbywa się elektronicznie za pośrednictwem dedykowanego formularza dostępnego na ePUAP oraz udostępnionego przez miniPortal (Formularz do komunikacji). We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (lub ID postępowania).

10. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem Formularza do komunikacji jako załączniki.
11. Sposób i forma sporządzenia dokumentów muszą być zgodne z wymaganiami określonymi w Rozporządzeniu 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), przepisami wydanymi na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2020 r. poz. 346, 568, 695, 1517 i 2320), a także Rozporządzeniem Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń jakich może żądać zamawiający od wykonawcy (DZ. U. 2020 r. poz. 2415).

XIII WSKAZANIE OSÓB UPRAWNIONYCH DO POROZUMIEWANIA SIĘ Z WYKONAWCAMI

Osoby uprawnione do porozumiewania się z wykonawcami:

Bartosz Biedrzycki e-mail: it@muzeumniepodleglosci.art.pl

XIV WYMAGANIA DOTYCZĄCE WADIUM

Zamawiający wymaga wniesienia wadium.

1) Wykonawca przystępujący do postępowania jest zobowiązany, przed upływem terminu składania ofert, wnieść wadium w kwocie:

   Część 1 – 3.500 zł (trzy tysiące pięćset złotych),

   Część 2 – 1.500 zł (tysiąc pięćset złotych),

   Część 3 – 1.500 zł (tysiąc pięćset złotych).

2) Wadium musi obejmować pełen okres związania ofertą.

3) Wadium może być wniesione w jednej lub kilku formach wskazanych w art. 97 ust. 7 ustawy Pzp tj.:

   - pieniądzu,
   - gwarancjach bankowych,
   - gwarancjach ubezpieczeniowych,
   - poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2019 r. poz. 310, 836 i 1562 ze zm.).

4) Wadium wnoszone w pieniądzu należy wpłacić przelewem na rachunek bankowy w PKO BP S.A. numer rachunku 59 1020 1042 0000 8502 0441 6947. Wadium musi wpłynąć na wskazany rachunek bankowy zamawiającego najpóźniej przed upływem terminu składania ofert (decyduje data wpływu na rachunek bankowy zamawiającego).

5) Wadium wnoszone w poręczeniach lub gwarancjach należy załączyć do oferty w oryginale w postaci dokumentu elektronicznego podpisanego kwalifikowanym podpisem elektronicznym przez wystawcę dokumentu i powinno zawierać następujące elementy:

   - nazwę dającego zlecenie (wykonawcy), beneficjenta gwarancji (zamawiającego), gwaranta/poręczyciela oraz wskazanie ich siedzib. Beneficjentem wskazanym w gwarancji lub poręczeniu musi być Muzeum Niepodległości w Warszawie,
   - określenie wierzytelności, która ma być zabezpieczona gwarancją/poręczeniem,
   - kwotę gwarancji/poręczenia,

- termin ważności gwarancji/poręczenia,
- zobowiązanie gwaranta do zapłacenia kwoty gwarancji/poręczenia bezwarunkowo, na pierwsze pisemne żądanie zamawiającego, w sytuacjach określonych w art. 98 ust. 6 ustawy Pzp.

6) W przypadku, gdy wykonawca nie wniósł wadium lub wniósł w sposób nieprawidłowy lub nie utrzymywał wadium nieprzerwanie do upływu terminu związania ofertą lub złożył wniosek o zwrot wadium, w przypadku o którym mowa w art. 98 ust. 2 pkt 3 ustawy Pzp, zamawiający odrzuci ofertę na podstawie art. 226 ust. 1 pkt 14 ustawy Pzp.

7) Zamawiający dokona zwrotu wadium na zasadach określonych w art. 98 ust. 1–5 ustawy Pzp. Zamawiający zwraca wadium niezwłocznie, nie później jednak niż w terminie 7 dni od dnia wystąpienia jednej z okoliczności:

   - upływu terminu związania ofertą;

   - zawarcia umowy w sprawie zamówienia publicznego;

   - unieważnienia postępowania o udzielenie zamówienia, z wyjątkiem sytuacji gdy nie zostało rozstrzygnięte odwołanie na czynność unieważnienia albo nie upłynął termin do jego wniesienia.

   Zamawiający, niezwłocznie, nie później jednak niż w terminie 7 dni od dnia złożenia wniosku zwraca wadium wykonawcy:

   - który wycofał ofertę przed upływem terminu składania ofert;

   - którego oferta została odrzucona;

   - po wyborze najkorzystniejszej oferty, z wyjątkiem wykonawcy, którego oferta została wybrana jako najkorzystniejsza;

   - po unieważnieniu postępowania, w przypadku gdy nie zostało rozstrzygnięte odwołanie na czynność unieważnienia albo nie upłynął termin do jego wniesienia.

8) Zamawiający zatrzymuje wadium wraz z odsetkami na podstawie art. 98 ust. 6 ustawy Pzp.

XV TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca pozostaje związany ofertą **do dnia 12.02.2022 r.**
2. Bieg terminu związania ofertą rozpoczyna się wraz z upływem terminu składania ofert.
3. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w ust. 1, zamawiający przed upływem terminu związania ofertą, zwraca się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
4. Przedłużenie terminu związania ofertą, o którym mowa w ust. 3, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XVI OPIS SPOSOBU PRZYGOTOWYWANIA OFERT

1. Wykonawca składa ofertę za pośrednictwem miniPortalu - Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPortalu. W formularzu oferty Wykonawca zobowiązany jest podać adres skrzynki ePUAP, na którym prowadzona będzie korespondencja związana z postępowaniem.
2. Oferta wraz z załącznikami musi zostać sporządzona w języku polskim, złożona w postaci elektronicznej oraz **podpisana kwalifikowanym podpisem elektronicznym, podpisem osobistym lub podpisem zaufanym pod rygorem nieważności**. Złożenie oferty wymaga od wykonawcy zarejestrowania się i zalogowania na miniPortalu.

3. Oferty, oświadczenia, o których mowa w art. 125 ust. 1 ustawy, podmiotowe środki dowodowe, w tym oświadczenie, o którym mowa w art. 117 ust. 4 ustawy oraz zobowiązanie podmiotu udostępniającego zasoby, o którym mowa w art. 118 ust. 3 ustawy, przedmiotowe środki dowodowe, pełnomocnictwo, dokumenty, o których mowa w art. 94 ust. 2 ustawy, sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. z 2020 r. poz. 346, 568, 695, 1517 i 2320), z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy, z uwzględnieniem rodzaju przekazywanych danych.
4. Informacje, oświadczenia lub dokumenty, inne niż określone w ust. 3, przekazywane w postępowaniu sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. *o informatyzacji działalności podmiotów realizujących zadania publiczne lub jako tekst wpisany bezpośrednio do wiadomości przekazywanej przy użyciu środków komunikacji elektronicznej.*
5. W przypadku, gdy dokumenty elektroniczne w postępowaniu przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2020 r. poz. 1913), wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
6. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
7. Szczegółowe warunki w tym zakresie oraz sposób poświadczania dokumentów określają przepisy Rozporządzenia 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).
8. Treść oferty musi odpowiadać treści SWZ.
9. Wykonawca ponosi wszelkie koszty związane z przygotowaniem i złożeniem oferty.
10. Wykonawca może przed upływem terminu do składania ofert zmienić lub wycofać ofertę za pośrednictwem Formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionych również na miniPortalu. Sposób zmiany i wycofania oferty został opisany w Instrukcji użytkownika dostępnej na miniPortalu. Wykonawca po upływie terminu do składania ofert nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
11. Zamawiający nie dopuszcza dokonywania w treści załączonych wzorów dokumentów jakichkolwiek zmian ich treści (skrótów, opuszczeń, skreśleń, poprawek lub dopisków) za wyjątkiem miejsc oznaczonych, lub wskazanych w inny wyraźny sposób.
12. Wykonawca ma prawo złożyć tylko jedną ofertę. Oferty wykonawcy, który przedłoży więcej niż jedną ofertę, zostaną odrzucone.
13. Oferta musi być podpisana przez osoby umocowane do reprezentowania wykonawcy i zaciągania w jego imieniu zobowiązań finansowych w wysokości odpowiadającej cenie oferty. Oznacza to, że jeżeli z dokumentu określającego status prawny wykonawcy lub pełnomocnictwa wynika, iż do reprezentowania wykonawcy upoważnionych jest łącznie kilka osób dokumenty wchodzące w skład oferty muszą być podpisane przez wszystkie te osoby.
14. Oferta musi zawierać:
    a) **formularz Oferty** - sporządzony na podstawie wzoru stanowiącego **załącznik nr 2 do SWZ:**
        - Formularz musi być złożony w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do

reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

b) **Formularz Cenowy** - sporządzony na podstawie wzoru stanowiącego **załącznik nr 7 do SWZ:**
   - Formularz musi być złożony w formie elektronicznej (tj. postać elektroniczna opatrzona kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

c) **oświadczenie o niepodleganiu wykluczeniu, o którym mowa w rozdziale XI pkt 1 SWZ** w formie wskazanej w ust. 3,

d) **oświadczenia zgodnie ze wzorem stanowiącym załącznik nr 4 i 5 od SWZ – jeżeli dotyczy**.

e) **Zobowiązanie podmiotu trzeciego (jeżeli dotyczy):**
   - Zobowiązanie musi być złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania podmiotu trzeciego zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

f) **Potwierdzenie umocowania do działania w imieniu wykonawcy:**
   - W celu potwierdzenia, że osoba działająca w imieniu wykonawcy jest umocowana do jego reprezentowania, zamawiający żąda od wykonawcy odpisu lub informacji z Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub innego właściwego rejestru.
   - Wykonawca nie jest zobowiązany do złożenia dokumentów, o których mowa w tiret pierwszym, jeżeli zamawiający może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, o ile wykonawca wskaże dane umożliwiające dostęp do tych dokumentów (dotyczy wykonawców mających miejsce zamieszkania lub siedzibę poza granicami RP) .
   - Jeżeli w imieniu wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów, o których mowa w tiret pierwszym, zamawiający żąda od wykonawcy pełnomocnictwa lub innego dokumentu potwierdzającego umocowanie do reprezentowania wykonawcy.
   - Postanowienia tiretów 1-3 stosuje się odpowiednio do osoby działającej w imieniu podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy lub podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach.
   - Gdy umocowanie osoby składającej ofertę nie wynika z dokumentów rejestrowych, wykonawca, który składa ofertę za pośrednictwem pełnomocnika, powinien dołączyć do oferty dokument pełnomocnictwa obejmujący swym zakresem umocowanie do złożenia oferty lub do złożenia oferty i podpisania umowy.
   - Pełnomocnictwo powinno zostać złożone w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym.
   - Dopuszcza się również przedłożenie elektronicznej kopii dokumentu poświadczonej za zgodność z oryginałem przez notariusza, tj. podpisanej kwalifikowanym podpisem elektronicznym osoby posiadającej uprawnienia notariusza.
   - W przypadku wykonawców ubiegających się wspólnie o udzielenie zamówienia wykonawcy zobowiązani są do ustanowienia pełnomocnika. Dokument pełnomocnictwa, z treści którego będzie wynikało umocowanie do reprezentowania w postępowaniu o udzielenie zamówienia tych wykonawców należy załączyć do oferty.
   - Pełnomocnictwo powinno zawierać w szczególności wskazanie:

- postępowania o zamówienie publiczne, którego dotyczy,
- wszystkich wykonawców ubiegających się wspólnie o udzielenie zamówienia wymienionych z nazwy z określeniem adresu siedziby,
- ustanowionego pełnomocnika oraz zakresu jego umocowania.

g) Oświadczenie wykonawców wspólnie ubiegających się o udzielenie zamówienia (jeżeli dotyczy):

- Wykonawcy wspólnie ubiegający się o udzielenie zamówienia, spośród których tylko jeden spełnia warunek dotyczący uprawnień, są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
- Wykonawcy wspólnie ubiegający się o udzielenie zamówienia mogą polegać na zdolnościach tych z wykonawców, którzy wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane. W takiej sytuacji wykonawcy są zobowiązani dołączyć do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy.
- Wykonawcy składają oświadczenia określone w niniejszej lit. e) w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

h) Zastrzeżenie tajemnicy przedsiębiorstwa (jeżeli dotyczy):

- W sytuacji, gdy oferta lub inne dokumenty składane w toku postępowania będą zawierały tajemnicę przedsiębiorstwa, wykonawca, wraz z przekazaniem takich informacji, zastrzega, że nie mogą być one udostępniane, oraz wykazuje, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji.*
- Dokument musi być złożony w formie elektronicznej lub w postaci elektronicznej opatrzonej podpisem zaufanym, lub podpisem osobistym osoby upoważnionej do reprezentowania wykonawców zgodnie z formą reprezentacji określoną w dokumencie rejestrowym właściwym dla formy organizacyjnej lub innym dokumencie.

XVII TERMIN SKŁADANIA I OTWARCIA OFERT

1. Ofertę należy złożyć w terminie do dnia **14 stycznia 2022 r. do godz. 10.00.**
2. Otwarcie ofert nastąpi w dniu **14 stycznia 2022 r. o godz. 10.30** poprzez odszyfrowanie wczytanych na Platformie ofert.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. 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 bądź miejscach zamieszkania wykonawców, których oferty zostały otwarte;
2) cenach lub kosztach zawartych w ofertach.

XVIII OPIS SPOSOBU OBLICZENIA CENY

1. Cenę oferty stanowi wartość wyrażona w jednostkach pieniężnych, którą zamawiający jest obowiązany zapłacić wykonawcy za przedmiot zamówienia.

2. W cenie oferty uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów przedmiot zamówienia podlega obciążeniu podatkiem od towarów i usług oraz podatkiem akcyzowym.

3. Cena oferty stanowić będzie:

   - cenę całkowitą podaną w ofercie, wyliczoną zgodnie z formularzem cenowym.

4. Cena oferty należy rozumieć jako wynagrodzenie:

   - umowne.

5. Zgodnie z art. 225 ustawy Pzp jeżeli została złożona oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z 11 marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny lub kosztu zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć. W takiej sytuacji wykonawca ma obowiązek:

   1) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
   2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
   3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
   4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

6. Informację w zakresie, o którym mowa w ust. 5 wykonawca składa w załączniku nr 2 do SWZ – formularz ofertowy. Brak złożenia ww. informacji będzie postrzegany jako brak powstania obowiązku podatkowego u zamawiającego.

XIX INFORMACJE DOTYCZĄCE WALUT OBCYCH, W JAKICH MOGĄ BYĆ PROWADZONE ROZLICZENIA MIĘDZY ZAMAWIAJĄCYM A WYKONAWCĄ

Cenę oferty należy wyrazić w złotych polskich.

XX OPIS KRYTERIÓW OCENY OFERT WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. W odniesieniu do wykonawców, którzy spełnili postawione warunki Zamawiający dokona oceny ofert na podstawie następujących kryteriów:

l.p.	Opis kryteriów oceny	Znaczenie
1.	Cena	60 %
2.	Termin dostawy	40 %

2. Zamawiający porówna i oceni oferty w następujący sposób:

a) W zakresie kryterium cena ocena kryterium nastąpi w skali punktowej od 0 do 60 pkt, według wzoru:

najniższa cena brutto spośród złożonych ofert/wartość brutto w ofercie badanej x 60 pkt.

b) W zakresie kryterium „Termin dostawy" punkty zostaną przyznane według następującego schematu:

dot. części 1-2:

- zaoferowanie terminu dostawy 90 dni licząc od dnia podpisania umowy – 0 pkt,
- zaoferowanie terminu dostawy 80 dni licząc od dnia podpisania umowy – 20 pkt,
- zaoferowanie terminu dostawy 70 dni licząc od dnia podpisania umowy – 40 pkt.

Maksymalna liczba punktów do uzyskania w przedmiotowym kryterium to 40 pkt. W przypadku braku określenia w złożonej ofercie terminu dostawy Zamawiający przyjmie, iż wykonawca oferuje najdłuższy dopuszczalny termin dostawy tj. 90 dni. W przypadku zaoferowania dłuższego terminu dostawy niż maksymalny dopuszczalny oferta zostanie odrzucona.

dot. części 3:

- zaoferowanie terminu dostawy 60 dni licząc od dnia podpisania umowy – 0 pkt,
- zaoferowanie terminu dostawy 50 dni licząc od dnia podpisania umowy – 20 pkt,
- zaoferowanie terminu dostawy 40 dni licząc od dnia podpisania umowy – 40 pkt.

Maksymalna liczba punktów do uzyskania w przedmiotowym kryterium to 40 pkt. W przypadku braku określenia w złożonej ofercie terminu dostawy Zamawiający przyjmie, iż wykonawca oferuje najdłuższy dopuszczalny termin dostawy tj. 60 dni. W przypadku zaoferowania dłuższego terminu dostawy niż maksymalny dopuszczalny oferta zostanie odrzucona.

3. Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyska najwyższą sumę punktów z wszystkich kryteriów.
4. W sytuacji, gdy zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o tej samej łącznej punktacji, wezwie on wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.
5. W toku badania i oceny ofert zamawiający może żądać od wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są obowiązani do przedstawienia wyjaśnień w terminie wskazanym przez zamawiającego.
6. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
7. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, zamawiający wezwie wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez zamawiającego terminie, pisemnej zgody na wybór jego oferty.
8. W przypadku braku zgody, o której mowa w pkt. 7 powyżej oferta podlega odrzuceniu, a zamawiający zwraca się o wyrażenie takiej zgody do kolejnego wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.

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

1. Zamawiający poinformuje wykonawcę, któremu zostanie udzielone zamówienie, o miejscu i terminie zawarcia umowy.
2. Wykonawca przed zawarciem umowy:

- poda wszelkie informacje niezbędne do wypełnienia treści umowy na wezwanie zamawiającego,
- wniesie zabezpieczenie należytego wykonania umowy.

3. Jeżeli zostanie wybrana oferta wykonawców wspólnie ubiegających się o udzielenie zamówienia, zamawiający będzie żądał przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców, w której m.in. zostanie określony pełnomocnik uprawniony do kontaktów z zamawiającym oraz do wystawiania dokumentów związanych z płatnościami, przy czym termin, na jaki została zawarta umowa, nie może być krótszy niż termin realizacji zamówienia.
4. Niedopełnienie powyższych formalności przez wybranego wykonawcę będzie potraktowane przez zamawiającego jako niemożność zawarcia umowy w sprawie zamówienia publicznego z przyczyn leżących po stronie wykonawcy i zgodnie z art. 98 ust. 6 pkt 3 ustawy Pzp, będzie skutkowało zatrzymaniem przez zamawiającego wadium wraz z odsetkami.
5. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577, w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
6. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 5, jeżeli w postępowaniu złożono tylko jedną ofertę.

XXII INFORMACJA O PROJEKTOWANYCH POSTANOWIENIACH UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI UMOWY

1. Projektowane postanowienia umowy, które zostaną wprowadzone do treści umowy określa załącznik nr 6 do SWZ stanowiący wzór umowy.
2. Zamawiający przewiduje dokonanie zmian postanowień treści zawartej umowy w przypadku zaistnienia okoliczności określonych w § 8 wzoru umowy.
3. Zamawiający nie przewiduje udzielenia zaliczek na poczet wykonania zamówienia.

XXIII WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający nie wymaga wniesienia zabezpieczenia należytego wykonania umowy.

XXIV WYJAŚNIENIA I ZMIANY W TREŚCI SWZ

1. Wykonawca może zwrócić się do zamawiającego o wyjaśnienie treści specyfikacji warunków zamówienia.
2. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem że wniosek o wyjaśnienie treści SWZ wpłynął do zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
3. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 2, zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
4. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
5. Treść zapytań wraz z wyjaśnieniami zamawiający udostępnia, bez ujawniania źródła zapytania, na stronie internetowej prowadzonego postępowania.
6. W uzasadnionych przypadkach zamawiający może przed upływem terminu składania ofert zmienić treść SWZ.

XXV POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

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 ustawy, przysługują środki ochrony prawnej na zasadach przewidzianych w dziale IX ustawy Pzp (art. 505–590).

XXVI POZOSTAŁE INFORMACJE

1. Zamawiający nie przewiduje aukcji elektronicznej.
2. Zamawiający nie wymaga złożenia ofert w postaci katalogów elektronicznych.
3. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

Załączniki do niniejszej SWZ:

1. opis przedmiotu zamówienia,
2. wzór formularza ofertowego,
3. wzór oświadczenia o niepodleganiu wykluczeniu z postępowania,
4. wzór oświadczenia wykonawcy jako administratora danych osobowych potwierdzający stosowanie przez wykonawcę przepisów RODO,
5. wzór oświadczenia wykonawcy działającego w imieniu zamawiającego, potwierdzający stosowanie przepisów RODO,
6. projektowane postanowienia umowy,
7. wzór formularza cenowego.

DYREKTOR

Warszawa 29 grudnia 2021 r. ……Tadeusz Skoczek……

(podpis Zamawiającego)

Załącznik nr 1 do SWZ

Opis przedmiotu zamówienia

Przedmiot zamówienia stanowi dostawa *i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19.* Przedmiot zamówienia podzielony został na trzy części.

Część 1.

Dostawa systemu ochrony styku z Internetem, przełącznika oraz UPS. Zamawiający w ramach przedmiotu zamówienia wymaga wykonania instalacji, konfiguracji i uruchomienia dostarczonego sprzętu/oprogramowania wraz z przeprowadzeniem szkolenia technicznego.
Zakres montażu i wyposażenia obejmuje:
Firewall sprzętowy 4 szt.,
Przełącznik sieciowy 2 szt.,
UPS 2 szt.

Wielofunkcyjna zapora sieciowa - UTM UTM – 2 szt.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od wykonawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej wykonawca a musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym. System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym lub monitorowania na porcie SPAN. W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.
2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 10 portami Gigabit Ethernet RJ-45.
   - 2 gniazdami SFP 1 Gbps.

2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.4 mln. jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1.7 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 6 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1.4 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 700 Mbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

13. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
14. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.

15. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
16. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
17. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
    - Producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

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

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze. W ramach postępowania musi zostać dostarczona platforma typu Sandbox wraz z niezbędnymi serwisami lub licencja upoważniająca do korzystania z usługi typu Sandbox w chmurze.
5. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
6. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

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

Kontrola aplikacji

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

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.

2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

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

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać

dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.

2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Serwisy i licencje

W ramach przedmiotu zamówienia powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres [36] miesięcy.

Gwarancja oraz wsparcie

Gwarancja: System musi być objęty serwisem gwarancyjnym wykonawcy przez okres [24] miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym dostarczenie sprzętu zastępczego na czas naprawy sprzętu w następnym dniu roboczym od momentu potwierdzenia zasadności zgłoszenia, przez okres 24 miesięcy.

Wielofunkcyjna zapora sieciowa - UTM – 2 szt.

Wymagania Ogólne

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej wykonawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym.
System realizujący funkcję Firewall musi dawać możliwość pracy w jednym z trzech trybów: Routera z funkcją NAT, transparentnym oraz monitorowania na porcie SPAN.
W ramach dostarczonego systemu bezpieczeństwa musi być zapewniona możliwość budowy minimum 2 oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: Routingu, Firewall'a, IPSec VPN, Antywirus, IPS, Kontroli Aplikacji. Powinna istnieć możliwość dedykowania co najmniej 4 administratorów do poszczególnych instancji systemu.
System musi wspierać IPv4 oraz IPv6 w zakresie:

- Firewall.
- Ochrony w warstwie aplikacji.
- Protokołów routingu dynamicznego.

Redundancja, monitoring i wykrywanie awarii

1. W przypadku systemu pełniącego funkcje: Firewall, IPSec, Kontrola Aplikacji oraz IPS – musi istnieć możliwość łączenia w klaster Active-Active lub Active-Passive. W obu trybach powinna istnieć funkcja synchronizacji sesji firewall.

2. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych.
3. Monitoring stanu realizowanych połączeń VPN.
4. System musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP. Powinna istnieć możliwość tworzenia interfejsów redundantnych.

Interfejsy, Dysk, Zasilanie:

1. System realizujący funkcję Firewall musi dysponować minimum:
   - 16 portami Gigabit Ethernet RJ-45.
   - 8 gniazdami SFP 1 Gbps.
   - 2 gniazdami SFP+ 10 Gbps.
2. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB.
3. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4. System musi być wyposażony w zasilanie AC.

Parametry wydajnościowe:

1. W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 52 tys. nowych połączeń na sekundę.
2. Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.1 Gbps.
4. Wydajność szyfrowania IPSec VPN nie mniej niż 10 Gbps.
5. Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.5 Gbps.
6. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 1 Gbps.
7. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

Funkcje Systemu Bezpieczeństwa:

W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub programowych:

1. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection.
2. Kontrola Aplikacji.
3. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN.
4. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS.
5. Ochrona przed atakami - Intrusion Prevention System.
6. Kontrola stron WWW.
7. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3.
8. Zarządzanie pasmem (QoS, Traffic shaping).
9. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10. Dwu-składnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwu-składnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11. Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12. Analiza ruchu szyfrowanego protokołem SSH.

13. Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system

Polityki, Firewall

14. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń.
15. System musi zapewniać translację adresów NAT: źródłowego i docelowego, translację PAT oraz:
    - Translację jeden do jeden oraz jeden do wielu.
    - Dedykowany ALG (Application Level Gateway) dla protokołu SIP.
16. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
17. Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
18. Element systemu realizujący funkcję Firewall musi integrować się z następującymi rozwiązaniami SDN w celu dynamicznego pobierania informacji o zainstalowanych maszynach wirtualnych po to aby użyć ich przy budowaniu polityk kontroli dostępu.
    - Amazon Web Services (AWS).
    - Microsoft Azure
    - Google Cloud Platform (GCP).
    - OpenStack.
    - VMware NSX.

Połączenia VPN

1. System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
    - Wsparcie dla IKE v1 oraz v2.
    - Obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM).
    - Obsługa protokołu Diffie-Hellman grup 19 i 20.
    - Wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE.
    - Tworzenie połączeń typu Site-to-Site oraz Client-to-Site.
    - Monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności.
    - Możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego.
    - Obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth.
    - Mechanizm „Split tunneling" dla połączeń Client-to-Site.
2. System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
    - Pracę w trybie Portal - gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki. W tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0.
    - Pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta.
    - oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

Routing i obsługa łączy WAN

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

Funkcje SD-WAN

1. System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.
2. Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

Zarządzanie pasmem

1. System Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu.
2. Musi istnieć możliwość określania pasma dla poszczególnych aplikacji.
3. System musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL.

Ochrona przed malware

1. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021).
2. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR.
3. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android).
4. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.
5. Możliwość wykorzystania silnika sztucznej inteligencji AI wytrenowanego przez laboratoria producenta.

Ochrona przed atakami

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

Kontrola aplikacji

1. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP.
2. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora.
3. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików.

4. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P.
5. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.

Kontrola WWW

1. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne.
2. W ramach filtra www powinny być dostępne kategorie istotne z punktu widzenia bezpieczeństwa, jak: malware (lub inne będące źródłem złośliwego oprogramowania), phishing, spam, Dynamic DNS, proxy.
3. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard.
4. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL.
5. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo.
6. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
7. W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych url - system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

Uwierzytelnianie użytkowników w ramach sesji

1. System Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą:
   - Haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu.
   - Haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP.
   - Haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych.
2. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego.
3. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.
4. Uwierzytelnianie w oparciu o protokół SAML w politykach bezpieczeństwa systemu dotyczących ruchu HTTP.

Zarządzanie

1. Elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania.
2. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów.
3. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego.
4. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6. Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.

7. Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

Logowanie

1. Elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach przedmiotu zamówienia musi zostać dostarczony komercyjny system logowania i raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej.
2. W ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania.
3. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu.
4. Musi istnieć możliwość logowania do serwera SYSLOG.

Serwisy i licencje

W ramach przedmiotu zamówienia powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować kontrolę Aplikacji, IPS, Antywirus (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych - co najmniej dla systemu operacyjnego Android), Analiza typu Sandbox, Antyspam, Web Filtering, bazy reputacyjne adresów IP/domen na okres 36 miesięcy.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe AHB/SOS

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, przez okres [24] miesięcy. Stosujemy w przypadku AHB 24x7xNBD

Przełącznik 2 szt.

Przełącznik sieciowy

W celu realizacji bezpiecznej infrastruktury teleinformatycznej, w której wymagane mechanizmy centralnego systemu bezpieczeństwa obejmują elementy warstwy dostępowej sieci, wymaganym jest dostarczenie przełącznika współpracującego z oferowanym systemem bezpieczeństwa, w zakresie opisanym w sekcjach: "Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC" oraz "Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa", o następujących parametrach:

Parametry fizyczne platformy

- Wymiary urządzenia muszą pozwalać na montaż w szafie rack 19", obudowa nie może być wyższa niż 1U.
- Zasilanie AC 230V.
- Maksymalny pobór mocy: 30 W.
- Minimalny zakres temperatury pracy: 0-40°C.

Interfejsy sieciowe - wymagania minimalne

Wymaganym jest aby przełącznik dysponował niezależnymi interfejsami sieciowymi (nie dopuszcza się portów typu combo) w ilości:

a) 24 porty GE RJ-45.

e) 4 porty 10 GE SFP+.

Zarządzanie

- Wbudowany 1 port konsoli szeregowej do pełnego zarządzania.
- Zarządzanie przez: command line (w tym poprzez SSH) oraz poprzez graficzny interfejs z wykorzystaniem przeglądarki (HTTPS).
- Wsparcie dla SNMP w wersjach 1-3
- Funkcja zarządzania poprzez dedykowany kontroler przełączników lub system zarządzania, pozwalający na automatyczne wykrywanie, centralne konfigurowanie oraz zarządzanie przełącznikami.
- Funkcja aktualizacji oprogramowania przez TFTP/FTP oraz za pomocą GUI.
- Konfiguracja w formie pliku tekstowego umożliwiającego edycję konfiguracji offline.
- Funkcja backupu konfiguracji z poziomu GUI jak również z CLI (TFTP/FTP).
- Funkcja definiowania administratorów lokalnie oraz wykorzystanie w tym celu serwerów Radius i TACACS+.
- Funkcja definiowania ról administratorów z możliwością określenia trybu dostępu (brak, tylko odczyt, odczyt oraz modyfikacja) do wybranych części konfiguracji.
- Automatycznie wykonywane rewizje konfiguracji.

Parametry wydajnościowe

- Przepustowość urządzenia - min. 125 Gbps (pełna prędkość, tzw. wire-speed na wszystkich portach) oraz min. 190 Mpps.
- Tablica adresów MAC o pojemności co najmniej 32k wpisów.
- Opóźnienie wprowadzane przez przełącznik - poniżej 2 mikrosekund.

Wymagane funkcje

- Funkcja automatycznej negocjacji prędkości i duplexu dla połączeń.
- Obsługa Jumbo Frames.
- Obsługa 802.1d (Spanning Tree), 802.1w (Rapid Spanning Tree), 802.1s (Multiple Spanning Tree).
- Agregacja portów zgodna ze standardem 802.3ad.
- Obsługa co najmniej 4000 VLAN'ów, zgodna ze standardem 802.1Q.
- Obsługa routingu statycznego.
- Port-mirroring.
- Uwierzytelnianie 802.1x na poziomie portu.
- Uwierzytelnianie 802.1x w oparciu o adres MAC.
- W ramach 802.1x wsparcie dla dedykowanego VLAN'u dla gości (guest VLAN).
- W ramach 802.1x wsparcie dla urządzeń, które nie obsługują tego protokołu, na podstawie adresu MAC urządzenia.
- W ramach 802.1x wsparcie dla dynamicznego przypisywania VLAN.
- Obsługa protokołu sFlow.

Dodatkowe funkcje urządzenia przy integracji z systemem centralnego zarządzania / NAC

1. Przełączniki muszą wspierać tryb pracy, w którym są zarządzane przez fizyczny element nadrzędny (przełącznik lub dedykowany kontroler) (tzw. port extender lub element leaf w architekturze spine-leaf). Zakres zarządzania przez element nadrzędny musi zawierać co najmniej:
   - Centralne zarządzanie konfiguracją urządzenia
   - Aktualizacja oprogramowania realizowana z systemu centralnego zarządzania
   - Centralne zarządzanie sieciami VLAN.
   - Blokowanie ruchu pomiędzy klientami w ramach jednego VLAN'u
   - Rozpoznawanie urządzeń uzyskujących dostęp do sieci, zarówno stacji klienckich, jak i urządzeń typu drukarki, routery, przełączniki, itp..
   - Przenoszenie zidentyfikowanych urządzeń do właściwych stref. W przypadku wykrycia urządzenia niepasującego do zaakceptowanych schematów, urządzenie powinno przenieść go do strefy odizolowanej.
   - Integrację z systemem kontroli dostępu. Urządzenie musi podejmować decyzje o dostępie na podstawie przynajmniej następujących czynników: nazwy hosta, nazwy użytkownika, typu urządzenia, typu systemu operacyjnego.
   - Automatyczna detekcja i rekomendacje konfiguracji.
   - Przesyłanie logów na zewnętrzny serwer syslog.
   - Funkcja uruchomienia Captive Portalu w celu identyfikacji użytkowników.
   - Obsługa białych i czarnych list adresów MAC.
   - Wykrywanie aplikacji komunikujących się w sieci.
2. Musi być możliwe redundantne połączenie z elementami zarządzającymi.
3. W ramach przedmiotu zamówienia koniecznym jest dostarczenie wszystkich licencji niezbędnych do uruchomienia na przełączniku w/w funkcji, polegających na integracji z systemem centralnego zarządzania lub NAC.

Funkcje urządzenia przy integracji z systemem centralnego zarządzania lub bezpieczeństwa

- System musi realizować funkcję Stateful Firewall pomiędzy sieciami VLAN realizowanymi na urządzeniu dostępowym.
- System musi zapewniać Routing statyczny i dynamiczny (co najmniej OSPF) oraz Policy Based Routing.

Gwarancja oraz wsparcie

System musi być objęty serwisem gwarancyjnym przez okres 24 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu wykonawca musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.

Rozszerzone wsparcie serwisowe

System musi być objęty rozszerzonym wsparciem technicznym gwarantującym udostępnienie oraz dostarczenie sprzętu zastępczego na czas naprawy sprzętu w Następnym Dniu Roboczym od momentu potwierdzenia zasadności zgłoszenia, przez okres [36] miesięcy.

UPS 2 sztuki

UPS 6000VA (parametry minimalne)	
Parametr	**Wymagania minimalne**
Moc pozorna	min. 6000VA
Moc rzeczywista	min. 6000W
Technologia	on-line (VFI), podwójna konwersja
Sprawność max (dla VFI)	> 95 %
Typ obudowy	Rack / tower
praca sieciowa	
Napięcie wejściowe	110V – 275V
Częstotliwość napięcia wejściowego	45 - 55Hz
Zakres napięcia wyjściowego	208 V AC / 220 V AC / 230 V AC / 240 V AC
Wartość napięcia wyjściowego ustawiana z panelu LCD	tak
Kształt napięcia wyjściowego	sinusoidalny
Czas przełączania sieć – UPS	0ms
Współczynnik odkształceń prądu wejściowego THDi	< 3%
praca bateryjna	
Napięcie wyjściowe	~230V ± 1%
Częstotliwość napięcia wyjściowego	50Hz/60Hz ± 1Hz
Kształt napięcia wyjściowego na pracy bateryjnej	sinusoidalny
Zabezpieczenie przeciwzwarciowe gniazd wyjściowych	Bezpiecznik automatyczny 20 A
Zabezpieczenie przeciążeniowe	elektroniczne
Akumulatory wewnętrzne w UPS lub w Modułach Bateryjnych	minimum 12V 9Ah; szczelne, bezobsługowe
Czas podtrzymania dla obciążenia 6000W	minimum 7 min
Pozostałe	
Przeciążalność	100%<obciążenie ≤105%: ciągłe 105%<obciążenie ≤125%: 10 minut 125%<obciążenie ≤150%: 30s >150% : 500m
Wejście zasilania	Listwa zaciskowa
Ilość i typ gniazd wyjściowych	minimum 2x IEC 320 C13 (10 A) + listwa zaciskowa
Sygnalizacja	Wyświetlacz LCD (informacje wskazujące pracę sieciową, bateryjną, przeciążenie i ładowanie akumulatora). Diody LED informujące o pracy bateryjnej oraz stanie alarmowym.
Test baterii	Wymagana możliwość wykonania testu baterii do niskiego poziomu - możliwości całkowitego rozładowania baterii

Możliwość podłączenia dodatkowych, zewnętrznych modułów bateryjnych	Wymagana możliwość podłączenia minimum 6 zewnętrznych modułów bateryjnych
Interfejs komunikacyjny	minimum RS232, USB HID, SNMP/HTTP
Złącze EPO	wymagane NC
Styki bez potencjałowe zamontowane na stałe w obudowie UPS	wymagany minimum 1x wejściowy i 1x wyjściowy
Możliwość pracy równoległej	wymagana
Wsporniki do montażu w szafie RACK	wymagane
Wymiary UPS - wersja RACK	nie większe niż: wysokość 86mm; szerokość 440mm; głębokość 575mm
Wymiary MODUŁ BATERYJNY - wersja RACK	nie większe niż: wysokość 130mm; szerokość 440mm; głębokość 595mm
Łączna wysokość w szafie RACK 19" dla oferowanego zestawu	nie więcej niż 5U
Gwarancja	minimum 24 miesiące na elektronikę i 24 miesiące na akumulatory; Gwarancja realizowana wyłącznie przez autoryzowany serwis producenta.
Serwis	naprawa w maksymalnie 5 dni roboczych, serwis realizowany w systemie door to door
Oprogramowanie	oprogramowanie w języku polskim do zarządzania i monitorowania pracy UPS dla Windows, Linux oraz systemów wirtualizacji VMware, Hyper-V, Citrix XenServer
	możliwość edycji nazw urządzeń na liście monitorowanych UPSów
	wymagane wsparcie (telefoniczne oraz mailowe) w języku polskim odnośnie konfiguracji i rozwiązywania problemów.
Certyfikaty producenta	ISO 9001:2015 dla producenta sprzętu obejmujący proces projektowania, produkcji i serwisowania
	Sprzęt musi spełniać wymagania dyrektyw tzw. "Nowego Podejścia" Unii Europejskiej (UE), tj. musi posiadać deklarację CE.

Część 2

Dostawa serwera wraz z oprogramowaniem:

1. Serwer wraz z oprogramowaniem – 1 sztuka,
2. Oprogramowanie – upgrade (aktualizacja) z posiadanej przez Zamawiającego wersji Windows Serwer 2012 R2 do wersji:
   - 2 sztuki Windows Serwer 2022 Standard EDU,
   - 1 sztuka Windows Serwer 2019 Essentials.

Parametr	Charakterystyka (wymagania minimalne)
Obudowa	Obudowa Rack o wysokości max 2U z możliwością instalacji min. 8 dysków 3.5" wraz z kompletem szyn umożliwiających montaż w szafie rack 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 (Android/ Apple iOS) przy użyciu jednego z protokołów BLE/ WIFI.
Płyta główna	Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.
Chipset	Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych.
Procesor	Zainstalowany jeden procesor min. szesnasto-rdzeniowy klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 174 punktów w teście SPECrate2017_int_base dostępnym na stronie www.spec.org dla dwóch procesorów.
RAM	64GB DDR4 RDIMM 3200MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 1TB pamięci RAM.
Zabezpieczenia pamięci RAM	Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling
Gniazda PCI	Min. dwa sloty PCIe Gen 3
Interfejsy sieciowe/FC/SAS	Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T.
Napęd optyczny	Brak
Dyski twarde	Możliwość instalacji dysków SATA, SAS, SSD. Zainstalowane 4 dyski SSD SAS 12Gb/s o pojemności min. 1.92TB oraz 2 dyski 300GB SAS 15k. Możliwość zainstalowania modułu dedykowanego dla hypervisora wirtualizacyjnego, możliwość wyposażenia w dwa nośniki typu flash o pojemności min. 64GB z możliwoscią konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmiejszenia ilości wnęk na dyski twarde. Pamięć flash musi pochodzić bezpośrednio od producenta serwera. Możliwość instalacji dwóch dysków M.2 SATA o pojemności min. 480GB z możliością konfiguracji RAID 1.
Kontroler RAID	Sprzętowy kontroler dyskowy z pojemnością cache 8GB, możliwe konfiguracje poziomów RAID: 0,1,5,6,10,50,60.
Wbudowane porty	min. 2 porty USB 2.0 oraz 2 porty USB 3.0, 2 porty RJ45, min. 1 port VGA.
Video	Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1600x1200.
Wentylatory	Redundantne
Zasilacze	Redundantne, Hot-Plug min. 750W.
System Operacyjny	Zakres Przedmiotu Zamówienia obejmuje dostarczenie i wdrożenie Oprogramowania Systemowego zwanego dalej SSO. Licencja musi uprawniać do uruchamiania SSO w środowisku fizycznym i dwóch wirtualnych środowisk SSO za pomocą wbudowanych mechanizmów wirtualizacji. SSO musi posiadać następujące, wbudowane cechy:

	a) możliwość wykorzystania, co najmniej 320 logicznych procesorów oraz co najmniej 4 TB pamięci RAM w środowisku fizycznym, b) możliwość wykorzystywania 64 procesorów wirtualnych oraz 1TB pamięci RAM i dysku o pojemności min. 64TB przez każdy wirtualny serwerowy system operacyjny, c) możliwość budowania klastrów składających się z 64 węzłów, z możliwością uruchamiania do 8000 maszyn wirtualnych, d) możliwość migracji maszyn wirtualnych bez zatrzymywania ich pracy między fizycznymi serwerami z uruchomionym mechanizmem wirtualizacji (hypervisor) przez sieć Ethernet, bez konieczności stosowania dodatkowych mechanizmów współdzielenia pamięci, e) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany pamięci RAM bez przerywania pracy, f) wsparcie (na umożliwiającym to sprzęcie) dodawania i wymiany procesorów bez przerywania pracy, g) automatyczna weryfikacja cyfrowych sygnatur sterowników w celu sprawdzenia, czy sterownik przeszedł testy jakości przeprowadzone przez producenta systemu operacyjnego, możliwość dynamicznego obniżania poboru energii przez rdzenie procesorów niewykorzystywane w bieżącej pracy (mechanizm ten musi uwzględniać specyfikę procesorów wyposażonych w mechanizmy Hyper-Threading), i) wbudowane wsparcie instalacji i pracy na wolumenach, które: I. pozwalają na zmianę rozmiaru w czasie pracy systemu, II. umożliwiają tworzenie w czasie pracy systemu migawek, dających użytkownikom końcowym (lokalnym i sieciowym) prosty wgląd w poprzednie wersje plików i folderów, III. umożliwiają kompresję "w locie" dla wybranych plików i/lub folderów, IV. umożliwiają zdefiniowanie list kontroli dostępu (ACL), j) wbudowany mechanizm klasyfikowania i indeksowania plików (dokumentów) w oparciu o ich zawartość, k) wbudowane szyfrowanie dysków l) możliwość uruchamiania aplikacji internetowych wykorzystujących technologię ASP.NET, m) możliwość dystrybucji ruchu sieciowego HTTP pomiędzy kilka serwerów, n) wbudowana zapora internetowa (firewall) z obsługą definiowanych reguł dla ochrony połączeń internetowych i intranetowych, o) graficzny interfejs użytkownika, p) zlokalizowane w języku polskim, co najmniej następujące elementy: menu, przeglądarka internetowa, pomoc, komunikaty systemowe, r) wsparcie dla większości powszechnie używanych urządzeń peryferyjnych (drukarek, urządzeń sieciowych, standardów USB, Plug&Play), s) możliwość zdalnej konfiguracji, administrowania oraz aktualizowania systemu, t) dostępność bezpłatnych narzędzi producenta systemu umożliwiających badanie i wdrażanie zdefiniowanego zestawu polityk bezpieczeństwa, u) możliwość implementacji następujących funkcjonalności bez potrzeby instalowania dodatkowych produktów (oprogramowania) innych producentów wymagających dodatkowych licencji: I. podstawowe usługi sieciowe: DHCP oraz DNS wspierający DNSSEC, II. usługi katalogowe oparte o LDAP i pozwalające na uwierzytelnianie użytkowników stacji roboczych, bez konieczności instalowania dodatkowego oprogramowania na tych stacjach, pozwalające na zarządzanie zasobami w sieci (użytkownicy, komputery, drukarki, udziały sieciowe), z możliwością wykorzystania następujących funkcji: 1) podłączenie SSO do domeny w trybie offline – bez dostępnego połączenia sieciowego z domeną, 2) ustanawianie praw dostępu do zasobów domeny na bazie sposobu logowania użytkownika – na przykład typu certyfikatu użytego do logowania,

	3) odzyskiwanie przypadkowo skasowanych obiektów usługi katalogowej z mechanizmu kosza, III. zdalna dystrybucja oprogramowania na stacje robocze, IV. praca zdalna na serwerze z wykorzystaniem terminala (cienkiego klienta) lub odpowiednio skonfigurowanej stacji roboczej, V. centrum Certyfikatów (CA), obsługa klucza publicznego i prywatnego) umożliwiające: 1) dystrybucję certyfikatów poprzez http, 2) konsolidację CA dla wielu lasów domeny, 3) automatyczne rejestrowania certyfikatów pomiędzy różnymi lasami domen, VI. szyfrowanie plików i folderów, VII. szyfrowanie połączeń sieciowych pomiędzy serwerami oraz serwerami i stacjami roboczymi (IPSec), VIII.możliwość tworzenia systemów wysokiej dostępności (klastry typu fail-over) oraz rozłożenia obciążenia serwerów, IX. serwis udostępniania stron WWW, X. wsparcie dla protokołu IP w wersji 6 (IPv6), XI. wbudowane mechanizmy wirtualizacji (Hypervisor) pozwalające na uruchamianie min. 1000 aktywnych środowisk wirtualnych systemów operacyjnych. Wirtualne maszyny w trakcie pracy i bez zauważalnego zmniejszenia ich dostępności mogą być przenoszone pomiędzy serwerami klastra typu failover z jednoczesnym zachowaniem pozostałej funkcjonalności. Mechanizmy wirtualizacji mają zapewnić wsparcie dla: 1) dynamicznego podłączania zasobów dyskowych typu hot-plug do maszyn wirtualnych, 2) obsługi ramek typu jumbo frames dla maszyn wirtualnych, 3) obsługi 4-KB sektorów dysków, 4) nielimitowanej liczby jednocześnie przenoszonych maszyn wirtualnych pomiędzy węzłami klastra, 5) możliwości wirtualizacji sieci z zastosowaniem przełącznika, którego funkcjonalność może być rozszerzana jednocześnie poprzez oprogramowanie kilku innych dostawców poprzez otwarty interfejs API, 6) możliwości kierowania ruchu sieciowego z wielu sieci VLAN bezpośrednio do pojedynczej karty sieciowej maszyny wirtualnej (tzw. trunk model), v) możliwość automatycznej aktualizacji w oparciu o poprawki publikowane przez producenta wraz z dostępnością bezpłatnego rozwiązania producenta SSO umożliwiającego lokalną dystrybucję poprawek zatwierdzonych przez administratora, bez połączenia z siecią Internet, w) wsparcie dostępu do zasobu dyskowego SSO poprzez wiele ścieżek (Multipath), x) możliwość instalacji poprawek poprzez wgranie ich do obrazu instalacyjnego, y) mechanizmy zdalnej administracji oraz mechanizmy (również działające zdalnie) administracji przez skrypty, z) możliwość zarządzania przez wbudowane mechanizmy zgodne ze standardami WBEM oraz WS-Management organizacji DMTF.
Bezpieczeństwo	Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą.
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowane port RJ-45 Gigabit Ethernet umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej • 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 SNMP; IPMI2.0, VLAN tagging, SSH • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer, dane historyczne powinny być dostępne przez min. 7 dni wstecz.

	• możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer • integracja z Active Directory • możliwość obsługi przez ośmiu administratorów jednocześnie • Wsparcie dla automatycznej rejestracji DNS • wsparcie dla LLDP • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej • możliwość podłączenia lokalnego poprzez złącze RS-232. • możliwość zarządzania bezpośredniego poprzez złącze microUSB umieszczone na froncie obudowy. • Monitorowanie zużycia dysków SSD • możliwość monitorowania z jednej konsoli min. 100 serwerami fizycznymi, • Automatyczne zgłaszanie alertów do centrum serwisowego producenta • Automatyczne update firmware dla wszystkich komponentów serwera • Możliwość przywrócenia poprzednich wersji firmware • Możliwość eksportu eksportu/importu konfiguracji (ustawienie karty zarządzającej, BIOSu, kart sieciowych, HBA oraz konfiguracji kontrolera RAID) serwera do pliku XML lub JSON • Możliwość zaimportowania ustawień, poprzez bezpośrednie podłączenie plików konfiguracyjnych • Automatyczne tworzenie kopii ustawień serwera w oparciu o harmonogram.
Oprogramowanie zarządzające	• Wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych • integracja z Active Directory • Możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta • Wsparcie dla protokołów SNMP, IPMI, Linux SSH, Redfish • Możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram • Szczegółowy opis wykrytych systemów oraz ich komponentów • Możliwość eksportu raportu do CSV, HTML, XLS, PDF • Możliwość tworzenia własnych raportów w opraciu o wszystkie informacje zawarte w inwentarzu. • Grupowanie urządzeń w oparciu o kryteria użytkownika • Tworzenie automatycznie grup urządzeń w opraciu o dowolny element konfiguracji serwera np. Nazwa, lokalizacja, system operacyjny, obsadzenie slotów PCIe, pozostałego czasu gwarancji • Możliwość uruchamiania narzędzi zarządzających w poszczególnych urządzeniach • Szybki podgląd stanu środowiska • Podsumowanie stanu dla każdego urządzenia • Szczegółowy status urządzenia/elementu/komponentu • Generowanie alertów przy zmianie stanu urządzenia. • Filtry raportów umożliwiające podgląd najważniejszych zdarzeń • Integracja z service desk producenta dostarczonej platformy sprzętowej • Możliwość przejęcia zdalnego pulpitu • Możliwość podmontowania wirtualnego napędu • Kreator umożliwiający dostosowanie akcji dla wybranych alertów • Możliwość importu plików MIB • Przesyłanie alertów „as-is" do innych konsol firm trzecich • Możliwość definiowania ról administratorów • Możliwość zdalnej aktualizacji oprogramowania wewnętrznego serwerów • Aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania)

	• Możliwość instalacji oprogramowania wewnętrznego bez potrzeby instalacji agenta • Możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów • Moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjne sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCI i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie i poziomie gwarancji, adresy IP kart sieciowych, występujących aletrów, MAC adresów kart sieciowych, stanie poszczególnych komponentów serwera. • Możliwość tworzenia sprzętowej konfiguracji bazowej i na jej podstwie weryfikacji środowiska w celu wykrycia rozbieżności. • Wdrażanie serwerów, rozwiązań modularnych oraz przełączników sieciowych w opraciu o profile • Możliwość migracji ustawień serwera wraz z wirtualnymi adresami sieciowymi (MAC, WWN, IQN) między urządzeniami. • Tworzenie gotowych paczek informacji umożliwiających zdiagnozowanie awarii urządzenia przez serwis producenta. • Zdalne uruchamianie diagnostyki serwera. • Dedykowana aplikacja na urządzenia mobilne integrująca się z wyżej opisanymi oprogramowaniem zarzadzającym. • Oprogramowanie dostarczane jako wirtualny appliance dla KVM, ESXi i Hyper-V.
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2015 oraz ISO-14001. Serwer musi posiadać deklaracja CE. Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows" dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2, Windows Server 2016, Microsoft Windows Server 2019, Windows Server 2022.
Normy Środowiskowe	Oferowane produkty muszą zawierać informacje dotyczące ponownego użycia i recyklingu, nie mogą zawierać farb i powłok na dużych plastikowych częściach, których nie da się poddać recyklingowi lub ponownie użyć. Wszystkie produkty zawierające podzespoły elektroniczne oraz niebezpieczne składniki powinny być bezpiecznie i łatwo identyfikowalne oraz usuwalne. Usunięcie materiałów i komponentów powinno odbywać się zgodnie z wymogami Dyrektywy WEEE 2002/96/EC. Produkty muszą składać się z co najmniej w 65% ze składników wielokrotnego użytku/zdatnych do recyklingu. We wszystkich produktach części tworzyw sztucznych większe niż 25-gramowe powinny zawierać nie więcej niż śladowe ilości środków zmniejszających palność sklasyfikowanych w dyrektywie RE 67/548/EEC. Potwierdzeniem spełnienia powyższego wymogu jest wydruk ze strony internetowej www.epeat.net potwierdzający spełnienie normy co najmniej Epeat Bronze według normy wprowadzonej w 2019 roku. Potwierdzenie spełnienia kryteriów środowiskowych, w tym zgodności z dyrektywą RoHS Unii Europejskiej o eliminacji substancji niebezpiecznych w postaci oświadczenia producenta serwera (wg wytycznych Krajowej Agencji Poszanowania Energii S.A., zawartych w dokumencie *„Opracowanie propozycji kryteriów środowiskowych dla produktów zużywających energię możliwych do wykorzystania przy formułowaniu specyfikacji na potrzeby zamówień publicznych"*, pkt 3.4.2.1; dokument z grudnia 2006 r.), w szczególności zgodności z normą ISO 1043-4 dla płyty głównej oraz elementów wykonanych z tworzyw sztucznych o masie powyżej 25 gr.
Warunki gwarancji	36 miesięcy gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia. Zamawiający wymaga od Wykonawcy aby serwis świadczony był przez producenta sprzętu lub autoryzowany przez niego podmiot. W przypadku wystąpienia awarii dysku twardego

	w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Podmiot serwisujący musi posiadać ISO 9001:2015 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń.
Dokumentacja użytkownika	Zamawiający wymaga dokumentacji w języku polskim lub angielskim. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela.

Zamawiający wymaga uruchomienia, wdrożenia powyższego serwera wraz z oprogramowaniem systemowym, oraz zwirtualizowania 2 maszyn (Intel Xeon E3-125 3.30GHz,, RAM 24GB, HDD 560GB, Windows Serwer 2012 oraz Intel(R) Xeon(R) E5-2407, RAM 24GB, HDD 300GB) obecnie używanych w siedzibie zamawiającego.

Część 3.

Dostawa komputerów przenośnych oraz serwera NAS.

1. Komputer przenośny – 15 sztuk

Procesor	W teście ogólnym PCMark 8 Work Score Accelerated v2 komputer powinien osiągać wydajność nie mniej niż 5000 pkt lub w teście Cinebench R15 CPU Single 64Bit co najmniej 150 pkt. Spełnienie tego wymogu należy potwierdzić w jeden z poniższych sposobów: - wskazanie modelu na liście opublikowanych wyników testów w serwisie notebookcheck.net, wykonanych oprogramowaniem PCMark 8 lub Cicnebench R15:
System operacyjny	64bit w polskiej wersji językowej, w najnowszym dostępnym wydaniu, zapewniający możliwość przyłączania do domeny Active Directory oraz uruchamiania użytkowanych przez Zamawiającego programów takich jak: Microsoft Office 2016, ABBY Fine Reader dla Windows. System operacyjny musi zapewnić możliwość wykonywania kopii zapasowych na dyski sieciowe za pomocą narzędzi producenta systemu.
Wyświetlacz	o przekątnej 15,6 cala i rozdzielczości FHD (1920 × 1080), z powłoką przeciwodblaskową i podświetleniem LED, bez obsługi dotykowej
Pamięć	min 16 GB
Dysk	SSD o min pojemności 256 GB
Porty:	2 porty USB 3.1 Gen 1, 1 port USB 2.0, 1 port HDMI, 1 czytnik kart pamięci SD (SD, SDHC, SDXC), 1 złącze RJ45 — GbE 10/100/1000 MB/s,
Zasilacz	zasilacz
Inne	Normatywny czas pracy na baterii przy standardowym obciążeniu nie powinien być krótszy niż 5h Klawiatura wbudowana: Standardowa, pełnowymiarowa klawiatura odporna na zalanie, klawiatura numeryczna z 10 klawiszami.
gwarancja	24 miesiące

2. **Serwer Nas – 1 sztuka**

Nazwa elementu, parametru lub cechy	Opis wymagań
Rozmiar urządzenia	Pojedyncza obudowa serwerowa typu RACK nie większa niż 2U do montażu w szafie serwerowej. Urządzenie wyposażone w podwójny redundantny system zasilania oraz przystosowane do montażu w szafie RACK o głębokości 90 cm. Szyny dedykowane umożliwiające zamontowanie urządzenia w szafie RACK
Wydajność obliczeniowa	Procesor czterordzeniowy o częstotliwości taktowania min. 1.7 GHz
Pamięć RAM	Co najmniej 4GB z możliwością rozbudowy do min 16GB
Rozbudowa	Możliwość rozbudowy o min 12 dodatkowych dysków 3.5 cala przy użyciu dedykowanej jednostki rozszerzającą pamięć masowej.
Kieszenie na dyski:	Co najmniej 12 w jednostce centralnej przystosowane do montażu dysków 3,5'' SATA(III) / SATA(II) lub 2,5'' SATA III / SATA II HDD, SSD 2,5" SATA(III) / SATA(II)
Zasilanie	Min. 2 redundantne zasilacze o mocy max 250W
Pojemność:	Minimalna pojemność urządzenia: 60 TB (minimum 6 sztuk dysk serwerowy 10 TB 3.5" SATA III (6 Gb/s)) z możliwością rozbudowy do min. 216 TB wykorzystując dyski 18TB
Interfejs sieciowy:	Urządzenie wyposażone w co najmniej 2 x Gigabit RJ45 LAN oraz 2 x SFP+ 10Gbe
Gniazda zewnętrzne	Co najmniej: 4x USB 3.2 Gen 1 1x Pcie Gen 2x2
Dodatkowa funkcjonalność:	- funkcja hot-swap (możliwość wymiany dysku podczas pracy urządzenia), - Wake on LAN. - Hardware encryption engine AES-NI - Obsługa sieci bezprzewodowej (dopuszczalny adapter)
Sposób zabezpieczenia danych	Systemowy kontroler RAID - obsługa mechanizmu RAID: JBOD, 0,1,5,6,10, 5+hotspare
Obsługa protokołów sieciowych	iSCSI, Telnet, SSH, SNMP, FTP, AFP, CIFS
iSCSI	Liczba jednostek LUN iSCSI do 256
Systemy plików	Dyski wewnętrzne: EXT4. Dyski zewnętrzne: FAT, NTFS, EXT3, EXT4, HFS+
Bezpieczeństwo	- FTP przez SSL/TLS, - automatyczne blokowanie adresów IP, - zapora sieciowa,
Zarządzanie	Co najmniej za pośrednictwem przeglądarki internetowej.
Wirtualizacja serwerów	Vmware vSphere min. 5, Citrix, Microsoft.
Gwarancja:	24 miesiące. Możliwość szybkiego zgłaszania usterek przez portal internetowy. Wsparcie producenta zawierać ma m.in. dostęp do portalu producenta na którym udostępniane będą aktualne sterowniki, oprogramowanie (np. zarządzające lub diagnostyczne) oraz aktualizacje firmware-a do oferowanego urządzenia, a także (opcjonalnie) dostęp do bazy wiedzy i aktualnej dokumentacji technicznej.

Certyfikat	Sprzęt musi spełniać wymagania dyrektyw tzw. "Nowego Podejścia" Unii Europejskiej (UE), tj. musi posiadać deklarację CE.

Załącznik nr 2 do SWZ – wzór formularza ofertowego

NR SPRAWY: ZP.272.4/2021

Dane Wykonawcy (-ów):
nazwa: .....
adres: .....
email: .....
ePuap: .....

Działając w imieniu wymienionego powyżej wykonawcy(ów) oferuję(emy) realizację na rzecz zamawiającego zamówienia publicznego na: *dostawę i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19*

OŚWIADCZAM(Y), ŻE:

1. zapoznałem się z treścią SWZ dla niniejszego zamówienia,
2. akceptuję w pełni i bez zastrzeżeń postanowienia: SWZ oraz wzoru umowy dla niniejszego zamówienia, wyjaśnień do SWZ oraz jej zmian,
3. oferuję realizację przedmiotu zamówienia na następujących warunkach:
   a) **cześć 1**:
   cena ..... (netto) PLN (słownie: ..... złotych) plus należny podatek VAT w wysokości ..... PLN, co czyni łącznie cenę brutto..... PLN (słownie: ..... złotych),
   termin dostawy – 70/80/90* dni licząc od dnia podpisania umowy.
   niepotrzebne skreślić
   b) **cześć 2:**
   cena ..... (netto) PLN (słownie: ..... złotych) plus należny podatek VAT w wysokości ..... PLN, co czyni łącznie cenę brutto ..... PLN (słownie: ..... złotych),
   termin dostawy – 70/80/90* dni licząc od dnia podpisania umowy.
   niepotrzebne skreślić
   c) **cześć 3:**
   cena ..... (netto) PLN (słownie: ..... złotych) plus należny podatek VAT w wysokości ..... PLN, co czyni łącznie cenę brutto..... PLN (słownie: ..... złotych),
   termin dostawy – 40/50/60* dni licząc od dnia podpisania umowy.
   niepotrzebne skreślić
4. Oświadczam, iż jestem związany ofertą do terminu wskazanego w SWZ.
5. Oświadczam, iż podany w mojej ofercie adres e-mailowy jest właściwy do komunikowania się z Zamawiającym.

6. Oświadczam, że wybór naszej oferty **będzie/nie będzie**** prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług w myśl art. 225 ustawy Pzp.

**niepotrzebne skreślić. Jeśli ten punkt nie zostanie wypełniony przez Wykonawcę, Zamawiający uznaje, że wybór oferty Wykonawcy nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług w myśl art. 225 ustawy Pzp. W przypadku, zaznaczenia, że wybór oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego wykonawca obowiązany jest wskazać:

- nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego,
- wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
- wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

7. Informuję, iż prowadzona działalność klasyfikuje się jako: **Mikroprzedsiębiorstwo/Małe przedsiębiorstwo/Średnie przedsiębiorstwo** *(niepotrzebne skreślić)*. Informacja niezbędna do celów statystycznych Urzędu Zamówień Publicznych zgodnie z zaleceniami Komisji Europejskiej.

   Mikroprzedsiębiorstwo - przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EURO.

   Małe przedsiębiorstwo – przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EURO.

   Średnie przedsiębiorstwo - przedsiębiorstwo, które nie jest mikroprzedsiębiorstwem ani małym przedsiębiorstwem i które zatrudnia mniej niż 250 osób i którego roczny obrót nie przekracza 50 milionów EURO lub roczna suma bilansowa nie przekracza 43 milionów EURO.

8. PODWYKONAWCY:

   Oświadczam, że[1]:

   a) przedmiot zamówienia wykonamy siłami własnymi;
   b) powierzymy następującym podwykonawcom realizację następujących części zamówienia:

L.p.	Nazwa (firma) podwykonawcy	Część (zakres) przedmiotu zamówienia powierzony podwykonawcy

   c) powołujemy się na zasoby niżej wymienionych podmiotów w celu wykazania spełnienia warunków udziału w postępowaniu, o których mowa w SWZ, na zasadach określonych w art. 118 ustawy Pzp.

Lp.	Nazwa (firma) podwykonawcy	Udostępnione zasoby

[1] Niepotrzebne skreślić. W przypadku nie skreślenia którejś z pozycji i nie wypełnienia tabeli w pozycji b) lub c) - Zamawiający uzna, odpowiednio, że Wykonawca nie zamierza powierzyć wykonania żadnej części zamówienia podwykonawcom i Wykonawca nie polega na zasobach podwykonawcy (innego podmiotu) w celu wykazania spełniania warunków udziału w postępowaniu, o których mowa w SWZ.

9. Niniejszym **wskazuję, iż** następujące informacje stanowią tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (Dz. U. z 2019 r. poz. 1010 i 1649):

L.p.	**Oznaczenie rodzaju (nazwy) informacji**

Podpis elektroniczny lub podpis zaufany albo podpis osobisty w postaci elektroniczne

Załącznik nr 3 do SWZ - wzór oświadczenia o niepodleganiu wykluczeniu z postępowania.

NR SPRAWY: ZP.272.4/2021

ZAMAWIAJĄCY:
Muzeum Niepodległości w Warszawie
al. Solidarności 62, 00-240 Warszawa

Wykonawca/Podwykonawca/Podmiot trzeci:

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

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp),
DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „*dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19*", prowadzonego przez Zamawiającego Muzeum Niepodległości w Warszawie, oświadczam, co następuje:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy Pzp

..... *(miejscowość),* dnia ..... r.

2. Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ..... ustawy Pzp *(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2, 5 i 6).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:
.....
..... *(miejscowość),* dnia ..... r.

3. Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia zamawiającego w błąd przy przedstawianiu informacji.

Podpis elektroniczny lub podpis zaufany albo podpis osobisty w postaci elektronicznej

Załącznik nr 4 do SWZ - wzór oświadczenia wykonawcy jako administratora danych osobowych w rozumieniu RODO potwierdzający stosowanie przez wykonawcę przepisów RODO.

NR SPRAWY: ZP.272.4/2021

ZAMAWIAJĄCY:
Muzeum Niepodległości w Warszawie
al. Solidarności 62, 00-240 Warszawa

Wykonawca:

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

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 13 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) zwanego dalej RODO,

DOTYCZĄCE POTWIERDZENIA STOSOWANIA PRZEZ WYKONAWCĘ PRZEPISÓW RODO

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „*dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19*", prowadzonego przez Zamawiającego Muzeum Niepodległości w Warszawie, oświadczam, co następuje:

OŚWIADCZENIE DOTYCZĄCE WYKONAWCY:

Oświadczam, że:
a) wypełniłem ciążące na mnie jako Administratorze danych osobowych w rozumieniu RODO obowiązki informacyjne przewidziane w art. 13 i/lub art. 14 RODO) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu;
b) wszelkie dane osobowe wskazane przeze mnie w treści jakichkolwiek dokumentów złożonych w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu pozyskałem i przetwarzam zgodnie z powszechnie obowiązującymi przepisami prawa.

Podpis elektroniczny lub podpis zaufany albo podpis osobisty w postaci elektronicznej

Załącznik nr 5 do SWZ - wzór oświadczenia wykonawcy działającego w imieniu zamawiającego, potwierdzający stosowanie przepisów RODO

NR SPRAWY: ZP.272.4/2021

ZAMAWIAJĄCY:
Muzeum Niepodległości w Warszawie
al. Solidarności 62, 00-240 Warszawa

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

.....
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie wykonawcy

składane na podstawie art. 14 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) zwanego dalej RODO,

DOTYCZĄCE ZOBOWIĄZANIA WYKONAWCY DZIAŁAJĄCEGO W IMIENIU ZAMAWIAJĄCEGO DO PRZEKAZANIA INFORMACJI WYMAGANYCH PRZEZ RODO

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. „*dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19*", prowadzonego przez Zamawiającego Muzeum Niepodległości w Warszawie, oświadczam, co następuje:

OŚWIADCZENIE DOTYCZĄCE WYKONAWCY:

Oświadczam, że zobowiązuję się do przekazania w imieniu Zamawiającego wszystkim osobom, których dane osobowe udostępniłem Zamawiającemu w celu ubiegania się o udzielenie zamówienia publicznego w prowadzonym postępowaniu oraz w związku z zawarciem umowy i jej realizacją, informacji, o których mowa w art. 14 RODO, chyba, że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO oraz na etapie ubiegania się o udzielnie zamówienia publicznego zobowiązuje się składać Zamawiającemu stosowne oświadczenie o wypełnieniu wyżej wskazanego obowiązku, a na etapie zawarcia i realizacji umowy zobowiązuję się każdorazowo poinformować Zamawiającego o wypełnianiu tego obowiązku.

Podpis elektroniczny lub podpis zaufany albo podpis osobisty w postaci elektronicznej

Załącznik nr 6 do SWZ – projektowane postanowienia umowy

WZÓR UMOWY

zawarta w dniu ..... w Warszawie pomiędzy:

Muzeum Niepodległości w Warszawie, al. Solidarności 62, 00-240 Warszawa, NIP: 526-030-79-04, Samorządową Instytucją Kultury wpisaną do Rejestru Instytucji Kultury pod nr 14/99, reprezentowanym przez:

.....

zwanym dalej **„Zamawiającym"**

a

..... z siedzibą w ..... ul ..... wpisaną do ..... prowadzonego przez ....., pod nr .....

reprezentowanym przez:

.....

zwanym dalej **„Wykonawcą"**

zwanymi również dalej łącznie **„Stronami"** lub pojedynczo **„Stroną"**

W wyniku rozstrzygnięcia postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym bez negocjacji na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129), zwanej dalej *ustawą* pod nazwą: „dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19", została zawarta umowa o następującej treści;

§1 Przedmiot Umowy

1. Przedmiot umowy stanowi dostawa i montaż urządzeń komputerowych i sieciowych na potrzeby Muzeum Niepodległości w Warszawie w związku z zapobieganiem i przeciwdziałaniem COVID-19 w zakresie **część 1/część 2/część 3** dla Muzeum Niepodległości w Warszawie w terminie i na warunkach określonych Umową.
2. Szczegółowy opis i zakres przedmiotu Umowy został określony w załączniku nr 1 do SWZ oraz ofercie Wykonawcy, które stanowią integralne części Umowy.
3. Wykonawca oświadcza, iż dostarczony przedmiot Umowy będzie fabrycznie nowy, wolny od wad fizycznych i prawnych, wcześniej nieużywany, zgodny ze złożoną przez Wykonawcę ofertą.
4. Wykonawca, w ramach przedmiotu Umowy, dostarczy niezbędne do działania dodatkowe (akcesoria), zapewniające możliwość należytego użytkowania dostarczonych urządzeń.
5. Wykonawca zobowiązuje się zrealizować przedmiot Umowy określony w § 1 zgodnie z:
   a) Opisem przedmiotu zamówienia oraz złożoną ofertą;
   b) Warunkami wynikającymi z przepisów technicznych oraz zaleceń producenta;
   c) Wymogami wynikającymi z obowiązujących norm i aprobat technicznych;
   d) Zasadami rzetelnej wiedzy technicznej, należytą zawodową starannością i najwyższymi normami branżowymi.
6. Wraz z dostawą przedmiotu umowy Wykonawca zobowiązany jest przekazać Zamawiającemu wszelkie dokumenty niezbędne do prawidłowego i zgodnego z przeznaczeniem używania przedmiotu Umowy, w tym przede wszystkim instrukcje obsługi i karty gwarancyjne.

§2 Termin realizacji

1. Wykonawca zobowiązany jest do wykonania Przedmiotu Umowy w terminie .... dni licząc od dnia podpisania umowy[2].
2. Wykonawca zobowiązuje się do dostawy przedmiotu Umowy na własny koszt i ryzyko do siedziby Zamawiającego po uprzednim uzgodnieniu daty dostawy z Zamawiającym, zgodnie z procedurą określoną w niniejszym paragrafie. Wraz z dostawą przedmiotu Umowy, Wykonawca dostarczy Zamawiającemu kartę katalogową, instrukcje oraz ewentualnie inne dokumenty wymagane przez obowiązujące przepisy, oraz niezbędne do prawidłowego i zgodnego z przeznaczeniem używania przedmiotu Umowy, w tym przede wszystkim instrukcje obsługi i karty gwarancyjne.
3. Do kontaktów bieżących w sprawie przedmiotu Umowy Strony wyznaczają swoich przedstawicieli:
   ze strony Zamawiającego:
   .....
   lub inna/inne wskazana/-e pisemnie osoba/-y
   ze strony Wykonawcy:
   .....
   lub inna/inne wskazana/-e pisemnie osoba/-y.
4. Wszelkie powiadomienia związane z wykonywaniem przedmiotu Umowy będą dokonywane drogą elektroniczną z wykorzystaniem danych kontaktowych, o których mowa w ust. 3.

§3 Wynagrodzenie

1. Strony ustalają wysokość wynagrodzenia Wykonawcy z tytułu należytego wykonania całości przedmiotu Umowy określonego w § 1, zgodnie ze złożoną przez Wykonawcę ofertą, na kwotę netto: _____ **zł** (słownie: _____ zł i __/100), plus należny podatek VAT w wysokości: _____ **zł** (słownie: _____ zł i __/100), razem brutto: _____ **zł** (słownie: _____ zł i __/100).
2. W wynagrodzeniu określonym w ust.1 mieszczą się wszelkie koszty wykonania przedmiotu Umowy w tym między innymi koszty transportu, montażu, koszty przeprowadzenia wszelkich pomiarów i sprawdzeń, koszty szkoleń, koszty ubezpieczenia, koszty napraw uszkodzonych elementów wystroju wnętrz, serwis gwarancyjny itp.
3. Podstawą płatności będzie wystawiona przez Wykonawcę faktura VAT obejmująca całość przedmiotu Umowy, przy czym Zamawiający zastrzega konieczność uzgodnienia zapisów na fakturach przed ich złożeniem pod rygorem ich nieprzyjęcia.
4. Podstawą wystawienia faktury jest podpisany przez upoważnionych przedstawicieli obu Stron Protokół odbioru końcowego, potwierdzającego odbiór bez zastrzeżeń przedmiotu Umowy.
5. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy Wykonawcy w terminie do 30 dni licząc od dnia przedłożenia Zamawiającemu prawidłowo wystawionej faktury, przy czym za dzień spełnienia świadczenia pieniężnego uważać się będzie dzień złożenia polecenia przelewu w banku Zamawiającego.
6. Zapłata będzie dokonywana z zastosowaniem mechanizmu podzielonej płatności, o którym mowa w art.108a-108d ustawy *o podatku od towaru i usług* (t.j. Dz. U. z 2019 poz. 1520).
7. Zamawiający zobowiązuje się do umieszczenia na fakturze rachunku bankowego, który widnieje na tzw. „białej liście podatników" prowadzonej przez Szefa Krajowej Administracji Skarbowej.

§ 4 [Odbiór przedmiotu Umowy]

1. Po wykonaniu przedmiotu Umowy, Wykonawca zgłosi pisemnie Zamawiającemu gotowość do odbioru.
2. Odbioru przedmiotu Umowy dokona komisja, w której znajdą się przedstawiciele Wykonawcy i Zamawiającego.

---

[2] Zgodnie ze złożoną ofertą

3. Czynności odbioru będą polegały na:
   1) weryfikacji kompletności i zgodności z Umową dostarczonego przedmiotu Umowy;
   2) weryfikacji kompletności i zgodności z Umową wszystkich dokumentów złożonych przez Wykonawcę, a w szczególności certyfikatów, oświadczeń oraz deklaracji wymaganych zgodnie z załącznikiem nr 1 do SWZ.
4. Dla dokonania odbioru przedmiotu Umowy, niezbędne jest stwierdzenie kompletności i zgodności z Umową dostarczonego przedmiotu Umowy potwierdzonego stosownym protokołem.
5. Za datę wykonania przedmiotu Umowy, przyjmuje się datę podpisania przez komisję, o której mowa w ust. 2, Protokołu odbioru końcowego.
6. Jeśli w toku czynności odbioru zostaną stwierdzone wady dające się usunąć, to Zamawiający odmówi odbioru do czasu ich usunięcia i wyznaczy Wykonawcy termin na ich usunięcie.
7. Zamawiający może podjąć decyzję o przerwaniu czynności odbioru, jeżeli w czasie tych czynności ujawniono istnienie takich wad, które uniemożliwiają używanie przedmiotu Umowy zgodnie z przeznaczeniem, aż do czasu usunięcia tych wad.
8. W przypadku niewykonania przedmiotu Umowy w dodatkowym terminie wyznaczonym przez Zamawiającego, o którym mowa w ust. 6 lub, gdy wady stwierdzone podczas procedury odbioru usunąć się nie dadzą albo gdy z okoliczności wynika, że Wykonawca nie zdoła ich usunąć w czasie odpowiednim, Zamawiający może od Umowy odstąpić, w całości lub niewykonanej części, jeżeli wady są istotne. Jeżeli wady nie są istotne, Zamawiający może żądać obniżenia wynagrodzenia w odpowiednim stosunku. To samo dotyczy wypadku, gdy Wykonawca nie usunął wad w terminie wyznaczonym przez Zamawiającego.

§5 Przedstawiciele stron

1. Przedstawicielem Zamawiającego upoważnionym w sprawach związanych z niniejszą Umową jest .....
2. Przedstawicielem Wykonawcy upoważnionym w sprawach związanych z niniejszą Umową jest ..... .

§6 Odstąpienie od Umowy

1. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu Zamawiający może odstąpić od Umowy w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.
2. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części Umowy.
3. Odstąpienie od Umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.
4. Zamawiającemu przysługuje prawo natychmiastowego odstąpienia od umowy w sytuacji, gdy:
   1) zostanie wydany nakaz zajęcia majątku Wykonawcy,
   2) Wykonawca nie rozpoczął realizacji Przedmiotu Umowy bez uzasadnionych przyczyn mimo uprzedniego wezwania go przez Zamawiającego i upływie dodatkowego terminu wyznaczonego do należytej realizacji Umowy;
   3) Wykonawca mimo upływu terminu wyznaczonego w wezwaniu do należytego wykonania umowy
   w dalszym ciągu w sposób nienależyty wykonuje zobowiązania zawarte w niniejszej Umowie;
5. Odstąpienie od Umowy następuje w formie pisemnej pod rygorem nieważności i powinno zawierać uzasadnienie. Prawo odstąpienia Zamawiający może wykonać w terminie 30 dni od daty powzięcia wiadomości o podstawach do jego wykonania.

§7 Kary umowne

1. Zamawiający uprawniony jest do naliczenia następujących kar umownych:
   1) za zwłokę w wykonaniu przedmiotu Umowy, karę w wysokości 0,2% wynagrodzenia brutto

ustalonego w § 3 ust. 1 Umowy, za każdy rozpoczęty dzień zwłoki,

2) za zwłokę w usuwaniu wad lub usterek przedmiotu Umowy w okresie gwarancji, w tym za zwłokę w dostarczeniu komponentów urządzeń wolnych od wad lub komponentu zastępczego, karę w wysokości 0,1 % wynagrodzenia brutto ustalonego w § 3 ust. 1 Umowy, za każdy rozpoczęty dzień zwłoki, liczony od następnego dnia po dniu wyznaczonym zgodnie z Umową na usunięcie wad lub dostarczenie urządzenia wolnego od wad lub urządzenia zastępczego,
3) za odstąpienie od Umowy w całości lub w części, przez którąkolwiek ze Stron, z przyczyn zależnych od Wykonawcy, karę w wysokości 20% wynagrodzenia brutto ustalonego w § 3 ust. 1 Umowy,
4) za każdy stwierdzony przypadek nienależytego wykonania umowy przez Wykonawcę w wysokości 0,2 % wynagrodzenia umownego brutto, ustalonego w § 3 ust. 1 Umowy, za każdy stwierdzony przypadek nienależytego wykonania umowy.

2. Kary mogą podlegać sumowaniu.
3. Zamawiający zastrzega sobie prawo do dochodzenia zapłaty odszkodowania uzupełniającego przenoszącego wysokość kar umownych do wysokości faktycznie poniesionej szkody.
4. Wykonawca ponosi pełną odpowiedzialność z tytułu niewykonania lub nienależytego wykonania przez niego zobowiązań, w tym w przypadku odstąpienia od Umowy lub rozwiązania Umowy z przyczyn leżących po stronie Wykonawcy.
5. Wykonawca ponosi pełną odpowiedzialność za działania lub zaniechania osób, którymi posługuje się przy wykonywaniu przedmiotu Umowy, przy czym Strony wyłączają zwolnienie się Wykonawcy z odpowiedzialności na podstawie art. 429 kodeksu cywilnego.
6. Wykonawca ponosi pełną odpowiedzialność za zapewnienie i przestrzeganie warunków bezpieczeństwa i higieny pracy oraz przepisów ppoż. w czasie wykonywania przedmiotu Umowy.
7. Łączna wysokość kar umownych należnych Zamawiającemu na podstawie niniejszej Umowy jest ograniczona do 30 % wynagrodzenia brutto, o którym mowa w § 3 ust. 1 Umowy.
8. Wykonawca zobowiązuje się do zapłacenia kary umownej w terminie 7 dni od otrzymania wezwania do zapłaty.

§8 Warunki zmiany Umowy

1. Zamawiający dopuszcza możliwość zmiany treści Umowy, poza przypadkami określonymi w art. 455 ustawy, w następujących sytuacjach:
   a) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań technologicznych lub technicznych, niż te istniejące w chwili zawarcia Umowy, nie powodujących zmiany przedmiotu Umowy,
   b) powstała możliwość zastosowania nowszych i korzystniejszych dla Zamawiającego rozwiązań w zakresie modelu/typu sprzętu/oprogramowania w przypadku zakończenia produkcji lub braku dostępności na rynku pod warunkiem, że sprzęt/program będzie posiadał parametry jakościowe i techniczne nie gorsze od oferowanego przez Wykonawcę w złożonej ofercie modelu/typu oprogramowania i nie spowoduje podwyższenia ceny,
   c) po zawarciu Umowy doszło do wydłużenia okresu gwarancyjnego przez producenta,
   d) wystąpienia przyczyn niezależnych od obu stron lub z powodu działania siły wyższej,
   e) ustawowej zmiany stawki podatku VAT na przedmiot niniejszej Umowy, jeśli zmiana nastąpi w czasie jej trwania. Zmiana stawek podatku VAT spowoduje zmianę kwot podatku VAT i ceny brutto wynikającej z Umowy, cena netto pozostanie niezmieniona.
2. Strona występująca o zmianę postanowień Umowy zobowiązana jest do udokumentowania zaistnienia okoliczności, o których mowa w ust. 1.
3. Wniosek o zmianę postanowień Umowy musi być wyrażony na piśmie.

§ 9 Gwarancja

1. Wykonawca na przedmiot Umowy udzieli gwarancji w zakresie i w terminach zgodnych z opisem przedmiotu zamówienia stanowiącym załącznik nr 1 do SWZ.

2. W ramach wynagrodzenia, o którym mowa w § 3 ust. 1 Umowy Wykonawca zobowiązuje się do zapewnienia w okresie gwarancji serwisu gwarancyjnego dostarczonych urządzeń w zakresie zgodnym z opisem przedmiotu zamówienia określonym w załączniku nr 1 do SWZ.
3. Wykonawca usunie wszelkie ujawnione wady i usterki Urządzeń w ramach gwarancji w terminie **3 dni roboczych** od momentu ich zgłoszenia na adres mail: _____ lub telefonicznie pod nr: _____. Przez usunięcie wad i usterek przedmiotu Umowy, rozumie się naprawę lub wymianę wadliwych komponentów przedmiotu Umowy na nowe lub dostarczenie urządzeń zastępczych o takich samych lub lepszych parametrach (do czasu docelowej naprawy). W przypadku wystąpienia wad i usterek, których ze względów technologicznych nie można usunąć w tym czasie, Wykonawca usunie je w terminie określonym przez Zamawiającego.
4. Zamawiający wymaga aby w przypadku ujawnionych wad i usterek, Wykonawca określił sposób usunięcia wady lub/i usterki w terminie 2 dni roboczych od momentu ich zgłoszenia na adres e-mail wskazany w § 2 ust. 3 umowy.
5. Okres gwarancji ulega odpowiedniemu przedłużeniu o czas trwania napraw gwarancyjnych.
6. Nieusunięcie przez Wykonawcę wad lub usterek w uzgodnionym terminie daje Zamawiającemu prawo do zlecenia ich usunięcia na koszt Wykonawcy. Powyższe nie będzie skutkować utratą praw z gwarancji.
7. Jeżeli z powodu nieusunięcia w uzgodnionym terminie wad i usterek, które ujawnią się w okresie gwarancji, wystąpią udokumentowane szkody poniesione przez Zamawiającego lub osoby trzecie, Wykonawca poniesie wszelkie koszty związane z naprawą tych szkód.
8. Wykonawca najpóźniej w dniu przekazania przedmiotu Umowy dostarczy Zamawiającemu dokumenty gwarancyjne, w których powinny być zawarte warunki serwisowe oraz wszelkie instrukcje obsługi.
9. Wykonawca zobowiązuje się odebrać wadliwe urządzenia osobiście lub pokryć koszty ich transportu do i z siedziby Wykonawcy, lub do i z wskazanego przez Wykonawcę autoryzowanego punktu serwisowego, właściwego dla producenta dostarczonego przedmiotu Umowy.
10. Strony przedłużają okres obowiązywania rękojmi do końca okresu gwarancji.

§ 10 Licencje i autorskie prawa majątkowe

1. W ramach wynagrodzenia określonego w § 3 ust. 1 Umowy, do oprogramowania wchodzącego w zakres przedmiotu umowy, jeżeli są autorstwa innych podmiotów niż Wykonawca, Wykonawca udzieli lub zapewni udzielenie przez podmiot trzeci Zamawiającemu licencji/sublicencji.
2. W odniesieniu do licencji/sublicencji na oprogramowanie wchodzące w zakres przedmiotu umowy, Wykonawca udziela Zamawiającemu lub zapewni udzielenie przez podmiot trzeci licencji/sublicencji niewyłącznej na czas nieoznaczony (bez prawa do jej wypowiedzenia przez okres 5 lat licząc od dnia odbioru przedmiotu umowy) do korzystania z oprogramowania wchodzącego w zakres przedmiotu umowy oraz z dokumentacji dotyczącej tego oprogramowania, na warunkach określonych przez producenta oprogramowania z zastrzeżeniem, że udzielona licencja/sublicencja obejmować będzie co najmniej następujące pola eksploatacji:
   a) trwałe lub czasowe zwielokrotnianie w całości lub w części jakimikolwiek środkami i w jakiejkolwiek formie, na jakichkolwiek nośnikach, w szczególności za pomocą druku, technik reprograficznych, filmu, na dysku komputerowym, w formie zapisu magnetycznego, na nośnikach cyfrowych, w szczególności w celu wprowadzania, wyświetlania, stosowania, przekazywania i przechowywania;
   b) tłumaczenie, przystosowanie, zmiana układu, tworzenie nowych wersji, opracowań, adaptacji lub jakiekolwiek inne zmiany na potrzeby Zamawiającego;
   c) rozpowszechnianie, w tym użyczenie, najem, dzierżawa, wniesienie jako aport oraz każde odpłatne i nieodpłatne oddanie do używania lub używania i pobierania pożytków z oprogramowania lub jego kopii.
3. Wykonawca zapewnia w ramach wynagrodzenia określonego w § 3 ust. 1 Umowy w okresie gwarancji aktualizacje oprogramowania wchodzącego w zakres przedmiotu umowy (np. w wyniku tworzenia aktualizacji lub nowych wersji oprogramowania).

4. Wykonawca zapewnia i gwarantuje, że przekazane Zamawiającemu oprogramowanie i licencja na korzystanie z oprogramowania wchodzącego w zakres przedmiotu umowy zostaną nabyte od podmiotów uprawnionych do ich sprzedaży lub udzielenia, i że Wykonawca jest uprawniony do przeniesienia tej licencji na Zamawiającego. Dostarczone oprogramowanie i licencja nie będzie naruszać praw osób trzecich.
5. Wynagrodzenie określone w § 3 ust. 1 obejmuje całkowite wynagrodzenie z tytułu udzielonej licencji/ sublicencji na korzystanie z oprogramowania, a Wykonawca oświadcza, że ani on, ani producent oprogramowania lub inna osoba trzecia nie będzie w przyszłości dochodzić od Zamawiającego zapłaty jakiegokolwiek wynagrodzenia z tego tytułu.
6. Wykonawca zobowiązuje się, że wykonując Umowę będzie przestrzegał przepisów o prawie autorskim i prawach pokrewnych i nie naruszy praw majątkowych osób trzecich, a utwór przekaże Zamawiającemu w stanie wolnym od obciążeń prawami tych osób.
7. W przypadku wystąpienia przez jakąkolwiek osobę trzecią w stosunku do Zamawiającego, z roszczeniem z tytułu naruszenia praw autorskich, zarówno osobistych jak i majątkowych, jeżeli naruszenie nastąpiło w związku z nienależytym wykonaniem postanowień niniejszych Umowy przez Wykonawcę, Wykonawca:
   a) przyjmie na siebie pełną odpowiedzialność za powstanie oraz wszelkie skutki powyższych zdarzeń;
   b) w przypadku skierowania sprawy na drogę postępowania sądowego wstąpi do procesu po stronie Zamawiającego i pokryje wszelkie koszty związane z udziałem Zamawiającego w postępowaniu sądowym oraz ewentualnym postępowaniu egzekucyjnym, w tym koszty obsługi prawnej postępowania;
   c) poniesie wszelkie koszty związane z ewentualnym pokryciem roszczeń majątkowych i niemajątkowych związanych z naruszeniem praw autorskich majątkowych lub osobistych osoby lub osób zgłaszających roszczenia.
   d) Wykonawca ma obowiązek, na swój koszt, uzyskać dla Zamawiającego prawo do dalszego używania oprogramowania wchodzącego w zakres przedmiotu umowy nieobciążonego wadami prawnymi lub zastąpić oprogramowanie innym produktem, nienaruszającym powyższych praw, lub zmienić je w taki sposób, że przestanie on naruszać powyższe prawa. Dostarczony zamiennie produkt będzie spełniał wymagania Zamawiającego w stopniu nie mniejszym, niż oprogramowanie podlegające wymianie.

§ 11 Poufność

1. W trakcie trwania niniejszej Umowy, a także po jej rozwiązaniu przez okres 3 lat Wykonawca zobowiązuje się zachować w bezwzględnej tajemnicy i nie przekazywać, nie ujawniać ani nie wykorzystywać bez pisemnej zgody Zamawiającego informacji organizacyjnych, księgowych, finansowych, personalnych, handlowych, statystycznych, pracowniczych, dotyczących Zamawiającego, lub podmiotów z nim współpracujących, które Wykonawca uzyska przy wykonywaniu niniejszej Umowy, chyba że stan tajemnicy wobec tych informacji ustał lub ich ujawnienia zażąda uprawniony organ w przewidzianej prawem formie, jednakże tylko w niezbędnym zakresie.
2. Wykonawca odpowiada również za zachowanie powyższych informacji w tajemnicy przez osoby, którym wykonanie swoich obowiązków powierzył.
3. Wykonawca zobowiązany jest do zachowania w tajemnicy wszelkich informacji mających wpływ na stan bezpieczeństwa Zamawiającego.
4. Wykonawca zobowiązuje się do wykorzystywania przetwarzanych przez niego w ramach realizacji niniejszej Umowy danych osobowych wyłącznie w celach określonych w Umowie i w tym zakresie umożliwi Zamawiającemu w każdym czasie i bez ograniczenia kontrolę procesu przetwarzania i ochrony danych osobowych.

§ 12 Klauzula informacyjna dotycząca RODO

Zgodnie z art. 13 ust. 1 i 2 oraz art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. 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, informuję, że:

1. Administratorem danych osobowych Wykonawcy jest Muzeum Niepodległości w Warszawie, al. Solidarności 62, 00-240 Warszawa.
2. Administrator wyznaczył Inspektora Ochrony Danych, z którym można skontaktować się pod adresem email: iod@muzeumniepodleglosci.art.pl;
3. Dane osobowe Wykonawcy będą przetwarzane na podstawie art. 6 ust. 1 lit. c RODO oraz na podstawie przepisów ustawy PZP w celu związanym z postępowaniem o udzielenie zamówienia publicznego, zawarciem umowy oraz jej realizacją oraz na podstawie art. 6 ust. 1 lit. f RODO zgodnie z pkt. 5. W przypadku przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. f) RODO za prawnie uzasadniony interes Administratora uznaje się:
   a) ustalenie lub dochodzenie przez Administratora roszczeń cywilnoprawnych wynikających z realizacji niniejszej Umowy, a także obrona przed takimi roszczeniami;
   b) weryfikacja danych osobowych w publicznych rejestrach.
4. Odbiorcami danych osobowych Wykonawcy będą osoby lub podmioty upoważnione zgodnie z przepisami prawa powszechnie obowiązującego, którym udostępniona zostanie dokumentacja postępowania, w tym w szczególności w oparciu o przepisy ustawy. Odbiorcami państwa danych będą: podmioty i organy, którym Administrator jest zobowiązany lub upoważniony udostępnić dane osobowe na podstawie powszechnie obowiązujących przepisów prawa, oraz podmioty, które na podstawie stosownych umów przetwarzają dane osobowe powierzone do przetwarzania przez Administratora w związku z realizacją usług gwarantujących należyte wykonanie niniejszej Umowy;
5. Dane osobowe Wykonawcy będą przechowywane, zgodnie z przepisami ustawy, 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. W przypadku zawarcia i realizacji umowy obejmuje również okres niezbędny do zabezpieczenia ewentualnych roszczeń wynikających z umowy, chyba, że przepisy szczegółowe stanowią inaczej;
6. Obowiązek podania przez Wykonawcę danych osobowych bezpośrednio dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp w związku z art. 6 ust. 1 lit. c RODO związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;
7. w odniesieniu do danych osobowych Wykonawcy decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8. Wykonawca posiada:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych dotyczących Wykonawcy;
   - na podstawie art. 16 RODO prawo do sprostowania danych osobowych Wykonawcy;
   - 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 Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;
   - prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych, który administrator przetwarza na podstawie art. 6 ust. 1 lit. f RODO w związku z treścią pkt 3 i 5;
9. 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.

§ 13 Informacja publiczna i dane osobowe

1. Wykonawca oświadcza, że znany jest mu fakt, iż treść umowy, a w szczególności przedmiot umowy i wysokość wynagrodzenia, stanowią informację publiczną w rozumieniu art. 1 ust. 1

ustawy z dnia 6 września 2001 r. *o dostępie do informacji publicznej*, która podlega udostępnieniu w trybie przedmiotowej ustawy, z zastrzeżeniem ust. 2 poniżej.

2. Wykonawca wyraża zgodę na udostępnianie w trybie ustawy, o której mowa w ust. 1 powyżej, zawartych w umowie dotyczących go danych osobowych w zakresie obejmującym ……..
3. Wykonawca niniejszym wyraża zgodę na przetwarzanie jego danych osobowych, wymienionych w umowie i załącznikach, w celu realizacji umowy oraz ich archiwizacji i udokumentowania przez Zleceniodawcę wypłaconych wynagrodzeń.

§14 Postanowienia końcowe

1. Ewentualne kwestie sporne wynikłe w trakcie realizacji niniejszej Umowy strony rozstrzygać będą polubownie. W przypadku nie dojścia do porozumienia spory rozstrzygane będą przez sąd właściwy dla siedziby Zamawiającego.
2. W sprawach nieuregulowanych postanowieniami niniejszej Umowy mają odpowiednie zastosowanie przepisy ustawy Prawo zamówień publicznych oraz Kodeksu Cywilnego.
3. Umowę sporządzono w 2 jednobrzmiących egzemplarzach po 1 dla każdej ze stron.

Zamawiający	**Wykonawca**
……	……

Załącznik nr 7 do SWZ – wzór formularza cenowego

Załącznik nr do SWZ – formularz cenowy

Część 1

Lp.	Nazwa towaru	Nawa urządzenia/ nazwa producenta	ilość	cena jednostkowa netto	wartość netto	wartość brutto
1.	Wielofunkcyjna zapora sieciowa 1		2 szt.			
2.	Wielofunkcyjna zapora sieciowa 2		2 szt.			
3.	Przełącznik sieciowy		2 szt.			
4.	UPS		2 szt.			
5.	Montaż, wdrożenie i konfiguracja wszystkich urządzeń w siedzibach zamawiającego	----------	1 kpl.			
					RAZEM brutto	

Część 2

Lp.	Nazwa towaru	Nawa urządzenia/ nazwa producenta	ilość	cena jednostkowa netto	wartość netto	wartość brutto
1.	Serwer wraz z oprogramowaniem		1 szt.			
2.	Windows Serwer 2022 Standard EDU		2 szt.			
3.	Windows Serwer 2019 Essentials		1 szt.			
4.	Montaż, wdrożenie, konfiguracja oraz wirtualizacja dwóch maszyn	----------	1 kpl.			
					RAZEM	

Część 3

Lp.	Nazwa towaru	Nawa urządzenia/ nazwa producenta	ilość	cena jednostkowa netto	wartość netto	wartość brutto
1.	Komputer przenośny		15 szt.			
2.	Serwer NAS		1 szt.			
					RAZEM brutto	

Podpis elektroniczny lub podpis zaufany albo podpis osobisty w postaci elektronicznej