SPECYFIKACJA WARUNKÓW ZAMÓWIENIA

Tryb podstawowy (bez negocjacji)

na zadanie pod nazwą:

Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”

(znak sprawy RR.PFZ.271.20.2022)

Szczytno, dnia 22.06.2022 r.

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.

I. INFORMACJE O ZAMAWIAJĄCYM

Gmina Szczytno
ul. Łomżyńska 3
12-100 Szczytno
Województwo: Warmińsko-Mazurskie
tel. (89) 623 25 80
fax. (89) 623 25 92
e-mail: ugszczytno@ug.szczytno.pl
www.ug.szczytno.pl
NIP: 745 181 12 30
REGON: 510 743 261

II. ADRES STRONY INTERNETOWEJ, NA KTÓREJ UDOSTĘPNIANE BĘDĄ ZMIANY I WYJAŚNIENIA TREŚCI SWZ ORAZ INNE DOKUMENTY ZAMÓWIENIA BEZPOŚREDNIO ZWIĄZANE Z POSTĘPOWANIEM O UDZIELENIE ZAMÓWIENIA

Zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postepowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: https://platformazakupowa.pl/pn/ug_szczytno.

III. TRYB UDZIELENIA ZAMÓWIENIA

1. Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129 z późn. zm.) [zwanej dalej także „pzp"].Zamawiający nie przewiduje wyboru najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
2. Podstawa prawna opracowania niniejszej SWZ:
1) ustawa z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2021 r., poz. 1129 z późn. zm.);
2) Ustawa z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (Dz.U. z 2022 r., poz. 835);
3) Rozporządzenie Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może zażądać zamawiający od wykonawcy (Dz. U. z 2020 r., poz. 2415);

4) Rozporządzenie 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).

Zamawiający zastrzega możliwość unieważnienia przedmiotowego postępowania, jeżeli środki, które Zamawiający zamierzał przeznaczyć na sfinansowanie całości lub części zamówienia, nie zostały mu przyznane - art. 310 pkt 1 ustawy Prawo zamówień publicznych.

IV. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa do siedziby Zamawiającego w ramach projektu grantowego „Cyfrowa Gmina":

Dostawa sprzętu sieciowego i serwerów

Kody CPV
48820000-2 Serwery
48823000-3 Serwery plików
48214000-1 Pakiety oprogramowania do sieciowego systemu operacyjnego
48219500-1 Pakiety oprogramowania do switcha lub routera
31154000-0 Bezprzestojowe źródła energii
48624000-8 Pakiety oprogramowania dla systemów operacyjnych komputerów osobistych (PC)
- serwer aplikacyjny szt. 1
- serwer NAS – służący do archiwizacji i backupu szt. 1
- przełącznik zarządzalny szt. 1
- UPS – zasilacz awaryjny szt. 1

Dostawa zapory sieciowej firewall

Kod CPV 48760000-3 Pakiety oprogramowania do ochrony antywirusowej

- Firewall UTM szt. 1 (Gmina)
- Firewall UTM szt. 1 (GOPS)

Dostawa komputerów stacjonarnych szt. 38

Kod CPV

30213100-5 komputery osobiste

48624000-8 Pakiety oprogramowania dla systemów operacyjnych komputerów osobistych (PC)

Przedmiot dostawy musi być fabrycznie nowy, nieużywany, wolny od wad i kompletny tj. posiadający wszelkie akcesoria, przewody, kable niezbędne do ich użytkowania. Zaoferowany sprzęt musi być gotowy do użytkowania bez dodatkowych zakupów. Musi pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych. Cały asortyment składający się na przedmiot zamówienia powinien być nowy, nie noszący śladów uszkodzeń zewnętrznych i uprzedniego używania, tzn. że żadne urządzenie, produkt nie może być wcześniej używane, winien być sprawny, odpowiednio zapakowany, spełniać wszelkie wymogi norm określonych obowiązującym prawem.

Szczegółowy opis przedmiotu zamówienia stanowi załącznik nr 1 do SWZ.

Zamawiający wymaga, aby Wykonawca w formularzu ofertowym w kolumnie „oferowane parametry" w każdym wierszu wskazał oferowane parametry poprzez podanie nazwy producenta, typu, modelu lub numeru katalogowego oferowanego sprzętu. Złożenie oferty poprzez wpisanie wyrażeń typu: „zgodnie z dokumentacją postępowania" lub przepisanie wymagań przedmiotowych określonych przez Zamawiającego z kolumny „minimalne wymagania" do kolumny „oferowane parametry" itp. jest niewystarczające i sama deklaracja realizacji zamówienia zgodnie z SWZ bez indywidualizacji, konkretyzacji, wskazania konkretnych parametrów bez podania nazwy producenta/ typu/ modelu/ nr katalogowego oferowanego przedmiotu zamówienia, stanowi niezgodność treści oferty z treścią SWZ i odrzucenie oferty na podstawie art. 226 ust. 1 pkt 5 ustawy prawo zamówień publicznych.

Załącznikami do szczegółowego opisu zamówienia są wyniki odpowiednich testów stanowiące minimalne wymagania stawiane przez Zamawiającego.

W przypadkach, kiedy w szczegółowym opisie przedmiotu zamówienia wskazane zostały znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, który charakteryzuje produkty lub usługi dostarczane przez konkretnego Wykonawcę, co prowadziłoby do uprzywilejowania lub wyeliminowania niektórych Wykonawców lub produktów, oznacza to, że Zamawiający nie może opisać przedmiotu zamówienia w wystarczająco precyzyjny i zrozumiały sposób i jest to uzasadnione specyfiką przedmiotu zamówienia. W

takich sytuacjach ewentualne wskazania na znaki towarowe, patenty, pochodzenie, źródło lub szczególny proces, należy odczytywać z wyrazami „lub równoważne".

W sytuacjach, kiedy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1, ust. 3 Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym, a wskazane powyżej odniesienia należy odczytywać z wyrazami „lub równoważne".

Pod pojęciem rozwiązań równoważnych Zamawiający rozumie taki sprzęt, który posiada parametry techniczne i funkcjonalne spełniające co najmniej warunki określone w szczegółowym opisie przedmiotu zamówienia stanowiącym załącznik nr 1 do SWZ. Wykonawca, który powołuje się na rozwiązania równoważne opisywanym przez Zamawiającego, jest obowiązany udowodnić w ofercie, że proponowane rozwiązania w równoważnym stopniu spełniają wymagania określone w szczegółowym opisie przedmiotu zamówienia.

Na realizację przedmiotowego zamówienia Zamawiający otrzymał grant nr 4215/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina".

2. Zamawiający dopuszcza powierzenie wykonania części zamówienia Podwykonawcy.

3. Zamawiający żąda wskazania przez Wykonawcę w ofercie części zamówienia, których wykonanie powierzy Podwykonawcom oraz podania nazw ewentualnych Podwykonawców, jeżeli są już znani.

4. Zamawiający nie dokonał podziału zamówienia na części, ponieważ przedmiotem zamówienia jest dostawa jednakowego asortymentu.

V. OPIS CZĘŚCI ZAMÓWIENIA, JEŻELI DOPUSZCZA SIĘ SKŁADANIE OFERT CZĘŚCIOWYCH

Zamawiający nie dopuszcza możliwości składania ofert częściowych.

VI. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie do 6 miesięcy od dnia podpisania umowy.

VII. 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. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną przy użyciu *platformy zakupowej* dostępnej pod adresem: https://platformazakupowa.pl/pn/ug_szczytno.

2. Zaleca się, aby Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, posiadał konto na *platformie zakupowej*. Rejestracja oraz logowanie dostępne jest pod adresem: https://platformazakupowa.pl/pn/ug_szczytno/login. Korzystanie z Platformy przez Wykonawcę jest bezpłatne.

3. Wymagania techniczne i organizacyjne wysyłania i odbierania korespondencji elektronicznej przekazywanej przy ich użyciu, opisane zostały w Regulaminie korzystania z *platformy zakupowej* dostępnym pod adresem: https://platformazakupowa.pl/strona/1-regulamin.

4. Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego, akceptuje warunki korzystania z *platformy zakupowej*, określone w Regulaminie dostępnym pod adresem: https://platformazakupowa.pl/strona/1-regulamin.

5. Maksymalny rozmiar plików przesyłanych za pośrednictwem dedykowanych formularzy do: złożenia i wycofania oferty oraz do komunikacji wynosi 150MB.

6. Za datę przekazania oferty, oświadczenia, o którym mowa w art. 125 ust. 1 pzp, podmiotowych środków dowodowych, przedmiotowych środków dowodowych oraz innych informacji, oświadczeń lub dokumentów, przekazywanych w postępowaniu, przyjmuje się datę ich przekazania na *platformę zakupową*.

7. W postępowaniu o udzielenie zamówienia korespondencja elektroniczna (inna niż oferta Wykonawcy i załączniki do oferty) odbywa się elektronicznie za pośrednictwem *platformy zakupowej* i formularza *Wyślij wiadomość.* Korespondencja przesłana za pomocą tego formularza nie może być szyfrowana. We wszelkiej korespondencji związanej z niniejszym postępowaniem Zamawiający i Wykonawcy posługują się numerem ogłoszenia (BZP).

8. Zamawiający może również komunikować się z Wykonawcami za pomocą poczty elektronicznej, email: ugszczytno@ug.szczytno.pl lub kamilasamsel@ug.szczytno.pl.

9. Dokumenty elektroniczne, oświadczenia lub elektroniczne kopie dokumentów lub oświadczeń składane są przez Wykonawcę za pośrednictwem formularza *Wyślij wiadomość* jako załączniki. Zamawiający dopuszcza również możliwość składania dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń za pomocą poczty elektronicznej, na adres email ugszczytno@ug.szczytno.pl.

Sposób sporządzenia dokumentów elektronicznych, oświadczeń lub elektronicznych kopii dokumentów lub oświadczeń musi być zgody 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).

10. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

VIII.INFORMACJA O WARUNKACH UDZIAŁU W POSTĘPOWANIU

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) nie podlegają wykluczeniu;
   2) spełniają warunki udziału w postępowaniu określone przez Zamawiającego w ogłoszeniu o zamówieniu i niniejszej SWZ.
2. Zamawiający wymaga wykazania przez Wykonawcę spełnienia warunków określonych w art. 112 ust. 2 ustawy pzp dotyczących zdolności technicznej i zawodowej:
   1) Zamawiający uzna warunek za spełniony, jeżeli wykonawca przedstawi wykaz dostaw, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, zrealizował co najmniej jedno zamówienie którego przedmiotem była dostawa sprzętu komputerowego o wartości minimalnej 100 000,00 zł (słownie sto tysięcy złotych) wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy.

3. Wykonawca może w celu potwierdzenia spełniania warunków udziału w postępowaniu, w stosownych sytuacjach polegać na zdolnościach technicznych lub zawodowych lub sytuacji finansowej lub ekonomicznej podmiotów udostępniających zasoby, niezależnie od charakteru prawnego łączących go z nimi stosunków pranych.
4. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia Wykonawcy mogą polegać na zdolnościach podmiotów udostępniających zasoby,

jeśli podmioty te wykonają roboty budowlane lub usługi, do realizacji których te zdolności są wymagane.

5. **Wykonawca, który polega na zdolnościach lub sytuacji podmiotów udostępniających zasoby, składa wraz z ofertą**, zobowiązanie podmiotu (wzór - załącznik nr 5 SWZ) udostępniającego zasoby do oddania mu do dyspozycji niezbędnych zasobów na potrzeby realizacji danego zamówienia lub inny podmiotowy środek dowodowy potwierdzający, że Wykonawca, realizując zamówienie, będzie dysponował niezbędnymi zasobami tych podmiotów. Zobowiązanie podmiotu udostępniającego zasoby ma potwierdzać, że stosunek łączący Wykonawcę z podmiotami udostępniającymi zasoby gwarantuje rzeczywisty dostęp do tych zasobów oraz określa w szczególności:
   1) zakres dostępnych Wykonawcy zasobów podmiotu udostępniającego zasoby;
   2) sposób i okres udostępnienia Wykonawcy i wykorzystania przez niego zasobów podmiotu udostępniającego te zasoby przy wykonywaniu zamówienia;
   3) czy i w jakim zakresie podmiot udostępniający zasoby, na zdolnościach którego Wykonawca polega w odniesieniu do warunków udziału w postępowaniu dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia, zrealizuje roboty budowlane lub usługi, których wskazane zdolności dotyczą.
6. W odniesieniu do warunków dotyczących wykształcenia, kwalifikacji zawodowych lub doświadczenia **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 takim przypadku Wykonawcy wspólnie ubiegający się o udzielenie zamówienia **dołączają do oferty oświadczenie**, z którego wynika, które roboty budowlane lub usługi wykonają poszczególni Wykonawcy.

IX. PODSTAWY WYKLUCZENIA WYKONAWCY Z POSTĘPOWANIA

1. O udzielenie przedmiotowego zamówienia mogą ubiegać się **Wykonawcy,** którzy nie podlegają wykluczeniu na podstawie art. 108 ust. 1 Ustawy pzp oraz art. 109 ust. 1 pkt 1, 4, i 7 Ustawy pzp oraz wykonawcy, w stosunku do którego zachodzi którakolwiek z okoliczności wskazanych w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.
2. Jeżeli Wykonawca **polega na zdolnościach lub sytuacji podmiotów** udostępniających zasoby Zamawiający zbada, czy nie zachodzą wobec tego podmiotu podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.
3. W przypadku wspólnego **ubiegania się** Wykonawców o udzielenie zamówienia Zamawiający bada, czy nie zachodzą podstawy wykluczenia wobec każdego z tych Wykonawców.

Jeżeli Wykonawca zamierza powierzyć wykonanie części zamówienia **Podwykonawcy,** Zamawiający zbada, czy nie zachodzą wobec tego Podwykonawcy podstawy wykluczenia, które zostały przewidziane względem Wykonawcy.

X. INFORMACJA O PODMIOTOWYCH I PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

1. **Wykonawca dołącza do oferty**, następujące podmiotowe środki dowodowe potwierdzające spełnianie warunków udziału w postępowaniu:

1) **wykaz dostaw**, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, zrealizował co najmniej jedno zamówienie którego przedmiotem była dostawa sprzętu komputerowego o wartości minimalnej 100 000,00 zł (słownie sto tysięcy złotych) wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów - oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy (wzór wykazu - załącznik nr 6 do SWZ);

2. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia należy przekazać Zamawiającemu przy użyciu środków komunikacji elektronicznej dopuszczonych w SWZ, w zakresie i sposób określony w przepisach 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). Podmiotowe środki dowodowe i przedmiotowe środki dowodowe sporządzone w języku obcym muszą być złożone wraz z tłumaczeniem na język polski.

3. Wykaz przedmiotowych środków dowodowych:

Dostawa sprzętu sieciowego i serwerów

- wyniki testu zaoferowanego procesora zgodnie z https://www.spec.org/cpu2017/results/ w dniu złożenia ofert

- Certyfikat ISO9001 oraz ISO-14001 dla producenta sprzętu

- Deklaracja zgodności CE

- wydruk ze strony potwierdzający, że serwer widnieje na liście Windows Server Catalog i posiada status „Certified for Windows" dla systemów Microsoft Windows Server 2019 i Windows Server 2022.

- oświadczenie podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego.

- Certyfikat ISO 9001:2008 dla firmy serwisującej na świadczenie usług serwisowych wraz z autoryzacją producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty.

- oświadczenie Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

Dostawa zapory sieciowej firewall

- certyfikat ICSA lub EAL4 dla funkcji Firewall

Dostawa komputerów stacjonarnych

- Deklaracja zgodności CE

- oświadczenie Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta.

4. Dopuszcza się złożenie przedmiotowych środków dowodowych w jednym egzemplarzu w przypadku, gdy odnoszą się równocześnie do dwóch lub więcej elementów przedmiotu zamówienia.

5. Przedmiotowe środki dowodowe składa się wraz z ofertą.

6. Zamawiający dopuszcza możliwość uzupełnienia przedmiotowych środków dowodowych.

XI. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert do dnia 29.07.2022 r.

2. W przypadku, gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w SWZ, Zamawiający przed upływem terminu związania oferta zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.

3. Przedłużenie terminu związania oferta, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XII. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Oferta musi być sporządzona w języku polskim, w postaci elektronicznej w formacie danych: .pdf, .doc, .docx, .rtf,.xps, .odt i opatrzona kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
2. Wykonawca w celu poprawnego zaszyfrowania oferty powinien mieć zainstalowane na komputerze oprogramowanie oraz aplikacje zgodne z wymogami opisanymi w *Instrukcji dla wykonawców* dostępnej pod adresem:
https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view.
3. Sposób zaszyfrowania oferty opisany został w *Instrukcji dla wykonawców* dostępnej pod adresem: https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view.
4. Do przygotowania oferty konieczne jest posiadanie przez osobę upoważnioną do reprezentowania Wykonawcy kwalifikowanego podpisu elektronicznego, podpisu osobistego lub podpisu zaufanego.
5. Jeżeli na ofertę składa się kilka dokumentów, Wykonawca powinien stworzyć folder, do którego przeniesie wszystkie dokumenty oferty, podpisane kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Następnie z tego folderu Wykonawca zrobi folder.zip (bez nadawania mu haseł i bez szyfrowania). W kolejnym kroku za pośrednictwem *platformy zakupowej* folder zawierający dokumenty składające się na ofertę Wykonawcy zostanie zaszyfrowany.
6. Wszelkie informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2020 r. poz. 1913 z późn. zm.), które Wykonawca zastrzeże, jako tajemnicę przedsiębiorstwa, powinny zostać złożone w osobnym pliku wraz z jednoczesnym zaznaczeniem polecenia „Załącznik stanowiący tajemnicę przedsiębiorstwa" a następnie wraz z plikami stanowiącymi jawną część skompresowane do jednego pliku archiwum (ZIP). Wykonawca zobowiązany jest, wraz z przekazaniem tych informacji, wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zaleca się, aby uzasadnienie zastrzeżenia informacji jako tajemnicy przedsiębiorstwa było sformułowane w sposób umożliwiający jego udostępnienie. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia, będzie traktowane przez Zamawiającego jako bezskuteczne ze względu na zaniechanie przez Wykonawcę podjęcia niezbędnych działań w celu zachowania poufności objętych klauzulą informacji zgodnie z postanowieniami art. 18 ust. 3 pzp.
7. Do oferty należy dołączyć oświadczenie o niepodleganiu wykluczeniu w postaci elektronicznej opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, a następnie wraz z plikami stanowiącymi ofertę skompresować do jednego pliku archiwum (ZIP).
8. Do przygotowania oferty zaleca się wykorzystanie Formularza Oferty, którego wzór stanowi Załącznik nr 2 do SWZ. W przypadku, gdy Wykonawca nie korzysta z przygotowanego przez Zamawiającego wzoru, w treści oferty należy zamieścić wszystkie informacje wymagane w Formularzu Ofertowym.
9. Do oferty należy dołączyć:
9.1. Pełnomocnictwo upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik;

9.2. Pełnomocnictwo dla pełnomocnika do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia;

9.3. **Wykonawca dołącza do oferty oświadczenie**, o którym mowa w art. 125 ust. 1 Ustawy, **którego wzór stanowią załączniki nr 3 i 4 do SWZ**. Oświadczenie stanowi dowód potwierdzający brak podstaw wykluczenia, spełnianie warunków udziału w postępowaniu na dzień składania ofert.

9.4. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców **oświadczenie,** o którym mowa powyżej - załączniki nr 3 i 4 do SWZ, składa każdy z Wykonawców. Oświadczenia te potwierdzają brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.

9.5. W przypadku polegania przez Wykonawcę na zdolnościach lub sytuacji podmiotów udostępniających zasoby, Wykonawca przedstawia, wraz z oświadczeniem, o którym mowa w ust. 2, także oświadczenie podmiotu udostępniającego zasoby - załączniki nr 3 i 4 do SWZ, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu w zakresie, w jakim Wykonawca powołuje się na jego zasoby.

9.6. W przypadku Wykonawcy, który zamierza powierzyć wykonanie części zamówienia Podwykonawcy**,** Wykonawca przedstawia, wraz z oświadczeniem, o którym mowa w pkt. 9.3, także oświadczenie Podwykonawcy - załącznik nr 3 do SWZ, potwierdzające brak podstaw wykluczenia tego Podwykonawcy.

9.7. Oświadczenia, o których mowa powyżej, składa się wraz z ofertą, pod rygorem nieważności, w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.

10. Oferta oraz oświadczenia, o których mowa w pkt. 9.3 muszą być złożone w oryginale.

11. Zamawiający zaleca ponumerowanie stron oferty.

12. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t. j. w formie elektronicznej lub postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. – Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.

13. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie.

XIII. WYMAGANIA DOTYCZĄCE WADIUM

1. Zamawiający wymaga od Wykonawców wniesienia wadium w wysokości:

3.000,00 zł (słownie: trzy tysiące złotych 00/100).

2. Wadium wnosi się przed upływem terminu składania ofert tj. **do dnia 30 czerwca 2022 r., do godz. 11:00** i utrzymuje nieprzerwanie do dnia upływu terminu związania ofertą, z wyjątkiem przypadków, o których mowa w art. 98 ust. 1 pkt 2 i 3 oraz ust. 2 Ustawy.

3. Wadium może być wnoszone według wyboru Wykonawcy w jednej lub kilku następujących formach:
1) pieniądzu;
2) gwarancjach bankowych
3) gwarancjach ubezpieczeniowych;
4) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z 9.11.2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (Dz. U. z 2019 r. poz. 310 ze zm.)
4. Wadium wnoszone w pieniądzu wpłaca się przelewem na rachunek bankowy Zamawiającego:

Gmina Szczytno ul. Łomżyńska 3, 12-100 Szczytno

Bank Spółdzielczy w Szczytnie nr 79 8838 0005 2001 0000 1661 0005

tytułem: „Wadium – Nr sprawy: RR.PFZ.271.20.2022”.

W przypadku wnoszenia wadium w pieniądzu, Zamawiający uzna je za **wniesione skutecznie jeżeli najpóźniej w terminie składania ofert, nastąpi uznanie wskazanego przez Zamawiającego rachunku bankowego o kwotę wadium.**

5. Jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, o których mowa w ust. 3 pkt 2 – 4 Wykonawca przekazuje Zamawiającemu **oryginał gwarancji lub poręczenia, w postaci elektronicznej.**

6. Z treści gwarancji (poręczenia) musi jednoznacznie wynikać nieodwoływalne i bezwarunkowe, na pierwsze żądanie zgłoszone przez Zamawiającego, zobowiązanie gwaranta (poręczyciela) do zapłaty Zamawiającemu pełnej kwoty wadium w okolicznościach określonych w art. 98 ust. 6 ustawy. Ponadto powinien być wskazany termin obowiązywania gwarancji (poręczenia), który nie może być krótszy niż termin związania ofertą.

XIV. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Wykonawca może złożyć tylko jedną ofertę.

2. Wykonawca składa ofertę, pod rygorem nieważności, w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci opatrzonej podpisem zaufanym lub podpisem osobistym.
3. Oferta powinna być podpisana przez osobę upoważnioną/osoby upoważnione do reprezentowania Wykonawcy.
4. Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie do jego reprezentowania nie wynika z dokumentów rejestrowych (KRS, CEiDG lub innego właściwego rejestru), Wykonawca dołącza do oferty pełnomocnictwo.
5. Pełnomocnictwo do złożenia oferty lub oświadczenia, o którym mowa w art. 125 ust. 1 Ustawy pzp, przekazuje się:

   1) w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) – jeżeli oferta została złożona w formie elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym;

   2) w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem zaufanym – jeżeli oferta została złożona w postaci elektronicznej opatrzonej podpisem zaufanym;

   3) w formie elektronicznej (tj. w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym) lub w postaci elektronicznej opatrzonej podpisem osobistym – jeżeli oferta została złożona w postaci elektronicznej opatrzonej podpisem osobistym.
6. W przypadku, gdy pełnomocnictwo do złożenia oferty lub oświadczenia, o którym mowa w art. 125 ust. 1 Ustawy pzp, zostało sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym – w zależności od tego jakim podpisem opatrzono ofertę, potwierdzającym zgodność odwzorowania cyfrowego z dokumentem w postaci papierowej. Odwzorowanie cyfrowe pełnomocnictwa powinno potwierdzać prawidłowość umocowania na dzień złożenia oferty lub oświadczenia, o którym mowa w art. 125 ust. 1 Ustawy pzp.
7. W przypadku Wykonawców ubiegających się wspólnie o udzielenie zamówienia do oferty należy załączyć pełnomocnictwo dla pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo do reprezentowania w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego.
8. Wykonawca składa ofertę za pośrednictwem Platformy **https://platformazakupowa.pl/pn/ug_szczytno.**
9. Sposób złożenia oferty został opisany w Regulaminie korzystania z platformy zakupowej.
10. Wszelkie informacje stanowiące **tajemnicę przedsiębiorstwa** w rozumieniu ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz.U. z 2019 r. poz. 1010 ze zm.), które Wykonawca

zastrzeże jako tajemnicę przedsiębiorstwa, powinny zostać przekazane w wydzielonym i odpowiednio oznaczonym pliku. Wykonawca zobowiązany jest wraz z przekazaniem informacji zastrzeżonych jako tajemnica przedsiębiorstwa wykazać spełnienie przesłanek określonych w art. 11 ust. 2 ustawy z 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji. Zastrzeżenie przez Wykonawcę tajemnicy przedsiębiorstwa bez uzasadnienia będzie traktowane przez Zamawiającego jako bezskuteczne, ze względu na zaniechanie przez Wykonawcę podjęcia, przy dołożeniu należytej staranności, działań w celu utrzymania poufności objętych klauzulą informacji zgodnie z art. 18 ust. 3 Ustawy pzp.

11. **Termin składania ofert upływa w dniu 30.06.2022 r., o godz. 11:00.** Decyduje data oraz dokładny czas (hh:mm:ss) generowany wg czasu lokalnego serwera synchronizowanego zegarem Głównego Urzędu Miar.

12. Oferta złożona po terminie zostanie odrzucona na podstawie art. 226 ust. 1 pkt 1 Ustawy pzp.

13. Wykonawca przed upływem terminu do składania ofert może **zmienić lub wycofać ofertę**. Zasady wycofania lub zmiany oferty określa *Instrukcja dla wykonawców* dostępna pod adresem: https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view.

14. Wykonawca nie może skutecznie wycofać oferty ani wprowadzić zmian w treści oferty po upływie terminu składania ofert.

XV. TERMIN OTWARCIA OFERT

1. **Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert, tj. w dniu 30.06.2022 roku o godz. 11:05.** Otwarcie ofert dokonywane jest przez odszyfrowanie i otwarcie ofert.

2. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania (Platformie) informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.

3. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania (platformie zakupowej).

4. Niezwłocznie po otwarciu ofert Zamawiający udostępni na stronie internetowej prowadzonego postępowania (platformie zakupowej) informacje o:

1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;

2) cenach lub kosztach zawartych w ofertach.

XVI. SPOSÓB OBLICZENIA CENY

1. Cena oferty stanowi wartość umowy za wykonanie przedmiotu zamówienia w całym zakresie.

2. Cenę oferty brutto za przedmiot zamówienia jest ceną ryczałtową, obejmującą koszt wykonania całego zakresu zamówienia opisanego w niniejszej SWZ i jej załącznikach.

3. Wykonawca, uwzględniając wszystkie wymogi, o których mowa w SWZ, zobowiązany jest w cenie brutto ująć wszelkie koszty niezbędne dla prawidłowego oraz pełnego wykonania przedmiotu zamówienia, zgodnie z warunkami wynikającymi z zamówienia.
4. Ceny wskazane przez Wykonawcę muszą być podane w PLN cyfrowo w zaokrągleniu do dwóch miejsc po przecinku (groszy). Zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę.
5. Rozliczenia pomiędzy Wykonawcą, a Zamawiającym będą dokonywane w złotych polskich (PLN).
6. Zamawiający do oceny oferty, której wybór prowadziłby do powstania obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, przyjmie cenę powiększoną o podatek VAT. Zamawiający jednocześnie informuje, że w przypadku, o którym mowa w zdaniu poprzedzającym wynagrodzenie Wykonawcy wynikające z umowy oraz ceny oferty brutto pomniejszone zostaną o wartość podatku od towarów i usług, którą Zamawiający miałby rozliczyć zgodnie z obowiązującymi przepisami.

XVII. OPIS KRYTERIÓW OCENY OFERT WRAZ Z PODANIEM WAG TYCH KRYTERIÓW I SPOSOBU OCENY OFERT

1. Przy wyborze oferty najkorzystniejszej zamawiający będzie kierował się następującymi kryteriami, z przypisaniem im odpowiednio wag:
   1) cena oferty – 60%
   2) termin realizacji – 40%
2. Sposób obliczania punktów dla poszczególnych kryteriów:
   1) **Punkty w kryterium cena brutto oferty w PLN** wyliczone będą z dokładnością do dwóch miejsc po przecinku (zasada zaokrąglania trzeciego miejsca po przecinku – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę) wg poniższego wzoru:

$$C = (Cmin : Cx) \times 100 \text{ pkt} \times 60\%$$

gdzie:

C – przyznane punkty w kryterium ceny oferty brutto w PLN;

Cmin - najniższa cena oferty brutto w PLN spośród ofert niepodlegających odrzuceniu;

Cx – cena brutto w PLN badanej oferty.

2) Punkty w kryterium **termin dostawy,** zostaną przyznane wg następujących zasad:

Termin dostawy – maksymalnie 40 pkt.

Punkty w kryterium termin dostawy zostaną przyznane zgodnie z poniższym wyszczególnieniem:

6 miesięcy, licząc od dnia podpisania umowy – 0 pkt.

4 miesiące, licząc od dnia podpisania umowy – 20 pkt.

3 miesiące i krócej, licząc od dnia podpisania umowy – 40 pkt.

Maksymalny termin dostawy wymagany przez Zamawiającego wynosi: 6 miesięcy liczone od dnia zawarcia umowy. W przypadku nie wskazania terminu dostawy w formularzu ofertowym Zamawiający uzna, że Wykonawca zobowiązuje się do dostawy w maksymalnym terminie dla poszczególnej części wymaganym przez Zamawiającego.
Oferty z terminem dostawy dłuższym niż maksymalny termin dostawy dla poszczególnej części zostaną odrzucone.
Podany przez Wykonawcę w formularzu ofertowym termin dostawy musi być podany w pełnych miesiącach.

3. Zamawiający za najkorzystniejszą uzna ofertę, która uzyska największą liczbę punktów łącznie ze wszystkich kryteriów. Ocenę łączną oferty stanowi suma punktów uzyskanych w ramach poszczególnych kryteriów. Zamawiający wyliczy ocenę łączą ocenianych ofert na podstawie poniższego wzoru:

E = C + T
gdzie:

E – łączna liczba punktów otrzymana przez ofertę we wszystkich kryteriach oceny,
C – liczba punktów w kryterium ceny oferty brutto w PLN,
T – liczba punktów w kryterium termin dostawy.

4. Zamawiający będzie zaokrąglał punkty do dwóch miejsc po przecinku w każdym wskaźniku. Zasada zaokrąglenia dotyczy trzeciego miejsca po przecinku – poniżej 5 końcówkę pominie, powyżej i równe 5 zaokrągli w górę.
5. Jeżeli nie można wybrać najkorzystniejszej oferty z uwagi na to, że dwie lub więcej ofert przedstawia taki sam bilans ceny i innych kryteriów oceny ofert, Zamawiający spośród tych ofert wybierze ofertę z najniższą ceną, a jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wezwie Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym ofert dodatkowych.

XVIII. INFORMACJE DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

1. Zamawiający będzie żądał od Wykonawcy, którego oferta zostanie wybrana jako najkorzystniejsza, wniesienia najpóźniej w dniu podpisania umowy zabezpieczenia należytego wykonania umowy w wysokości **5% ceny całkowitej podanej w ofercie**.
2. Zabezpieczenie może być wniesione, według wyboru Wykonawcy, w jednej lub w kilku następujących formach:

1) pieniądzu(zabezpieczenie należytego wykonania umowy wnoszone w pieniądzu należy przekazać przelewem na konto zamawiającego w Banku Spółdzielczym w Szczytnie nr 79 8838 0005 2001 0000 1661 0005);
2) poręczeniach bankowych lub poręczeniach spółdzielczej kasy oszczędnościowo-kredytowej, z tym że zobowiązanie kasy jest zawsze zobowiązaniem pieniężnym;
3) gwarancjach bankowych;
4) gwarancjach ubezpieczeniowych;
5) poręczeniach udzielanych przez podmioty, o których mowa w art. 6b ust. 5 pkt 2 ustawy z 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości.

3. Poręczenie lub gwarancja stanowiące formę zabezpieczenia należytego wykonania umowy winno zawierać stwierdzenie, że na pierwsze pisemne żądanie Zamawiającego wzywające do zapłaty kwoty z tytułu nienależytego wykonania umowy, zgodnie z warunkami umowy, następuje jego bezwarunkowa wypłata (bez jakichkolwiek zastrzeżeń gwaranta/poręczyciela w treści dokumentu w stosunku do Zamawiającego) do wysokości sumy gwarancyjnej. Jako Beneficjenta należy wpisać Gminę Szczytno**.**
4. Zamawiający dokona zwrotu zabezpieczenia należytego wykonania umowy w terminie 30 dni od dnia wykonania przedmiotu umowy i uznania przez Zamawiającego przedmiotu za należycie wykonany.

XIX. INFORMACJE O FORMALNOŚCIACH, JAKIE MUSZĄ ZOSTAĆ DOPEŁNIONE PO WYBORZE OFERTY W CELU ZAWARCIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO

1. Jeżeli zostanie wybrana oferta Wykonawców wspólnie ubiegających się o udzielenie zamówienia, Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych Wykonawców.
2. Zamawiający powiadomi wybranego Wykonawcę o terminie podpisania umowy w sprawie zamówienia publicznego.
3. W przypadku, gdy Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego lub nie wnosi wymaganego zabezpieczenia należytego wykonania umowy, zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.
4. Przed podpisaniem umowy wybrany Wykonawca przekaże Zamawiającemu informacje niezbędne do wpisania do treści umowy (np. imiona i nazwiska upoważnionych osób, które będą reprezentować Wykonawcę przy podpisaniu umowy).

5. Do zawarcia umowy w formie elektronicznej wymagane jest posiadanie kwalifikowanego podpisu elektronicznego.

XX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

Wykonawcy oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów Ustawy pzp, przysługują środki ochrony prawnej określone w dziale IX Ustawy pzp.

XXI. KLAUZULA INFORMACYJNA DOTYCZĄCA PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", informuję, że:

1) administratorem Pani/Pana danych osobowych jest *Gmina Szczytno, ul. Łomżyńska 3, 12-100 Szczytno; tel. (89) 62 32 580, e-mail: ugszczytno@ug.szczytno.pl*

2) inspektorem ochrony danych osobowych w Gminie Szczytno jest *Pan Kamil Maliszewski, kontakt: e-mail: iodo@ug.szczytno.pl, tel. (89) 62 32 583;*

3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z niniejszym postępowaniem o udzielenie zamówienia publicznego*;*

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 1 ustawy pzp;

5) Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 78 ustawy Pzp, przez okres co najmniej 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;

6) obowiązek podania przez Panią/Pana danych osobowych bezpośrednio Pani/Pana dotyczących jest wymogiem ustawowym określonym w przepisach ustawy Pzp, związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego; konsekwencje niepodania określonych danych wynikają z ustawy Pzp;

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

8) 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;

− 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 uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO;

9) 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.

XXII. PROJEKTOWANE POSTANOWIENIA UMOWY

UMOWA Nr …… (*projekt*)

zawarta w dniu …… r. w Szczytnie

pomiędzy:

Gminą Szczytno, z siedzibą w Szczytnie, ul. Łomżyńska 3, 12-100 Szczytno, NIP 745-181-12-30, reprezentowaną przez

Wójta Gminy Szczytno – Sławomira Wojciechowskiego

przy kontrasygnacie **Skarbnika Gminy Jolanty Godlewskiej**

zwaną „Zamawiającym”,

a ……..……..……z siedzibą w ……..., NIP: ….....; REGON: …..... ,reprezentowanym przez:

- .....

zwanym w dalszej treści umowy „Wykonawcą”,

§ 1

Przedmiot umowy

1. W wyniku wyboru oferty w postępowaniu o udzieleniu zamówienia publicznego prowadzonym w trybie podstawowym na podst. art. 275 pkt 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r., poz. 1129 z późn. zm.), zwanej dalej ustawą Zamawiający powierza, a Wykonawca zobowiązuje się zrealizować zamówienie pn.: ***Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”***
2. Przedmiot zamówienia obejmuje dostawę:

sprzętu sieciowego i serwerów:

- *serwer szt. 1*

- *serwer NAS – służący do archiwizacji i backupu szt. 1*

- *przełącznik zarządzalny szt. 1*

- *UPS – zasilacz awaryjny szt. 1*

- *Firewall UTM szt. 1*

- *Firewall UTM szt. 1*

- *38 komputerów stacjonarnych,*

o parametrach określonych w ***Załączniku Nr 1 do SWZ****.

3. **Na realizację przedmiotowego zamówienia Zamawiający otrzymał grant nr 4215/2022 w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020 Osi Priorytetowej V Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU działania 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowa Gmina”.**
4. Przedmiot dostawy musi być fabrycznie nowy, nieużywany, wolny od wad i kompletny tj. posiadający wszelkie akcesoria, przewody, kable niezbędne do ich użytkowania. Zaoferowany sprzęt musi być gotowy do użytkowania bez dodatkowych zakupów. Musi pochodzić z oficjalnych kanałów dystrybucyjnych producenta, zapewniających w szczególności realizację uprawnień gwarancyjnych. Cały asortyment składający się na przedmiot zamówienia powinien być nowy, nie noszący śladów uszkodzeń zewnętrznych i uprzedniego używania, tzn. że żadne urządzenie, produkt nie może być wcześniej używane, winien być sprawny, odpowiednio zapakowany, spełniać wszelkie wymogi norm określonych obowiązującym prawem.
5. Przedmiot umowy dostarczony zostanie Zamawiającemu z:
   1) kartą gwarancyjną
   2) instrukcją obsługi i dokumentacją techniczną w języku polskim
   3) dokumentem określającym zasady świadczenia usług przez autoryzowany serwis w okresie gwarancyjnym i pogwarancyjnym
   4) licencjami jak również wszelkimi prawami na dostarczone programy i systemy operacyjne, wystawionymi na rzecz Zamawiającego.

§ 2

Obowiązki stron

1. Wykonawca zobowiązuje się do prawidłowego wykonania przedmiotu Umowy, zgodnie z postanowieniami niniejszej umowy oraz Specyfikacją Warunków Zamówienia, zasadami wiedzy technicznej, zasadami należytej staranności oraz obowiązującymi normami i przepisami.

2. Przedmiot zamówienia, o którym mowa w §1 należy dostarczyć na adres: ul. Łomżyńska 3, 12-100 Szczytno.
3. O terminie dostawy Wykonawca zobowiązany jest zawiadomić Zamawiającego co najmniej z -2 dniowym wyprzedzeniem. Dostawa przedmiotu umowy nastąpi w godzinach 8:00-14:00.
4. Wykonawca zobowiązuje się dostarczyć przedmiot Zamówienia na własny koszt i ryzyko do miejsca wskazanego przez Zamawiającego.
5. Odbiór dostarczonego sprzętu nastąpi w formie protokołu, po uprzednim stwierdzeniu jego zgodności z warunkami zamówienia.
6. Zamawiający dokona sprawdzenia dostarczonego sprzętu. Jeżeli w trakcie sprawdzenia stwierdzona zostanie wada, Zamawiający może odmówić jego odbioru, a Wykonawca zobowiązany będzie do wymiany wadliwego przedmiotu umowy na wolny od wad. Przez wadę rozumie się w szczególności jakąkolwiek niezgodność dostarczonego sprzętu z opisem przedmiotu umowy stanowiącym **załącznik nr 1** do niniejszej umowy lub ofertą Wykonawcy stanowiącą **załącznik nr 2** do niniejszej umowy.
7. Jeżeli w toku czynności odbioru zostaną stwierdzone wady przedmiotu umowy lub brak wymaganych dokumentów, to Zamawiającemu przysługują następujące uprawnienia:

1) jeżeli wady nie nadają się do usunięcia to:

a) jeżeli umożliwiają one użytkowanie przedmiotu umowy zgodnie z przeznaczeniem, Zamawiający może odebrać przedmiot odbioru i obniżyć odpowiednio wynagrodzenie Wykonawcy,

b) jeżeli uniemożliwiają użytkowanie przedmiotu umowy zgodnie z przeznaczeniem, Zamawiający może odstąpić od umowy lub żądać wykonania przedmiotu umowy po raz drugi na koszt Wykonawcy,

2) jeżeli wady lub braki nadają się do usunięcia to zamawiający może:

a) odmówić odbioru do czasu usunięcia wad; w przypadku odmowy odbioru, zamawiający określa w protokole powód nie odebrania przedmiotu umowy i termin usunięcia wad lub

b) dokonać odbioru i wyznaczyć termin usunięcia wad zatrzymując odpowiednią do kosztów usunięcia wad część wynagrodzenia Wykonawcy tytułem kaucji gwarancyjnej.

8. Nie usunięcie wad w wyznaczonym terminie spowoduje zlecenie ich wykonania na rachunek i koszt Wykonawcy, na co Wykonawca wyraża zgodę. Wszelkie powstałe z tego tytułu koszty Zamawiający może pokryć z wynagrodzenia należnego Wykonawcy z tytułu realizacji niniejszej umowy na co Wykonawca wyraża zgodę.
9. Prawo własności przedmiotu umowy przechodzi na Zamawiającego z chwilą podpisania protokołu odbioru.
10. Dokonanie odbioru przedmiotu umowy nie wpływa na możliwość skorzystania przez zamawiającego z uprawnień przysługujących mu na mocy przepisów prawa lub umowy w przypadku nienależytego wykonania umowy, a w szczególności na prawo naliczenia kar umownych, dochodzenia odszkodowań oraz odstąpienia od umowy, jeżeli fakt nienależytego wykonania umowy zostanie ujawniony po dokonaniu odbioru.

11. Przez okres gwarancji serwis urządzeń będzie realizowany przez producenta lub autoryzowanego partnera serwisowego producenta.

§ 3

Termin realizacji umowy

Termin wykonania przedmiotu zamówienia: **…… miesięcy od dnia zawarcia umowy**.

§ 4

Podwykonawstwo

1. Wykonawca oświadcza, że przedmiot umowy wykona samodzielnie (własnymi siłami), za wyjątkiem części określonych w formularzu oferty stanowiącym załącznik nr 2 do umowy, które zamierza powierzyć podwykonawcom.
2. Poprzez umowę o podwykonawstwo należy rozumieć umowę w formie pisemnej o charakterze odpłatnym, zawartą między wykonawcą a podwykonawcą, a także między podwykonawcą a dalszym podwykonawcą lub między dalszymi podwykonawcami, na mocy której odpowiednio podwykonawca lub dalszy podwykonawca, zobowiązuje się wykonać część przedmiotu umowy.
3. Przed przystąpieniem do wykonania przedmiotu umowy wykonawca, o ile są już znane, zobowiązany jest przekazać Zamawiającemu nazwy, dane kontaktowe oraz przedstawicieli, podwykonawców zaangażowanych w realizację przedmiotu umowy. Wykonawca zawiadamia Zamawiającego o wszelkich zmianach w odniesieniu do informacji, o których mowa w zdaniu pierwszym, w trakcie realizacji umowy, a także przekazuje wymagane informacje na temat nowych podwykonawców, którym w późniejszym okresie zamierza powierzyć realizację części przedmiotu umowy.
4. Każdy podwykonawca nie może podlegać wykluczeniu na podstawie art. 108 ust. 1 ustawy Prawo zamówień publicznych. Jeżeli Zamawiający stwierdzi, że wobec danego podwykonawcy zachodzą podstawy wykluczenia, wykonawca obowiązany jest zastąpić tego podwykonawcę lub zrezygnować z powierzenia wykonania części zamówienia temu podwykonawcy.

§ 5

Wynagrodzenie i sposób rozliczeń

1. Strony ustalają, iż obowiązującą formą wynagrodzenia za wykonanie przedmiotu umowy jest wynagrodzenie ryczałtowe zgodnie z przedstawionym formularzem ofertowym.
2. Za wykonanie przedmiotu umowy Zamawiający zapłaci Wykonawcy wynagrodzenie w wysokości …… zł brutto (słownie: …….. złotych 00/100 złotych), w tym należny podatek VAT w kwocie …… (słownie: …….).
3. Rozliczenie za wykonanie przedmiotu zamówienia odbędzie się na podstawie faktury VAT wystawionej przez Wykonawcę.

4. Podstawą do wystawienia faktury VAT jest protokół odbioru przedmiotu zamówienia nie zawierający uwag, podpisany przez przedstawicieli Zamawiającego i Wykonawcy.
5. Faktura zostanie wystawiona na Gminę Szczytno, ul. Łomżyńska 3, 12-100 Szczytno, NIP 745-181-12-30.
6. Płatność za fakturę VAT, o której mowa w ust. 3 będzie dokonywana przelewem na konto wskazane na fakturze przez Wykonawcę w terminie do 21 dni licząc od daty otrzymania przez Zamawiającego prawidłowo wystawionej faktury i po spełnieniu warunków wyżej opisanych.
7. Wynagrodzenie uwzględnia wszystkie koszty, jakie poniesie Wykonawca z tytułu należytej i zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia, bez prawa odrębnego dochodzenia ich zwrotu.

§ 6

Kary umowne

1. Strony postanawiają, ze w przypadku niewykonania lub nienależytego wykonania postanowień niniejszej Umowy obowiązującą formą odszkodowania będą kary umowne.
2. Wykonawca zapłaci Zamawiającemu kary umowne:
   1) za odstąpienie od umowy z przyczyn leżących po stronie Wykonawcy - w wysokości 10% wynagrodzenia umownego brutto określonego w § 5 ust. 2 niniejszej umowy,
   2) za zwłokę w dostarczeniu przedmiotu umowy w wysokości 0,05 % wynagrodzenia umownego brutto określonego w § 5 ust. 2 niniejszej umowy za każdy dzień zwłoki, licząc od umownego terminu realizacji umowy.
3. Zamawiający zapłaci Wykonawcy karę umowną za odstąpienie od umowy z przyczyn leżących po stronie Zamawiającego w wysokości 10% wynagrodzenia umownego brutto określonego w § 5 ust 2 niniejszej umowy, za wyjątkiem wystąpienia sytuacji przedstawionej w art. 456 ust. 1 pkt.1 ustawy Prawo zamówień publicznych.
4. Łączna wysokość kar umownych, których mogą dochodzić strony nie może przekroczyć 20% wartości umowy brutto, o której mowa w § 5 ust 2 niniejszej umowy.
5. Termin zapłaty kary umownej wynosi 14 dni od dnia doręczenia wezwania.
6. Wykonawca wyraża zgodę na potrącenia naliczonych kar z przysługującego mu wynagrodzenia.
7. Zapłata kary przez Wykonawcę lub potracenie przez Zamawiającego kwoty kary z płatności należnej Wykonawcy nie zwalnia Wykonawcy z obowiązku wykonania zobowiązań wynikających z umowy.
8. Stronom przysługuje prawo do odszkodowania uzupełniającego na zasadach ogólnych, przewidzianych w Kodeksie cywilnym.

§ 7

Zabezpieczenie należytego wykonania umowy

1. Przed zawarciem Umowy Wykonawca złoży Zamawiającemu zabezpieczenie należytego wykonania umowy w wysokości 5 % ceny całkowitej brutto podanej w ofercie tj. …… zł (słownie: …….. zł) zgodnie z art. 452 ust. 2 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.).
2. Zabezpieczenie służy pokryciu roszczeń z tytułu niewykonania lub nienależytego wykonania postanowień Umowy.
3. Zamawiający zwróci Wykonawcy zabezpieczenie w terminie 30 dni od dnia wykonania przedmiotu Umowy i uznania przez Zamawiającego przedmiotu umowy za należycie wykonany.
4. Koszty ustanowienia zabezpieczenia ponosi Wykonawca.
5. Zamawiający zastrzega sobie prawo do potrącania z wniesionego zabezpieczenia należytego wykonania umowy ewentualnych roszczeń w stosunku do Wykonawcy z tytułu nienależytego wykonania Umowy oraz kar umownych.
6. Zabezpieczenie należytego wykonania umowy zostało wniesione w formie …….

§ 8

Uprawnionymi do kontaktów i osobami odpowiedzialnymi za przebieg oraz realizację umowy są:

1) z ramienia Zamawiającego: ……,
2) z ramienia Wykonawcy: ……..

§ 9

Gwarancja i rękojmia

1. Wykonawca udziela gwarancji, że przedmiot dostawy jest fabrycznie nowy i wolny od wad, oraz że może być użytkowany zgodnie z przeznaczeniem.
2. Okres gwarancji przedmiotu zamówienia został określony w załączniku nr 1 do SWZ stanowiącym załącznik do oferty Wykonawcy i liczony będzie od dnia protokolarnego odbioru przedmiotu zamówienia.
3. Wykonawca zobowiązuje się do bezpłatnego wykonania naprawy gwarancyjnej przedmiotu umowy nie później niż w ciągu 3 dni od momentu zgłoszenia usterki.
4. W przypadku naprawy komputerów przenośnych, okres gwarancji ulegnie przedłużeniu o okres wykonywania naprawy; natomiast w przypadku dokonania wymiany komputerów przenośnych okres gwarancji zostanie ustalony zgodnie z gwarancją nowego sprzętu.
5. Odpowiedzialność z tytułu gwarancji jakości obejmuje zarówno wady powstałe z przyczyn tkwiących w wyposażeniu objętym przedmiotem umowy w chwili dokonania jego odbioru przez Zamawiającego, jak i wszelkie inne wady fizyczne powstałe z przyczyn, za które Wykonawca lub inny gwarant ponosi odpowiedzialność, pod warunkiem, że wady te ujawnią się w okresie obowiązywania gwarancji.
6. Jeżeli w terminie, o którym mowa w § 9 ust. 2 ujawnią się takie wady fizyczne przedmiotu umowy, które nie kwalifikują się do ich usunięcia, bądź jeżeli przedmiot umowy był naprawiany co najmniej 2 –

krotnie, Wykonawca zobowiązuje się do dostarczenia przedmiotu umowy wolnego od wad o parametrach nie gorszych lub lepszych. W przypadku ziszczenia się obowiązku wymiany przedmiotu umowy na nowy, Wykonawca zobowiązuje się do tego w terminie 3 dni roboczych od momentu powstania obowiązku wymiany.

7. W przypadku niedotrzymania terminu naprawy gwarancyjnej, bądź niedotrzymania terminu wymiany przedmiotu zamówienia na wolny od wad, Zamawiający jest uprawniony do usunięcia wad w drodze naprawy na ryzyko i koszt Wykonawcy, zachowując przy tym inne uprawnienia przysługujące mu na podstawie Umowy, a w szczególności roszczenia z tytułu rękojmi za wady fizyczne lub Zamawiający będzie naliczał karę umowną w wysokości 100,00 zł za każdy dzień zwłoki.
8. Szczegółowe warunki gwarancji określi dokument gwarancyjny wystawiony przez Wykonawcę. Postanowienia dokumentu gwarancyjnego sprzeczne z odpowiednimi postanowieniami zawartymi w niniejszej umowie są nieważne, w ich miejsce zastosowanie znajdują odpowiednie postanowienia niniejszej umowy. Nie dotyczy to postanowień korzystniejszych dla Zamawiającego, a zwłaszcza wydłużenia terminów określonych w § 9 ust. 2 umowy.
9. Wykonawca jest odpowiedzialny względem Zamawiającego za wszelkie wady prawne przedmiotu umowy, w tym również za ewentualne roszczenia.

§ 10

Postanowienia końcowe

1. Zmiana postanowień zawartej umowy może nastąpić za zgodą obu stron wyrażoną na piśmie w postaci kolejnych aneksów, pod rygorem nieważności takiej zmiany.
2. Zamawiający na mocy art. 455 ust. 1 pkt 1 ustawy PZP dopuszcza możliwość zmiany zawartej umowy w zakresie:

   1) Zmiany terminu realizacji zamówienia:

   a) wydłużenie terminu realizacji zamówienia w przypadku działania siły wyższej (należy przez nią rozumieć wystąpienie zdarzeń i okoliczności, na które strony nie mają wpływu i przed którymi nie mogły się zabezpieczyć, w tym w szczególności pożaru, zalania, wojny, zamieszek, innych klęsk żywiołowych) mającej bezpośredni wpływ na terminowość realizacji zamówienia, które uniemożliwiły wykonanie Umowy w dotychczas ustalonym terminie.

   b) wydłużenie terminu realizacji zamówienia w przypadku konieczności zmiany oferowanego produktu na inny w przypadku wystąpienia okoliczności o których mowa w § 10 ust. 2 pkt. 2 ppkt. a) i b).

   – termin wykonania Umowy może ulec zmianie o czas, o jaki wyżej wskazane okoliczności wpłynęły na termin wykonania Umowy przez Wykonawcę, to jest uniemożliwiły Wykonawcy terminową realizację przedmiotu Umowy.

   2) oferowanego produktu na inny o parametrach nie gorszych niż zaoferowane przez Wykonawcę w ofercie i spełniających wymagania zawarte w SWZ (spełniające minimalne parametry zastępowanego przedmiotu zamówienia) w sytuacji, gdy:

a) Wykonawca wykaże, że zaproponowane przez niego w ofercie produkty nie są dostępne na rynku w wyniku zakończenia ich produkcji lub wycofania ze sprzedaży.

b) Wykonawca wykaże, że zaproponowane przez niego w ofercie produkty nie są dostępne na rynku w wymaganej ilości do zrealizowania zamówienia, co w istotny sposób wpływa na możliwość wykonania przez Wykonawcę Umowy, przede wszystkim dostawa przedmiotu zamówienia może nie zostać wykonana w umówionym terminie.

3) Zmian regulacji prawnych obowiązujących w dniu podpisania umowy.

4) W innych przypadkach, określonych w art. 455 ustawy PZP.

2. Treść niniejszej umowy nie podlega negocjacjom i zawiera wszelkie istotne dla Zamawiającego warunki realizacji umowy.

3. Zamawiającemu przysługuje prawo odstąpienia od Umowy w następujących przypadkach:

1) w razie zaistnienia co najmniej jednej z przesłanek odstąpienia od umowy, o których mowa w art. 456 ust. 1 ustawy,

2) gdy zostanie wydany nakaz zajęcia majątku Wykonawcy odstąpienie od Umowy w tym przypadku może nastąpić w terminie 30 dni od powzięcia wiadomości o powyższych okolicznościach.

4. W sprawach nieuregulowanych postanowieniami Umowy zastosowanie mają przepisy Kodeksu cywilnego.

5. Wszelkie spory wynikające z niniejszej umowy rozstrzygać będzie Sąd właściwy dla Zamawiającego.

6. Integralną część umowy stanowią załączniki do umowy:

1) Załącznik Nr 1 – Opis przedmiotu zamówienia,

2) Załącznik Nr 2 – Oferta Wykonawcy.

7. Umowę niniejszą sporządzono w wersji elektronicznej.

WYKONAWCA: **ZAMAWIAJĄCY:**

Wykaz załączników do SWZ:

1. Szczegółowy opis przedmiotu zamówienia
2. Wzór – formularz oferty (obowiązkowy)
3. Wzór – oświadczenie dot. przesłanek wykluczenia z postępowania (obowiązkowy)
4. Wzór – oświadczenie dot. spełniania warunków udziału w postępowaniu (obowiązkowy)
5. Wzór – zobowiązanie podmiotu (obowiązkowy – jeśli dotyczy)
6. Wzór – wykaz dostaw (na wezwanie Zamawiającego)

Wójt Gminy Szczytno

Sławomir Wojciechowski

Szczytno, 22.06.2022 r.

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.

Załącznik nr 1 do SWZ

Dostawa sprzętu sieciowego i serwerów

1. Parametry serwera (opis)

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)**
Obudowa	Obudowa RACK o wysokości maksymalnie 1U z możliwością instalacji minimum 4 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora lub więcej. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych	
Procesor	Jeden procesor 8-rdzeniowy, min. 2.6GHz częstotliwości bazowej/nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej: SPECrate2017_int_base wynik min. 60pkt SPECrate2017_int_peak wynik min. 63pkt SPECrate2017_fp_base wynik min. 52pkt SPECrate2017_fp_peak wynik min. 56pkt Maksymalny TDP dla procesora 65W Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty. Do oferty należy załączyć wyniki testów	
Pamięć RAM	Minimum 32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s w układzie 2x16GB Płyta powinna obsługiwać do minimum 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci.	
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200	
Wbudowane porty	Minimum. 3 porty USB Minimum 1 port VGA i 1 port RS232	
Gniazda PCI	Minimum 2 sloty PCIe	
Interfejsy sieciowe LAN	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT	
Kontroler dysków	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50	
Dyski twarde	W chwili dostawy możliwość instalacji dysków SAS, SATA, SSD, NL-SAS Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1 pod virtualizator Zainstalowane 4 dyski SSD o minimalnych parametrach 480GB SATA 6Gb/s Read Intensive DWPD min.1 typu Hot Plug pod konfigurację Raid5 Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde	
Wentylatory	Minimum 4 wentylatory	
Zasilacze	szt. 2 Redundantne, o mocy minimalnej 600W.	
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0	

Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 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 Server 2019, Windows Server 2022.	
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.	
Warunki gwarancji	24 miesięcy gwarancji, z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzony dysk pozostaje u Zamawiającego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego autoryzowanego przedstawiciela.	

2. Serwer NAS – służący do archiwizacji i backupu

Cecha	**Wymagania minimalne**	**Parametry oferowane (w każdym wierszu należy określić typ/model/ producent/ nr katalogowy)**
Specyfikacja sprzętowa		
Procesor	Procesor 64 bit Intel x86 o taktowaniu nie mniejszym niż 2.0 GHz	
Procesor liczba rdzeni	Nie mniej niż 4	
Pamięć RAM	Nie mniej niż 4GB DDR4	

Pamieć RAM liczba slotów	Minimum 4 sloty	
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 16GB	
Pamięć Flash	Nie mniej niż 4GB	
Liczba zatok na dyski twarde	Minimum 4	
Obsugiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD	
Pojemność dysków twardych	Minimum do 8TB (minimum 4 dyski)	
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2	
Porty LAN 2,5 GbE	Minimum 2	
Diody LED	Minimum Status, LAN, HDD,	
Porty USB 3.2 Gen 1	Minimum 2	
Porty USB 2.0	Minimum 2	
Port PCiE	Tak, minimum 1 Gen3	
Przyciski	Reset, Zasilanie	
Typ obudowy	RACK, 1U	
Dopuszczalna temperatura pracy	od 0 do 40˚C	
Wilgotność względna podczas pracy	5-95% R.H.	
Zasilanie	Zasilacz redundatny 2 x 250 W, 100-240 V	
Szyny rackowe	Tak, w zestawie	
Specyfikacja oprogramowania		
Agregacja łączy	Tak	
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+	
Możliwość podłączenia karty WLAN na USB	Tak	
Szyfrowanie wolumenów	Tak, min AES 256	
Szyfrowanie dysków zewnętrznych	Tak	
Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek	

Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN	
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla pod folderów, Windows ACL	
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP	
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,	
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box	
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android	
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu	
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN	
Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu	
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.	

Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker	
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS	
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek	
Dyski twarde	Macierz zostanie wyposażona w 4 dyski twarde 3.5” SATA 6Gb/s przystosowane do pracy z urządzeniami NAS (zapis ciągły 24/7) o pojemności min. 8 TB, prędkości 7200obr./min. Cache min. 256 MB. Dodatkowo dyski powinny posiadać parametr MTBF min. 2 mln godz. Wymaga się, aby dyski znajdowały się na liście kompatybilności dostarczanego urządzenia NAS zapewniając kompatybilność oraz wydajność.	
Gwarancja	2 lata na urządzenie 2 lat gwarancji na dyski.	

3. Przełącznik zarządzalny

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry techniczne oferowanego urządzenia
1	**2**	**3**	**4**
1.	Typ	Przełącznik sieciowy Ethernet Smart Management rack 1Gbit. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.	…… …… */wpisać model, symbol, producenta urządzenia/*
2.	Porty	a) Minimum 48 porty 1G RJ45 10/100/1000BASE-T b) Minimum 4 porty SFP+ z możliwością pracy 1G/10G Porty SFP+ muszą być obsadzone wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX	…… …… */wskazać ilość portów dla pkt a i b/*
3.	Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19’’	
4.	Pamięć	Co najmniej 512 MB SDRAM Co najmniej 256 MB pamięci flash Bufor pakietów co najmniej 1.5 MB CPU ARM Cortex-A9 @ 800 MHz	…… …… */wskazać wielkość pamięci DRAM i flash/*
5.	Wielkość tablicy adresów MAC	Co najmniej 16000	…… …… */wypełnić/*
6.	Ilość obsługiwanych sieci VLAN	Co najmniej 256	…… …… */wypełnić/*

7.	Wydajność	• Przepustowość przełączania: min. 176 Gbit/s • Przełączanie dla pakietów: min. 130 Mpps. • Opóźnienie: < 4.5 uSec dla 100 Mb < 2.2 uSec dla 1000 Mb <1.2 uSec dla 10 Gbps	…… …… */wypełnić/*
8.	Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów	
9.	Funkcjonalność urządzenia	• obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), • obsługa protokołu SNTP, • Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s) • Minimum 256 obsługiwanych sieci VLAN • Automatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED. • Minimum 50 możliwych do utworzenia list ACL, • CoS zgodna z 802.1p • Voice VLAN • Minimum 509 wpisów ARP • Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy • Port Security • DHCP Snooping • Klient Radius • Port mirroring, • DHCP Relay, • DoS Protection, • ARP Attack Protection, • Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu	
10.	Zasilanie	Zasilacz 230V AC wbudowany,	
11.	Temperatura pracy	0°C do 40°C	
12.	Zarządzanie	WWW (GUI), SNMP Manager, cloud-based web portal	
13.	Gwarancja	2 lata	

4. UPS – zasilacz awaryjny

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry techniczne oferowanego urządzenia
1	**2**	**3**	**4**
1.	Typ	Bezprzerwowy zasilacz UPS	…… */wpisać model, symbol, producenta urządzenia/*
2.	moc	3000 VA / 3000 W	…… */wskazać /*
3.	Ilość Faz	1 + G	
4.	Zakres napięcia	10 VAC - 300 VAC ± 5 % (w zależności od obciążenia)	…… */wskazać/*
5.	Sprawność całkowita	90 %	…… */wypełnić/*
6.	Obudowa	RACK maksymalnie 3 U	…… */wypełnić/*

7.	Czas podtrzymania	Minimum 8 minut przy obciążeniu 50% oraz 5 minut przy obciążeniu 100%	…… */wypełnić/*
8.	komunikacja	Port komunikacyjny RS232 i USB	
9.	Zarządzanie	Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną: Windows Server 2012 Micorosft Hyper-V 2012 Windows Server 2008 Micorosft Hyper-V 2012 Windows Server 2003 Windows 8 WMware ESXi VMware ESX Red Hat Enterprise Linux Ubuntu Linux SuSE Linux Enterprise Server	
10.	Akcesoria	Szyny montażowe do szafy rack	
11.	Gwarancja	2 lata	

Dostawa zapory sieciowej firewall

5. Firewall UTM (dla Gminy) szt. 1

Cecha	Wymagania minimalne	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
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 dostawca 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 3 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.	
Interfejsy, Dysk, Zasilanie:	1. System realizujący funkcję Firewall musi dysponować minimum 4 portami Gigabit Ethernet RJ-45. 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 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 2. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 3. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 4. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 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 1,0 Gbps. 6. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 7. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 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.	

Polityki, Firewall	1. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 2. 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. 3. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 4. 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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
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	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	

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.	
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.	
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 Firewall 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.	
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola 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 **5 lat**	
Gwarancja oraz wsparcie	1. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

6. Firewall UTM (dla GOPS) szt. 1

Cecha	Wymagania minimalne	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
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 dostawca 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 3 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	4. 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. 5. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 6. Monitoring stanu realizowanych połączeń VPN.	
Interfejsy, Dysk, Zasilanie:	5. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 6. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 7. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 8. System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe:	8. W zakresie Firewall'a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 9. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 10. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 11. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. 12. 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 1,0 Gbps. 13. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 14. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 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: 12. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 13. Kontrola Aplikacji. 14. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 15. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 16. Ochrona przed atakami - Intrusion Prevention System. 17. Kontrola stron WWW. 18. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 19. Zarządzanie pasmem (QoS, Traffic shaping). 20. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 21. 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. 22. Analiza ruchu szyfrowanego protokołem SSL.	

Polityki, Firewall	5. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 6. 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. 7. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 8. 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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
Połączenia VPN	3. 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. 4. 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	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	

Ochrona przed malware	6. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 7. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 8. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 9. 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. 10. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Ochrona przed atakami	8. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 9. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 10. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 11. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 12. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 13. 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. 14. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Kontrola aplikacji	7. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 8. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 9. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 10. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 11. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
Kontrola WWW	8. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 9. 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. 10. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 11. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 12. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 13. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 14. 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	4. 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. 5. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 6. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
Zarządzanie	2. 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. 3. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 4. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 5. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 6. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 7. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 8. 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	12. 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. 13. 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. 14. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 15. Musi istnieć możliwość logowania do serwera SYSLOG.	
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola 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 **5 lat**	
Gwarancja oraz wsparcie	9. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Dostawa komputerów stacjonarnych

7. Parametry komputera stacjonarnego (opis)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja graficzna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.	
2.	Obudowa	Typu mini / midi tower z obsługą kart PCI Express. Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napedów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy. Wyposażona w czytnik kart multimedialnych Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym Wyposażona w budowany głośnik o mocy min. 2W	
3.	Zasilacz	Zasilacz minimalnie 500W o sprawności minimum 85%	
4.	Chipset	Dostosowany do zaoferowanego procesora	
5.	Płyta główna	Wyposażona w złącza min.: 1) 1 x PCI Express 3.0 x16, 2) 1 x PCI Express 3.0 x1, 3) 1 x M.2	
6.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi AMD Ryzen 5 5600G na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na	

		http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
7.	Pamięć operacyjna	Min. 16GB DDR4 3200MHz z możliwością rozszerzenia do 32 GB	
8.	Dysk twardy	Min 256GB SSD M.2 PCIe NVMe zawierający recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
9.	Napęd optyczny	Nagrywarka DVD +/-RW	
10.	Karta graficzna	dedykowana karta graficzna wyposażona w minimum 6 GB RAM, Szyna danych 192 bit Taktowanie pamięci minimum 15000 MHz, taktowanie rdzenia minimum 1777 Rodzaj pamięci RAM GDDR6	
11.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
12.	Karta sieciowa	LAN 10/100/1000 Mbit/s z funkją PXE oraz Wake on LAN WiFi 802.11ac 1x1 + BT 5.0	
13.	Porty/złącza	Wbudowane porty/złącza: 1) 1 x VGA, 2) 1 x HDMI, 3) 8 x USB w tym min. 4 x USB3.1 4) port sieciowy RJ-45, 5) porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy 6) czytnik kart pamięci min. SD Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
14.	Monitor	Matryca 24” z podświetleniem w technologii LED, Kąt widzenia (stopnie): 178 (pion), 178 (poziom)Czas reakcji: 4 ms Kontrast: 3000:1 Rodzaj matrycy: VA	
15.	Klawiatura/mysz	Klawiatura przewodowa w układzie US Mysz przewodowa (scroll)	
16.	System operacyjny	Microsoft Windows 10 64 bit lub Windows 11 64 bit lub równoważny system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 1) Dostępne dwa rodzaje graficznego interfejsu użytkownika: a) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, b) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 2) Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 3) Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 4) Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 5) Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 6) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 7) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 8) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 9) Wbudowany system pomocy w języku polskim. 10) Możliwość przystosowania stanowiska dla osób	

		niepełnosprawnych (np. słabo widzących). 11) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 12) Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 13) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 14) Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 15) Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 16) Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 17) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 18) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 19) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 20) Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 21) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 22) Wbudowany mechanizm wirtualizacji typu hypervisor." 23) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 24) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 25) Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 26) Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 27) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 28) Możliwość tworzenia wirtualnych kart inteligentnych. 29) Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (SecureBoot) 30) Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 31) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 32) Mechanizmy logowania w oparciu o: a) Login i hasło, b) Karty inteligentne i certyfikaty (smartcard), c) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), d) Certyfikat/Klucz i PIN e) Certyfikat/Klucz i uwierzytelnienie biometryczne 33) Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 34) Wbudowany agent do zbierania danych na temat zagrożeń na	

		stacji roboczej. 35) Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 36) Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 37) Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished.	
17.	BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: 1) modelu komputera, PN 2) numerze seryjnym, 3) AssetTag, 4) MAC Adres karty sieciowej, 5) wersja Biosu wraz z datą produkcji, 6) zainstalowanym procesorze, jego taktowaniu i ilości rdzeni 7) ilości pamięci RAM wraz z taktowaniem, 8) stanie pracy wentylatora na procesorze 9) napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) Możliwość z poziomu Bios: 1) wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy 2) wyłączenia selektywnego (pojedynczego) portów SATA, 3) wyłączenia karty sieciowej, karty audio, portu szeregowego, 4) możliwość ustawienia portów USB w jednym z dwóch trybów: a) użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB b) użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej 5) ustawienia hasła: administratora, Power-On, HDD, 6) blokady aktualizacji BIOS bez podania hasła administratora 7) załadowania optymalnych ustawień Bios 8) obsługa Bios za pomocą klawiatury i myszy	
19.	Certyfikaty i standardy	1) Deklaracja zgodności CE (załączyć do oferty)	
20.	Bezpieczeństwo i zdalne zarządzanie	1) Czujnik otwarcia obudowy	
21.	Gwarancja	*2 lata*	

Załącznik nr 2 do SWZ

(obowiązkowy)

FORMULARZ OFERTOWY

Nazwa Wykonawcy: .....

Adres Wykonawcy: .....

NIP: ..... **REGON:**.....

Nr telefonu .....

Adres e-mail: .....
(na który Zamawiający będzie przesyłać korespondencję)

Adres skrzynki ePUAP: .....

Gmina Szczytno
ul. Łomżyńska 3
12-100 SZCZYTNO

Nawiązując do ogłoszenia o zamówieniu po zapoznaniu się z warunkami prowadzonego postępowania w trybie podstawowym na podstawie art. 275 ust. 1 ustawy Prawo zamówień publicznych składamy ofertę na realizację zadania pn.:

Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”

1. Oświadczamy, że Wykonamy dostawę **za cenę brutto** ..... **zł**

   słownie złotych: .....,

   w tym należny **podatek VAT w kwocie …….. zł (słownie: ……)** wynikającą z następującego wyliczenia:

Lp.	Nazwa asortymentu	J.m.	Ilość	Cena jednostkowa brutto
1	Serwer aplikacyjny	szt.	1	
2	Serwer NAS – służący do archiwizacji i backupu	szt.	1	
3	Przełącznik zarządzalny	Szt.	1	
4	UPS – zasilacz awaryjny	Szt.	1	
5	Firewall UTM (Gmina)	Szt.	1	
6	Firewall UTM (GOPS)	Szt.	1	

7	Komputer stacjonarny	szt.	38	
Razem wartość brutto				

(wypełnić zgodnie z wymaganiami zamawiającego: tj. w kolumnie „Parametry oferowane" w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy oferowanego komponentu).

Dostawa sprzętu sieciowego i serwerów

1. **Parametry serwera (opis)**

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)**
Obudowa	Obudowa RACK o wysokości maksymalnie 1U z możliwością instalacji minimum 4 dysków 2,5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych	
Płyta główna	Płyta główna z możliwością zainstalowania jednego procesora lub więcej. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym.	
Chipset	Dedykowany przez producenta procesora do pracy w serwerach jednoprocesorowych	
Procesor	Jeden procesor 8-rdzeniowy, min. 2.6GHz częstotliwości bazowej/nominalnej, osiągający minimalne wyniki testów w konfiguracji jednoprocesorowej: SPECrate2017_int_base wynik min. 60pkt SPECrate2017_int_peak wynik min. 63pkt SPECrate2017_fp_base wynik min. 52pkt SPECrate2017_fp_peak wynik min. 56pkt Maksymalny TDP dla procesora 65W Wynik testu musi być opublikowany na stronie https://www.spec.org/cpu2017/results/ w dniu złożenia oferty. Do oferty należy załączyć wyniki testów	
Pamięć RAM	Minimum 32GB pamięci RAM ECC UDIMM o częstotliwości pracy 3200MT/s w układzie 2x16GB Płyta powinna obsługiwać do minimum 128GB, na płycie głównej powinno znajdować się minimum 4 sloty przeznaczone dla pamięci.	
Karta graficzna	Zintegrowana karta graficzna umożliwiająca rozdzielczość min. 1920x1200	
Wbudowane porty	Minimum. 3 porty USB Minimum 1 port VGA i 1 port RS232	
Gniazda PCI	Minimum 2 sloty PCIe	
Interfejsy sieciowe LAN	Wbudowane minimum 2 interfejsy sieciowe 1Gb Ethernet w standardzie BaseT	
Kontroler dysków	Sprzętowy kontroler dyskowy posiadający min. 8GB nieulotnej pamięci cache, umożliwiający konfigurację poziomów RAID: 0, 1, 5, 6, 10, 50	
Dyski twarde	W chwili dostawy możliwość instalacji dysków SAS, SATA, SSD, NL-SAS Zainstalowane 2 dyski M.2 SATA o pojemności min. 240GB Hot-Plug w konfiguracji RAID 1 pod virtualizator Zainstalowane 4 dyski SSD o minimalnych parametrach 480GB SATA 6Gb/s Read Intensive DWPD min.1 typu Hot Plug pod konfigurację Raid5 Możliwość zainstalowania dedykowanego modułu dla hypervisora wirtualizacyjnego, wyposażony w 2 nośniki typu flash o pojemności min. 64GB, z możliwością konfiguracji zabezpieczenia synchronizacji pomiędzy nośnikami z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde	

Wentylatory	Minimum 4 wentylatory	
Zasilacze	szt. 2 Redundantne, o mocy minimalnej 600W.	
Bezpieczeństwo	Zatrzask górnej pokrywy oraz blokada na ramce panela frontowego zamykane na klucz w celu do ochrony nieautoryzowanego dostępu do dysków twardych i wewnętrznych elementów serwera. Możliwość wyłączenia w BIOS funkcji przycisku zasilania. BIOS ma możliwość przejścia do bezpiecznego trybu rozruchowego z możliwością zarządzania blokadą zasilania, panelem sterowania oraz zmianą hasła Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. Moduł TPM 2.0	
Karta Zarządzania	Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca: • zdalny dostęp do graficznego interfejsu Web karty zarządzającej; • zdalne monitorowanie i informowanie o statusie serwera (np. prędkości obrotowej wentylatorów, konfiguracji serwera); • szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika; • możliwość podmontowania zdalnych wirtualnych napędów; • wirtualną konsolę z dostępem do myszy, klawiatury; • wsparcie dla IPv6; • wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish; • możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer; • możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer; • integracja z Active Directory; • możliwość obsługi przez dwóch administratorów jednocześnie; • wsparcie dla dynamic DNS; • wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej. • możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera • możliwość zarządzania do 100 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera	
Certyfikaty	Serwer musi być wyprodukowany zgodnie z normą ISO-9001 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 Server 2019, Windows Server 2022.	
Dokumentacja	Zamawiający wymaga dokumentacji w języku polskim lub angielskim.	
Warunki gwarancji	24 miesięcy gwarancji, z czasem reakcji serwisu do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii 24x7x365 poprzez ogólnopolską linię telefoniczną producenta. Uszkodzony dysk pozostaje u Zamawiającego. Zamawiający wymaga od podmiotu realizującego serwis lub producenta sprzętu dołączenia do oferty oświadczenia, że w przypadku wystąpienia awarii dysku twardego w urządzeniu objętym aktywnym wparciem technicznym, uszkodzony dysk twardy pozostaje u Zamawiającego. Firma serwisująca musi posiadać ISO 9001:2008 na świadczenie usług serwisowych oraz posiadać autoryzacje producenta urządzeń – dokumenty potwierdzające należy załączyć do oferty. Wymagane dołączenie do oferty oświadczenia Producenta potwierdzając, że Serwis urządzeń będzie realizowany bezpośrednio przez Producenta i/lub we współpracy z Autoryzowanym Partnerem Serwisowym Producenta. Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego autoryzowanego przedstawiciela.	

2. Serwer NAS – służący do archiwizacji i backupu

Cecha	Wymagania minimalne	Parametry oferowane (w każdym wierszu należy określić typ/model/ producent/ nr katalogowy)
Specyfikacja sprzętowa		
Procesor	Procesor 64 bit Intel x86 o taktowaniu nie mniejszym niż 2.0 GHz	
Procesor liczba rdzeni	Nie mniej niż 4	
Pamięć RAM	Nie mniej niż 4GB DDR4	
Pamieć RAM liczba slotów	Minimum 4 sloty	
Pamięć RAM - możliwość rozszerzenia	Nie mniej niż do 16GB	
Pamięć Flash	Nie mniej niż 4GB	
Liczba zatok na dyski twarde	Minimum 4	
Obsugiwane dyski twarde	3.5" oraz 2.5" SATA oraz 2.5" SATA SSD	
Pojemność dysków twardych	Minimum do 8TB (minimum 4 dyski)	
Możliwość podłączenia modułu rozszerzającego	Tak, co najmniej 2	
Porty LAN 2,5 GbE	Minimum 2	
Diody LED	Minimum Status, LAN, HDD,	
Porty USB 3.2 Gen 1	Minimum 2	
Porty USB 2.0	Minimum 2	
Port PCiE	Tak, minimum 1 Gen3	
Przyciski	Reset, Zasilanie	
Typ obudowy	RACK, 1U	
Dopuszczalna temperatura pracy	od 0 do 40˚C	
Wilgotność względna podczas pracy	5-95% R.H.	
Zasilanie	Zasilacz redundatny 2 x 250 W, 100-240 V	
Szyny rackowe	Tak, w zestawie	
Specyfikacja oprogramowania		
Agregacja łączy	Tak	
Obsługiwane systemy plików	Dyski wewnętrzne: EXT4 Dyski zewnętrzne: EXT3, EXT4, NTFS, FAT32, HFS+	
Możliwość podłączenia karty WLAN na USB	Tak	
Szyfrowanie wolumenów	Tak, min AES 256	
Szyfrowanie dysków zewnętrznych	Tak	

Zarządzanie dyskami	Pojedynczy Dysk, 0, 1, 5, 6, 10, JBOD, Obsługa Hot Spare per grupa RAID oraz global hot spare Rozszerzanie pojemności Online RAID Migracja poziomów Online RAID HDD S.M.A.R.T. Skanowanie uszkodzonych bloków (pliku) Przywracanie macierzy RAID Obsługa map bitowych Pula pamięci masowej Obsługa migawek Obsługa replikacji migawek	
Wbudowana obsługa iSCSI	Multi-LUNs na Target Obsługa LUN Mapping & Masking Obsługa SPC-3 Persistent Reservation Obsługa MPIO & MC/S, Migawka / kopia zapasowa iSCSI LUN	
Zarządzanie prawami dostępu	Ograniczenie dostępnej pojemności dysku dla użytkownika Importowanie listy użytkowników Zarządzanie kontami użytkowników Zarządzanie grupą użytkowników Zarządzanie współdzieleniem w sieci Tworzenie użytkowników za pomocą makr Obsługa zaawansowanych uprawnień dla pod folderów, Windows ACL	
Obsługa Windows AD	Logowanie użytkowników poprzez CIFS/SMB, AFP, FTP oraz menadżera plików sieci Web Funkcja serwera LDAP	
Funkcje backup	Oprogramowanie do tworzenia kopii bezpieczeństwa producenta urządzenia dla systemów Windows, backup na zewnętrzne dyski twarde,	
Współpraca z zewnętrznymi dostawcami usług chmury	Przynajmniej: Google Drive, Dropbox, Microsoft OneDrive, Microsoft OneDrive for Business i Box	
Darmowe aplikacje na urządzenia mobilne	Monitoring / Zarządzanie / Współdzielenie plików / obsługa kamer / Odtwarzacz muzyki Dostępne na systemy iOS oraz Android	
Minimum obsługiwane serwery	Serwer plików Serwer FTP Serwer WEB Serwer kopii zapasowych Serwer multimediów UPnP Serwer pobierania (Bittorrent / HTTP / FTP) Serwer Monitoringu	
VPN	VPN client / VPN server. Obsługa PPTP, OpenVPN	

Administracja systemu	Połączenia HTTP/HTTPS Powiadamianie przez e-mail (uwierzytelnianie SMTP) Powiadamianie przez SMS Ustawienia inteligentnego chłodzenia DDNS oraz zdalny dostęp w chmurze SNMP (v2 & v3) Obsługa UPS z zarządzaniem SNMP (USB) Obsługa sieciowej jednostki UPS Monitor zasobów Kosz sieciowy dla CIFS/SMB oraz AFP Monitor zasobów systemu w czasie rzeczywistym Rejestr zdarzeń System plików dziennika Całkowity rejestr systemowy (poziom pliku) Zarządzanie zdarzeniami systemowymi, rejestr, bieżące połączenie użytkowników on-line Aktualizacja oprogramowania Kopia zapasowa ustawień/przywracanie ustawień/resetowanie ustawień systemu	
Wirtualizacja	Wbudowana aplikacja umożliwiająca tworzenie środowiska wirtualnego wraz z instalacją maszyn wirtualnych na systemach Windows, Linux i Android. Dostęp do konsoli maszyn za pośrednictwem przeglądarki z HTML5 Funkcjonalności importu, eksportu, klonowania i wykonywania migawek maszyn wirtualnych.	
Konteneryzacja	Możliwość uruchomienia wirtualnych kontenerów dla LXC i Docker	
Zabezpieczenia	Filtracja IP Ochrona dostępu do sieci z automatycznym blokowaniem Połączenie HTTPS FTP z SSL/TLS (Explicit) Obsługa SFTP Szyfrowanie AES 256-bit Szyfrowana zdalna replikacja (Rsync poprzez SSH) Import certyfikatu SSL Powiadomienia o zdarzeniach za pośrednictwem Email i SMS	
Możliwość instalacji dodatkowego oprogramowania	Tak, sklep z aplikacjami; możliwość instalacji z paczek	
Dyski twarde	Macierz zostanie wyposażona w 4 dyski twarde 3.5” SATA 6Gb/s przystosowane do pracy z urządzeniami NAS (zapis ciągły 24/7) o pojemności min. 8 TB, prędkości 7200obr./min. Cache min. 256 MB. Dodatkowo dyski powinny posiadać parametr MTBF min. 2 mln godz. Wymaga się, aby dyski znajdowały się na liście kompatybilności dostarczanego urządzenia NAS zapewniając kompatybilność oraz wydajność.	
Gwarancja	2 lata na urządzenie 2 lat gwarancji na dyski.	

3. Przełącznik zarządzalny

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry techniczne oferowanego urządzenia
1	2	3	4

14.	Typ	Przełącznik sieciowy Ethernet Smart Management rack 1Gbit. W ofercie wymagane jest podanie modelu, symbolu oraz producenta.	…… …… */wpisać model, symbol, producenta urządzenia/*
15.	Porty	c) Minimum 48 porty 1G RJ45 10/100/1000BASE-T d) Minimum 4 porty SFP+ z możliwością pracy 1G/10G Porty SFP+ muszą być obsadzone wkładkami 10 Gigabit Ethernet – minimum 10GBase-SR, LR, Gigabit Ethernet – minimum 1000Base- SX, 1000Base LX	…… …… */wskazać ilość portów dla pkt a i b/*
16.	Parametry fizyczne	Wysokość maksymalnie 1U, montowany w szafie typu rack 19''	
17.	Pamięć	Co najmniej 512 MB SDRAM Co najmniej 256 MB pamięci flash Bufor pakietów co najmniej 1.5 MB CPU ARM Cortex-A9 @ 800 MHz	…… …… */wskazać wielkość pamięci DRAM i flash/*
18.	Wielkość tablicy adresów MAC	Co najmniej 16000	…… …… */wypełnić/*
19.	Ilość obsługiwanych sieci VLAN	Co najmniej 256	…… …… */wypełnić/*
20.	Wydajność	• Przepustowość przełączania: min. 176 Gbit/s • Przełączanie dla pakietów: min. 130 Mpps. • Opóźnienie: < 4.5 uSec dla 100 Mb < 2.2 uSec dla 1000 Mb <1.2 uSec dla 10 Gbps	…… …… */wypełnić/*
21.	Obsługa ramek Jumbo	O wielkości co najmniej 9216 bajtów	
22.	Funkcjonalność urządzenia	• obsługa agregacji portów zgodnie z LACP (IEEE 802.3ad), • obsługa protokołu SNTP, • Spanning Tree (802.1d), Rapid Convergence Spanning Tree (802.1w), MSTP (802.1s) • Minimum 256 obsługiwanych sieci VLAN • Automatyczne przydzielanie klasy urządzenia PoE w oparciu o LLDP oraz LLDP-MED. • Minimum 50 możliwych do utworzenia list ACL, • CoS zgodna z 802.1p • Voice VLAN • Minimum 509 wpisów ARP • Możliwość przechowywania dwóch obrazów oprogramowania: aktywny I zapasowy • Port Security • DHCP Snooping • Klient Radius • Port mirroring, • DHCP Relay, • DoS Protection, • ARP Attack Protection, • Możliwość utworzenia minimum 32 statycznych wpisów w tablicy routingu	
23.	Zasilanie	Zasilacz 230V AC wbudowany,	
24.	Temperatura pracy	0°C do 40°C	
25.	Zarządzanie	WWW (GUI), SNMP Manager, cloud-based web portal	

26.	Gwarancja	2 lata

4. UPS – zasilacz awaryjny

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne	Parametry techniczne oferowanego urządzenia
1	2	3	4
12.	Typ	Bezprzerwowy zasilacz UPS	…… */wpisać model, symbol, producenta urządzenia/*
13.	moc	3000 VA / 3000 W	…… */wskazać /*
14.	Ilość Faz	1 + G	
15.	Zakres napięcia	10 VAC - 300 VAC ± 5 % (w zależności od obciążenia)	…… */wskazać/*
16.	Sprawność całkowita	90 %	…… */wypełnić/*
17.	Obudowa	RACK maksymalnie 3 U	…… */wypełnić/*
18.	Czas podtrzymania	Minimum 8 minut przy obciążeniu 50% oraz 5 minut przy obciążeniu 100%	…… */wypełnić/*
19.	komunikacja	Port komunikacyjny RS232 i USB	
20.	Zarządzanie	Oprogramowanie zarządzające z możliwością zamykania systemów operacyjnych poprzez sieć logiczną: Windows Server 2012 Micorosft Hyper-V 2012 Windows Server 2008 Micorosft Hyper-V 2012 Windows Server 2003 Windows 8 WMware ESXi VMware ESX Red Hat Enterprise Linux Ubuntu Linux SuSE Linux Enterprise Server	
21.	Akcesoria	Szyny montażowe do szafy rack	
22.	Gwarancja	3 lata	

Dostawa zapory sieciowej firewall

5. Firewall UTM (dla Gminy) szt. 1

Cecha	Wymagania minimalne	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
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 dostawca 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 3 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	7. 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. 8. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 9. Monitoring stanu realizowanych połączeń VPN.	
Interfejsy, Dysk, Zasilanie:	9. System realizujący funkcję Firewall musi dysponować minimum 4 portami Gigabit Ethernet RJ-45. 10. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 11. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 12. System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe:	15. W zakresie Firewall'a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 16. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 17. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 18. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. 19. 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 1,0 Gbps. 20. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 21. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 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: 23. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 24. Kontrola Aplikacji. 25. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 26. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 27. Ochrona przed atakami - Intrusion Prevention System. 28. Kontrola stron WWW. 29. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 30. Zarządzanie pasmem (QoS, Traffic shaping). 31. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).	

	32. 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. 33. Analiza ruchu szyfrowanego protokołem SSL.	

Polityki, Firewall	9. Polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń. 10. 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. 11. W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN. 12. 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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
Połączenia VPN	5. 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. 6. 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	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	

Ochrona przed malware	11. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 12. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 13. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 14. 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. 15. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Ochrona przed atakami	15. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 16. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 17. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 18. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 19. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 20. 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. 21. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Kontrola aplikacji	16. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 17. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 18. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 19. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 20. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
Kontrola WWW	15. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 16. 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. 17. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 18. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 19. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 20. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 21. 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	8. 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. 9. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 10. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
Zarządzanie	8. 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. 9. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 10. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 11. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 12. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 13. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 14. 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	5. 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. 6. 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. 7. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 8. Musi istnieć możliwość logowania do serwera SYSLOG.	
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola 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 **5 lat**	
Gwarancja oraz wsparcie	10. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

6. Firewall UTM (dla GOPS) szt. 1

Cecha	Wymagania minimalne	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
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 dostawca 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 3 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	10. 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. 11. Monitoring i wykrywanie uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łączy sieciowych. 12. Monitoring stanu realizowanych połączeń VPN.	
Interfejsy, Dysk, Zasilanie:	13. System realizujący funkcję Firewall musi dysponować minimum 10 portami Gigabit Ethernet RJ-45. 14. System Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB. 15. W ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q. 16. System musi być wyposażony w zasilanie AC.	
Parametry wydajnościowe:	22. W zakresie Firewall'a obsługa nie mniej niż 600 tys. jednoczesnych połączeń oraz 35 tys. nowych połączeń na sekundę. 23. Przepustowość Stateful Firewall: nie mniej niż 5 Gbps dla pakietów 512 B. 24. Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 990 Mbps. 25. Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps. 26. 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 1,0 Gbps. 27. 8. Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 600 Mbps. 28. 9. Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu HTTPS – minimum 310 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: 34. Kontrola dostępu - zapora ogniowa klasy Stateful Inspection. 35. Kontrola Aplikacji. 36. Poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN. 37. Ochrona przed malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS. 38. Ochrona przed atakami - Intrusion Prevention System. 39. Kontrola stron WWW. 40. Kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3. 41. Zarządzanie pasmem (QoS, Traffic shaping). 42. Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP). 43. 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. 44. Analiza ruchu szyfrowanego protokołem SSL.	

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. 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 • Cisco ACI. • Google Cloud Platform (GCP). • OpenStack. • VMware vCenter (ESXi).	
Połączenia VPN	7. 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. 8. 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	W zakresie routingu rozwiązanie powinno zapewniać obsługę: • Routingu statycznego. • Policy Based Routingu. • Protokołów dynamicznego routingu w oparciu o protokoły: RIPv2, OSPF, BGP oraz PIM.	

Ochrona przed malware	16. Silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021). 17. System musi umożliwiać skanowanie archiwów, w tym co najmniej: zip, RAR. 18. System musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android). 19. 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. 20. System musi umożliwiać usuwanie aktywnej zawartości plików PDF oraz Microsoft Office bez konieczności blokowania transferu całych plików.	
Ochrona przed atakami	22. Ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych. 23. System powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach. 24. Baza sygnatur ataków powinna zawierać minimum 5000 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 25. Administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur. 26. System musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS. 27. 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. 28. Wykrywanie i blokowanie komunikacji C&C do sieci botnet.	
Kontrola aplikacji	9. Funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP. 10. Baza Kontroli Aplikacji powinna zawierać minimum 2000 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora. 11. Aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików. 12. Baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P. 13. Administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur.	
Kontrola WWW	22. Moduł kontroli WWW musi korzystać z bazy zawierającej co najmniej 40 milionów adresów URL pogrupowanych w kategorie tematyczne. 23. 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. 24. Filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard. 25. Administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL. 26. Funkcja Safe Search – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google, oraz Yahoo. 27. Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania. 28. 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	11. 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. 12. Musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwu-składnikowego. 13. Rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów: RADIUS lub API.	
Zarządzanie	11. 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. 12. Komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów. 13. Powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwu-składnikowego dla dostępu administracyjnego. 14. System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow. 15. System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację. 16. Element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall. 17. 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	14. 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. 15. 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. 16. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. 17. Musi istnieć możliwość logowania do serwera SYSLOG.	
Certyfikaty	Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać następujące certyfikacje: • ICSA lub EAL4 dla funkcji Firewall.	
Serwisy i licencje	W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: a) Kontrola 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 **5 lat**	
Gwarancja oraz wsparcie	18. Gwarancja: System musi być objęty serwisem gwarancyjnym producenta przez okres 12 miesięcy, polegającym na naprawie lub wymianie urządzenia w przypadku jego wadliwości. W ramach tego serwisu producent musi zapewniać również dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7.	

Dostawa komputerów stacjonarnych

7. Parametry komputera stacjonarnego (opis)

Lp.	Nazwa komponentu	Wymagane minimalne parametry techniczne komputerów	Parametry oferowane (w każdym wierszu należy określić typ/ model/ producent/ nr katalogowy)
1.	Komputer	Komputer będzie wykorzystywany dla potrzeb aplikacji biurowych, dostępu do Internetu oraz poczty elektronicznej, jako lokalna baza danych, stacja graficzna. W ofercie należy podać nazwę producenta, typ, model, oraz numer katalogowy oferowanego sprzętu.	
2.	Obudowa	Typu mini / midi tower z obsługą kart PCI Express. Fabrycznie umożliwiająca montaż min. 2 kieszeni: 1 szt. na napęd optyczny (dopuszcza się stosowanie napedów slim) zewnętrzna, 1 szt. 3,5”na standardowy dysk twardy. Wyposażona w czytnik kart multimedialnych Obudowa trwale oznaczona nazwą producenta, nazwą komputera, numerem MTM, PN, numerem seryjnym Wyposażona w budowany głośnik o mocy min. 2W	
3.	Zasilacz	Zasilacz minimalnie 500W o sprawności minimum 85%	
4.	Chipset	Dostosowany do zaoferowanego procesora	
5.	Płyta główna	Wyposażona w złącza min.: 4) 1 x PCI Express 3.0 x16, 5) 1 x PCI Express 3.0 x1, 6) 1 x M.2	
6.	Procesor	Procesor wielordzeniowy ze zintegrowaną grafiką, zaprojektowany do pracy w komputerach stacjonarnych klasy x86, o wydajności liczonej w punktach równej lub wyższej procesorowi AMD Ryzen 5 5600G na podstawie PerformanceTest w teście CPU Mark według wyników Avarage CPU Mark opublikowanych na	

		http://www.cpubenchmark.net/. Wykonawca w składanej ofercie winien podać dokładny model oferowanego podzespołu.	
7.	Pamięć operacyjna	Min. 16GB DDR4 3200MHz z możliwością rozszerzenia do 32 GB	
8.	Dysk twardy	Min 256GB SSD M.2 PCIe NVMe zawierający recovery umożliwiające odtworzenie systemu operacyjnego fabrycznie zainstalowanego na komputerze po awarii.	
9.	Napęd optyczny	Nagrywarka DVD +/-RW	
10.	Karta graficzna	dedykowana karta graficzna wyposażona w minimum 6 GB RAM, Szyna danych 192 bit Taktowanie pamięci minimum 15000 MHz, taktowanie rdzenia minimum 1777 Rodzaj pamięci RAM GDDR6	
11.	Audio	Karta dźwiękowa zintegrowana z płytą główną, zgodna z High Definition.	
12.	Karta sieciowa	LAN 10/100/1000 Mbit/s z funkją PXE oraz Wake on LAN WiFi 802.11ac 1x1 + BT 5.0	
13.	Porty/złącza	Wbudowane porty/złącza: 7) 1 x VGA, 8) 1 x HDMI, 9) 8 x USB w tym min. 4 x USB3.1 10) port sieciowy RJ-45, 11) porty słuchawek i mikrofonu na przednim lub tylnym panelu obudowy 12) czytnik kart pamięci min. SD Wymagana ilość i rozmieszczenie (na zewnątrz obudowy komputera) portów USB nie może być osiągnięta w wyniku stosowania konwerterów, przejściówek itp.	
14.	Monitor	Matryca 24” z podświetleniem w technologii LED, Kąt widzenia (stopnie): 178 (pion), 178 (poziom)Czas reakcji: 4 ms Kontrast: 3000:1 Rodzaj matrycy: VA	
15.	Klawiatura/mysz	Klawiatura przewodowa w układzie US Mysz przewodowa (scroll)	
16.	System operacyjny	Microsoft Windows 10 64 bit lub Windows 11 64 bit lub równoważny system operacyjny klasy PC, który spełnia następujące wymagania poprzez wbudowane mechanizmy, bez użycia dodatkowych aplikacji: 38) Dostępne dwa rodzaje graficznego interfejsu użytkownika: c) Klasyczny, umożliwiający obsługę przy pomocy klawiatury i myszy, d) Dotykowy umożliwiający sterowanie dotykiem na urządzeniach typu tablet lub monitorach dotykowych 39) Funkcje związane z obsługą komputerów typu tablet, z wbudowanym modułem „uczenia się” pisma użytkownika – obsługa języka polskiego 40) Interfejs użytkownika dostępny w wielu językach do wyboru – w tym polskim i angielskim 41) Możliwość tworzenia pulpitów wirtualnych, przenoszenia aplikacji pomiędzy pulpitami i przełączanie się pomiędzy pulpitami za pomocą skrótów klawiaturowych lub GUI. 42) Wbudowane w system operacyjny minimum dwie przeglądarki Internetowe 43) Zintegrowany z systemem moduł wyszukiwania informacji (plików różnego typu, tekstów, metadanych) dostępny z kilku poziomów: poziom menu, poziom otwartego okna systemu operacyjnego; system wyszukiwania oparty na konfigurowalnym przez użytkownika module indeksacji zasobów lokalnych, 44) Zlokalizowane w języku polskim, co najmniej następujące elementy: menu, pomoc, komunikaty systemowe, menedżer plików. 45) Graficzne środowisko instalacji i konfiguracji dostępne w języku polskim 46) Wbudowany system pomocy w języku polskim. 47) Możliwość przystosowania stanowiska dla osób	

		niepełnosprawnych (np. słabo widzących). 48) Możliwość dokonywania aktualizacji i poprawek systemu poprzez mechanizm zarządzany przez administratora systemu Zamawiającego. 49) Możliwość dostarczania poprawek do systemu operacyjnego w modelu peer-to-peer. 50) Zabezpieczony hasłem hierarchiczny dostęp do systemu, konta i profile użytkowników zarządzane zdalnie; praca systemu w trybie ochrony kont użytkowników. 51) Możliwość dołączenia systemu do usługi katalogowej on-premise lub w chmurze. 52) Umożliwienie zablokowania urządzenia w ramach danego konta tylko do uruchamiania wybranej aplikacji - tryb "kiosk". 53) Możliwość automatycznej synchronizacji plików i folderów roboczych znajdujących się na firmowym serwerze plików w centrum danych z prywatnym urządzeniem, bez konieczności łączenia się z siecią VPN z poziomu folderu użytkownika zlokalizowanego w centrum danych firmy. 54) Transakcyjny system plików pozwalający na stosowanie przydziałów (ang. quota) na dysku dla użytkowników oraz zapewniający większą niezawodność i pozwalający tworzyć kopie zapasowe. 55) Oprogramowanie dla tworzenia kopii zapasowych (Backup); automatyczne wykonywanie kopii plików z możliwością automatycznego przywrócenia wersji wcześniejszej. 56) Możliwość przywracania obrazu plików systemowych do uprzednio zapisanej postaci. 57) Możliwość przywracania systemu operacyjnego do stanu początkowego z pozostawieniem plików użytkownika. 58) Możliwość blokowania lub dopuszczania dowolnych urządzeń peryferyjnych za pomocą polityk grupowych (np. przy użyciu numerów identyfikacyjnych sprzętu)." 59) Wbudowany mechanizm wirtualizacji typu hypervisor." 60) Dostępność bezpłatnych biuletynów bezpieczeństwa związanych z działaniem systemu operacyjnego. 61) Wbudowana zapora internetowa (firewall) dla ochrony połączeń internetowych, zintegrowana z systemem konsola do zarządzania ustawieniami zapory i regułami IP v4 i v6. 62) Identyfikacja sieci komputerowych, do których jest podłączony system operacyjny, zapamiętywanie ustawień i przypisywanie do min. 3 kategorii bezpieczeństwa (z predefiniowanymi odpowiednio do kategorii ustawieniami zapory sieciowej, udostępniania plików itp.). 63) Wbudowany system uwierzytelnienia dwuskładnikowego oparty o certyfikat lub klucz prywatny oraz PIN lub uwierzytelnienie biometryczne. 64) Wbudowane mechanizmy ochrony antywirusowej i przeciw złośliwemu oprogramowaniu z zapewnionymi bezpłatnymi aktualizacjami. 65) Możliwość tworzenia wirtualnych kart inteligentnych. 66) Wsparcie dla firmware UEFI i funkcji bezpiecznego rozruchu (SecureBoot) 67) Wbudowany w system, wykorzystywany automatycznie przez wbudowane przeglądarki filtr reputacyjny URL. 68) Wsparcie dla IPSEC oparte na politykach – wdrażanie IPSEC oparte na zestawach reguł definiujących ustawienia zarządzanych w sposób centralny. 69) Mechanizmy logowania w oparciu o: f) Login i hasło, g) Karty inteligentne i certyfikaty (smartcard), h) Wirtualne karty inteligentne i certyfikaty (logowanie w oparciu o certyfikat chroniony poprzez moduł TPM), i) Certyfikat/Klucz i PIN j) Certyfikat/Klucz i uwierzytelnienie biometryczne 70) Wsparcie dla uwierzytelniania na bazie Kerberos v. 5 71) Wbudowany agent do zbierania danych na temat zagrożeń na	

		stacji roboczej. 72) Wsparcie .NET Framework 2.x, 3.x i 4.x – możliwość uruchomienia aplikacji działających we wskazanych środowiskach 73) Wsparcie dla VBScript – możliwość uruchamiania interpretera poleceń 74) Wsparcie dla PowerShell 5.x – możliwość uruchamiania interpretera poleceń Nie dopuszcza się zaoferowania systemu operacyjnego typu refurbished.	
17.	BIOS	BIOS zgodny ze specyfikacją UEFI Możliwość, bez uruchamiania systemu operacyjnego z dysku twardego komputera lub innych podłączonych do niego urządzeń zewnętrznych informacji o: 10) modelu komputera, PN 11) numerze seryjnym, 12) AssetTag, 13) MAC Adres karty sieciowej, 14) wersja Biosu wraz z datą produkcji, 15) zainstalowanym procesorze, jego taktowaniu i ilości rdzeni 16) ilości pamięci RAM wraz z taktowaniem, 17) stanie pracy wentylatora na procesorze 18) napędach lub dyskach podłączonych do portów SATA oraz M.2 (model dysku i napędu optycznego) Możliwość z poziomu Bios: 5) wyłączania/włączania portów USB zarówno z przodu jak i z tyłu obudowy 6) wyłączenia selektywnego (pojedynczego) portów SATA, 7) wyłączenia karty sieciowej, karty audio, portu szeregowego, 8) możliwość ustawienia portów USB w jednym z dwóch trybów: c) użytkownik może kopiować dane z urządzenia pamięci masowej podłączonego do pamięci USB na komputer ale nie może kopiować danych z komputera na urządzenia pamięci masowej podłączone do portu USB d) użytkownik nie może kopiować danych z urządzenia pamięci masowej podłączonego do portu USB na komputer oraz nie może kopiować danych z komputera na urządzenia pamięci masowej 5) ustawienia hasła: administratora, Power-On, HDD, 6) blokady aktualizacji BIOS bez podania hasła administratora 7) załadowania optymalnych ustawień Bios 8) obsługa Bios za pomocą klawiatury i myszy	
19.	Certyfikaty i standardy	2) Deklaracja zgodności CE (załączyć do oferty)	
20.	Bezpieczeństwo i zdalne zarządzanie	2) Czujnik otwarcia obudowy	
21.	Gwarancja	*2 lata*	

2. Oświadczamy, że oferta gwarantuje **gwarancję na okres wymagany dla poszczególnych komponentów określony w SWZ.**

3. Zobowiązujemy do wykonania dostawy przedmiotu zamówienia w terminie: **…….. miesięcy od dnia zawarcia umowy**.

4. Oświadczamy, że akceptujemy warunki płatności określone w Specyfikacji Warunkach Zamówienia.

5. Oświadczamy, że jesteśmy związani ofertą od dnia upływu terminu składania ofert do dnia określonego w SWZ.

6. Oświadczamy, że w cenie zostały uwzględnione wszystkie koszty wykonania zamówienia.

7. Oświadczamy, że zapoznaliśmy się z projektowanymi postanowieniami umowy i zobowiązujemy się w przypadku wyboru niniejszej oferty do zawarcia umowy na warunkach w nich określonych.

8. Oświadczamy, że przedmiot zamówienia wykonamy **samodzielnie*/przy pomocy podwykonawców***

   ……..……
   ……
   (należy wskazać część zamówienia, której wykonanie zamierza powierzyć podwykonawcom oraz podać nazwy podwykonawców jeżeli są już znani).

9. Oświadczamy, iż wybór naszej oferty **prowadzi* / nie prowadzi*** do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą o podatku towarów i usług (art. 225 ustawy Pzp).

   ……
   ……..…..
   (w przypadku, gdy wybór oferty będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego należy wskazać nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, wskazać ich wartość towaru lub usługi bez kwoty podatku oraz wskazać stawkę podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie – dla każdej wybranej części zamówienia osobno).

10. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO[1)] wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.**

    [1)]*rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1).*

11. Rodzaj Wykonawcy *(należy wybrać właściwe)*:

    ☐ mikroprzedsiębiorstwo

    ☐ małe przedsiębiorstwo

    ☐ średnie przedsiębiorstwo

    ☐ prowadzenie jednoosobowej działalności

    ☐ osoba fizyczna nie prowadząca działalności gospodarczej

    ☐ inny rodzaj

    Por. zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych.
    Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR.
    Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR.

Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwamii które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR lub roczna suma bilansowa nie przekracza 43 milionów EUR.

.....

miejscowość, data

(należy opatrzyć kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym osoby uprawnionej lub osób uprawnionych do reprezentowania Wykonawcy)

**niewłaściwe skreślić*

*** w przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO treści oświadczenia wykonawca nie składa (usunięcie treści oświadczenia np. przez jego wykreślenie).*

UWAGA!

Wykonawcy składający ofertę wspólnie w miejscu „Pieczęć firmowa Wykonawcy" wpisują dane wszystkich Wykonawców występujących wspólnie.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym.

Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Projekt „Cyfrowa gmina" jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.

Wzór - załącznik nr 3 do SWZ

(obowiązkowy)

Zamawiający:

Gmina Szczytno

ul. Łomżyńska 3

12-100 Szczytno

Wykonawca/podmiot udostępniający zasoby/podwykonawca*:

……

…….....

……

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

reprezentowany przez:

……

……

(imię, nazwisko, stanowisko/podstawa do 200 reprezentacji)

Oświadczenie Wykonawcy/podmiotu udostępniającego zasoby/podwykonawcy*

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako: Ustawą),

DOTYCZĄCE PRZESŁANEK WYKLUCZENIA Z POSTĘPOWANIA

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** prowadzonego przez **Gminę Szczytno**, oświadczam, co następuje

OŚWIADCZENIA DOTYCZĄCE WYKONAWCY / PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY / PODWYKONAWCY1:

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 Ustawy pzp.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 1,

4 i 7 Ustawy pzp.

3. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie w art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego.

……..…..... *(miejscowość),* dnia ……..…..... r.

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 lub art. 109 ust. 1 pkt 1, 4 i 7 Ustawy pzp).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 Ustawy podjąłem następujące środki naprawcze:

…….....
……
……
……

…….....…. *(miejscowość),* dnia …….....…..... r.

*– niepotrzebne skreślić;

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Wzór - Załącznik nr 4 do SWZ

(obowiązkowy)

Zamawiający:

Gmina Szczytno

ul. Łomżyńska 3

12-100 Szczytno

Wykonawca/podmiot udostępniający zasoby/podwykonawca*:

……

…….....

……

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

reprezentowany przez:

……

……

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Oświadczenie Wykonawcy/podmiotu udostępniającego zasoby*

składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r.

Prawo zamówień publicznych (dalej jako: Ustawa),

DOTYCZĄCE SPEŁNIANIA WARUNKU UDZIAŁU W POSTĘPOWANIU

Na potrzeby postępowania o udzielenie zamówienia publicznego pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** prowadzonego przez **Gminę Szczytno**, oświadczam, co następuje:

INFORMACJA DOTYCZĄCA WYKONAWCY/PODMIOTU UDOSTĘPNIAJĄCEGO ZASOBY:**

Oświadczam, że spełniam warunek udziału w postępowaniu określony przez Zamawiającego w ……..……..……
……..

(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu).

……..……. *(miejscowość),* dnia ……..……. r.

INFORMACJA W ZWIĄZKU Z POLEGANIEM NA ZASOBACH INNYCH PODMIOTÓW:**

Oświadczam, że w celu wykazania spełniania warunku udziału w postępowaniu, określonego przez Zamawiającego w ……..…….. *(wskazać dokument i właściwą jednostkę redakcyjną dokumentu, w której określono warunki udziału w postępowaniu),* polegam na zasobach następującego/ych podmiotu/ów:

..…….

w następującym zakresie:
……..……..……
……
(określić odpowiedni zakres dla wskazanego podmiotu).

……..……. *(miejscowość),* dnia ……..……. r.

*** – niepotrzebne skreślić;**
****– wypełnia tylko Wykonawca, który w celu wykazania spełnienia warunków udziału polega na zasobach podmiotu**

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Wzór - Załącznik nr 5 do SWZ

(obowiązkowy- jeśli dotyczy)

Zobowiązanie podmiotu o oddaniu Wykonawcy swoich zasobów
w zakresie zdolności technicznych/zawodowych

Ja/My

.....*

(nazwa podmiotu udostępniającego zasoby)

zobowiązujemy się do oddania do dyspozycji Wykonawcy:

.....*

(nazwa Wykonawcy ubiegającego się o udzielenie zamówienia)

niezbędnych zasobów na potrzeby wykonania zamówienia pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”** w związku z powołaniem się na te zasoby w celu spełniania warunku udziału w postępowaniu przez Wykonawcę w zakresie zdolności technicznych/zawodowych poprzez udział w realizacji zamówienia w charakterze **Podwykonawcy/w innych charakterze**** w zakresie ……*(należy wypełnić w takim zakresie w jakim podmiot zobowiązuje się oddać Wykonawcy swoje zasoby w zakresie zdolności technicznych/zawodowych)* na okres ……..……*

***– należy wypełnić**

****– niepotrzebne skreślić**

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.

Wzór - Załącznik nr 6 do SWZ

(na wezwanie Zamawiającego)

WYKAZ DOSTAW

Dotyczy: postępowania pn. **Zakup sprzętu komputerowego i wyposażenia serwerowni Urzędu Gminy Szczytno i jednostek podległych Gminie Szczytno w ramach projektu „Cyfrowa Gmina”**

L.p.	Przedmiot realizowanych dostaw	Wartość zrealizowanych dostaw (brutto)	Czas realizacji dostaw	Nazwa podmiotu, na którego rzecz dokonano dostaw
1				
2				
3				

Do Wykazu załączam dowody potwierdzające, że wskazane dostawy wykonane zostały w sposób należyty.

Dokument należy wypełnić i podpisać kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Zamawiający zaleca zapisanie dokumentu w formacie PDF.

Projekt „Cyfrowa gmina” jest finansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 - 2020.