WZ.7011.3.2023.WJ1 Stargard, 22.05.2023 r.

POWIAT STARGARDZKI
ul. Skarbowa 1
73-110 Stargard
NIP 854-22-28-620

**ZAPROSZENIE DO SKŁADANIA OFERT**
na dostawę dwóch zapór sieciowych wraz z licencjami

**I. Tryb postępowania**

1. Zamówienie finansowane w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Osi Priorytetowej V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowy Powiat"
2. Wartość niniejszego zamówienia nie przekracza kwoty 130 000 zł, o której mowa w art. 2 ust. 1 pkt 1 ustawy – Prawo zamówień publicznych, w związku z tym w niniejszym postępowaniu zastosowanie mają zasady udzielania zamówień publicznych określone w art. 16 przywołanej ustawy. Postępowanie prowadzone jest z zastosowaniem zasady konkurencyjności, opisanej w podrozdziale 6.5.2 Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020.

**II. Przedmiot zamówienia**

1. Przedmiotem zamówienia jest:
   1) dostawa dwóch urządzeń – zapór sieciowych wraz z licencjami w celu rozbudowy zabezpieczeń logicznych (firewall, systemy IDS, IPS),
   2) zdalna asysta przy konfiguracji dostarczonych urządzeń i oprogramowania.

   Zamawiający informuje, że dokona podłączenia urządzeń we własnym zakresie.
2. Szczegółowy opis przedmiotu zamówienia zawarto w **Załączniku nr 1**, który stanowi integralną część niniejszego Zaproszenia.
3. Oznaczenie przedmiotu zamówienia wg Wspólnego Słownika Zamówień CPV:
   KOD – 48210000-3 – Pakiety oprogramowania dla sieci
   KOD – 32420000-3 – Urządzenia sieciowe

**III. Warunki i termin gwarancji**

1. Zamawiający wymaga udzielenia 36 miesięcznej gwarancji.
2. Warunki gwarancji określono w *Projekcie Umowy* – **Załącznik Nr 2**, który stanowi integralną część niniejszego Zaproszenia.

**IV. Termin realizacji**

1. Termin realizacji zamówienia: do 22.06.2023 r.
2. Terminem rozpoczęcia realizacji zadania jest dzień podpisania umowy.
3. Terminem zakończenia realizacji zadania jest termin zakończenia konfiguracji dostarczonych urządzeń oraz oprogramowania.
4. Szczegółowe zasady przeprowadzania odbioru zawarto w Załączniku Nr 2 – *Projekt Umowy.*

**V. Warunki udziału w postępowaniu**

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
   1) nie podlegają wykluczeniu z udziału w postępowaniu z przyczyn opisanych w pkt. V. 2 niniejszego zaproszenia,
   2) spełniają warunki udziału w postępowaniu, tj. posiadają zdolności techniczne i zawodowe niezbędne do realizacji niniejszego zamówienia, a mianowicie:

a) podmioty będące autoryzowanym przedstawicielem producenta bądź odpowiednio dystrybutora oferowanych urządzeń,
b) podmioty dysponujące co najmniej dwiema osobami posiadającymi odpowiednie kwalifikacje zawodowe niezbędne do prawidłowej realizacji zamówienia w zakresie konfiguracji i usług serwisowych, tj.: aktualny certyfikat producenta oferowanego rozwiązania, przy czym Zamawiający pożąda aby w przypadku stosowania przez producenta stopniowego systemu certyfikacji, co najmniej jedna z osób wyznaczonych do realizacji zamówienia posiadała najwyższy stopień certyfikacji,

2. Zamawiający wykluczy z postępowania Wykonawcę:
   1) który jest powiązany osobowo lub kapitałowo z Zamawiającym. Przez powiązania kapitałowe lub osobowe rozumie się wzajemne powiązania między Zamawiającym lub osobami upoważnionymi do zaciągania zobowiązań w imieniu Zamawiającego lub osobami wykonującymi w imieniu Zamawiającego czynności związane z przeprowadzeniem procedury wyboru Wykonawcy a Wykonawcą, polegające w szczególności na:
      a) uczestniczeniu w spółce jako wspólnik spółki cywilnej lub spółki osobowej,
      b) posiadaniu co najmniej 10% udziałów lub akcji, o ile niższy próg nie wynika z przepisów prawa lub nie został określony przez instytucję zarządzającą programem operacyjnym,
      c) pełnieniu funkcji członka organu nadzorczego lub zarządzającego, prokurenta, pełnomocnika,
      d) pozostawaniu w związku małżeńskim, w stosunku pokrewieństwa lub powinowactwa w linii prostej, pokrewieństwa drugiego stopnia lub powinowactwa drugiego stopnia w linii bocznej lub w stosunku przysposobienia, opieki lub kurateli.
   2) będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
      a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
      b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
      c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46– 48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2020 r. poz. 1133 oraz z 2021 r. poz. 2054) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2021 r. poz. 523, 1292, 1559 i 2054),
      d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
      e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
      f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
      g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
      h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej
      - lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
   3) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w ppkt 2 lit. a-h,
   4) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub

zdrowotne, chyba że Wykonawca odpowiednio przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności,

5) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne,
6) jeżeli Zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że Wykonawca zawarł z innymi Wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty lub oferty częściowe, chyba że wykażą, że przygotowali te oferty niezależnie od siebie,
7) jeżeli doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego Wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie Wykonawcy z udziału w postępowaniu o udzielenie zamówienia,
8) w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury,
9) zgodnie z 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 (Dz. U. z 2022 r. poz. 835):
   a) wymienionego w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisanego na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3,
   b) którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz. U. z 2022 r. poz. 593 i 655) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3,
   c) którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz. 217, 2105 i 2106) jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3.

3. W przypadku Wykonawcy wykluczonego na podstawie art. 7 ust. 1 ustawy o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, Zamawiający odrzuca ofertę takiego Wykonawcy.
4. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia.

**VI. Kryteria oceny ofert**

Przy wyborze oferty Zamawiający będzie kierował się kryterium cena – 100%

1. Kryterium procentowe zostanie zmienione na punkty według następującego wzoru:

$$Lp = Cn : Cb \times 100$$

   Lp – liczba punktów,
   Cn – cena brutto najniższa spośród zaoferowanych,
   Cb – cena brutto badana
2. Zamawiający oceni i porówna jedynie te oferty, które nie zostaną odrzucone.
3. Ostateczna ocena punktowa oferty:
   1) ocena punktowa oferty będzie zaokrąglona do dwóch miejsc po przecinku,

2) za najkorzystniejszą zostanie uznana oferta, nie podlegająca odrzuceniu, która otrzyma największą liczbę punktów.

3. W toku badania i oceny ofert Zamawiający może żądać od potencjalnych Wykonawców uzupełnień i wyjaśnień treści złożonych ofert.
4. Zamawiający zastrzega, że w przypadku, gdy cena oferty będzie wydawać się rażąco niska w stosunku do przedmiotu zamówienia i będzie budzić wątpliwości co do możliwości wykonania przedmiotu zamówienia, zgodnie z wymaganiami określonymi w zaproszeniu do składania ofert, a w szczególności, gdy będzie niższa o 30% od wartości zamówienia lub średniej arytmetycznej cen wszystkich złożonych ofert, wystąpi o udzielenie wyjaśnień. W przypadku, gdy Wykonawca nie wykaże, że oferta nie zawiera rażąco niskiej ceny, oferta taka będzie podlegała odrzuceniu.

**VII. Sposób złożenia oferty oraz dokumenty potwierdzające spełnienie warunków**

1. Wykonawca składa ofertę na Formularzu oferty, zgodnie z **Załącznikiem Nr 3** do niniejszego zaproszenia. Wraz z ofertą należy złożyć:
   1) aktualne na dzień składania ofert *Oświadczenie Wykonawcy o braku podstaw do wykluczenia z postępowania oraz o spełnianiu warunków udziału w postępowaniu* – wg wzoru stanowiącego **Załącznik Nr 4** do niniejszego zaproszenia,
   2) dokument potwierdzający, że Wykonawca jest autoryzowanym przedstawicielem producenta bądź odpowiednio autoryzowanego przedstawiciela dystrybutora oferowanych urządzeń,
   3) certyfikat potwierdzający kwalifikacje osób wyznaczonych do realizacji zamówienia zgodnie z zapisami w Dziale V pkt 1 ppkt 2 lit. b,
   4) aktualny odpis z właściwego rejestru lub z centralnej ewidencji i informacji o działalności gospodarczej, jeżeli odrębne przepisy wymagają wpisu do rejestru lub ewidencji, wystawiony nie wcześniej niż 6 miesięcy przed upływem terminu składania ofert,
   5) upoważnienie osób podpisujących ofertę do reprezentacji Wykonawcy, w przypadku, gdy ofertę podpisują osoby inne niż wymienione w wypisie z właściwego rejestru bądź innym dokumencie dopuszczającym Wykonawcę do obrotu prawnego.
2. Oferta powinna być podpisana przez osobę upoważnioną do reprezentowania Wykonawcy, zgodnie z formą reprezentacji określoną w rejestrze lub innym dokumencie, właściwym dla danej formy organizacyjnej Wykonawcy albo przez upełnomocnionego przedstawiciela Wykonawcy,
3. Ofertę oraz wszystkie wymagane oświadczenia i dokumenty, należy złożyć pod rygorem nieważności w formie elektronicznej, tj. w postaci elektronicznej opatrzonej elektronicznym podpisem kwalifikowanym, podpisem zaufanym lub podpisem osobistym.:
   a) za pośrednictwem poczty elektronicznej na adres: zampub@powiatstargardzki.eu lub
   b) za pośrednictwem bazy konkurencyjności: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl (szczegóły dotyczące sposobu składania ofert znajdują się na wskazanej stronie),
4. W przypadku braków formalnych, oferta podlega jednokrotnemu uzupełnieniu przez Wykonawcę na wezwanie Zamawiającego. Nieuzupełnienie oferty w zakresie wskazanym przez Zamawiającego lub w wyznaczonym przez niego terminie skutkować będzie odrzuceniem oferty.
5. Oferta oraz wszelkie oświadczenia i zaświadczenia składane w trakcie postępowania są jawne, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł że nie mogą być one udostępnione innym uczestnikom postępowania oraz wykazał, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, dotyczących nazwy Wykonawcy oraz cen zawartych w ofertach. Dokumenty niejawne, nie podlegające udostępnieniu innym uczestnikom postępowania, Wykonawca zobowiązany jest wyszczególnić w formularzu ofertowym.

**VIII. Opis sposobu obliczenia ceny oferty**

1. Zaoferowana cena musi obejmować koszty związane z realizacją zamówienia.
2. Kalkulując cenę Wykonawca winien brać pod uwagę wszelkie czynniki mające wpływ na jej wartość w całym okresie realizacji zamówienia z uwzględnieniem okresu gwarancji, w tym m.in. koszty dostawy urządzeń, zdalnej asysty przy konfiguracji, koszty transportu, dojazdów

Wykonawcy do siedziby Zamawiającego, a także koszty serwisowania w okresie gwarancji i rękojmi.

3. Cena muszą zawierać wszystkie koszty związane z wykonaniem zamówienia, w tym podatek VAT i muszą być podane cyfrowo i słownie, z wyodrębnionym podatkiem VAT.
4. Wartość stanowiąca cenę oferty, którą należy wpisać do formularza oferty – **Załącznik Nr 3** będzie podlegała ocenie zgodnie z zasadami określonymi w Dziale VI.
5. Podstawą oceny ofert będzie cena oferty, ustalona zgodnie z art. 3 ust. 1 pkt 1) oraz ust. 2 ustawy o informowaniu o cenach towarów i usług z dnia 9 maja 2014 roku, tj. wartość wyrażona w jednostkach pieniężnych, którą kupujący jest obowiązany zapłacić przedsiębiorcy za towar lub usługę. W cenie uwzględnia się podatek od towarów i usług oraz podatek akcyzowy, jeżeli na podstawie odrębnych przepisów sprzedaż towaru (usługi) podlega obciążeniu podatkiem od towarów i usług lub podatkiem akcyzowym. Cena, o której mowa, otrzymuje nazwę „cena brutto oferty".
6. Cena oferty powinna być wyrażona w złotych polskich z dokładnością do drugiego miejsca po przecinku, zgodnie z art. 1 ust.2 ustawy z dn. 7 lipca 1994 r. o denominacji złotego (Dz. U. z 1994 r Nr 84, poz. 386, z późn. zm.), zgodnie z którym jednostka pieniężna o nazwie złoty dzieli się na 100 groszy.
7. Zamawiający poprawia w tekście oferty oczywiste omyłki pisarskie, rachunkowe z uwzględnieniem konsekwencji rachunkowych dokonanych poprawek.

**IX. Warunki płatności:**

1. Rozliczenie między Zamawiającym a Wykonawcą za realizację przedmiotu zamówienia będzie dokonane wyłącznie w walucie polskiej.
2. Zapłata wynagrodzenia za wykonanie przedmiotu umowy nastąpi po zrealizowaniu przedmiotu umowy, tj. po dostarczeniu i skonfigurowaniu urządzeń potwierdzonych podpisaniem protokołu odbioru, na podstawie prawidłowo wystawionej faktury.
3. Szczegółowe warunki i zasady płatności zawarto w *Projekcie umowy*, stanowiącym Załącznik Nr 2 do niniejszego Zaproszenia.

**X. Termin składania ofert**

1. Termin złożenia oferty: do dnia 30.05.2023 roku do godz. 9:00.
2. Za moment złożenia oferty przyjmuje się termin otrzymania oferty przez Zamawiającego.

**XI. Informacja o ofertach częściowych i wariantowych**

1. Zamawiający nie przewiduje składania ofert częściowych.
2. Zamawiający nie przewiduje składania ofert wariantowych.

**XII. Termin związania ofertą**

1. Termin związania ofertą wynosi 30 dni.
2. Bieg terminu rozpoczyna się wraz z upływem terminu składania ofert.

**XIII. Przesłanki odrzucenia oferty**

Oferta podlega odrzuceniu w przypadku, gdy:

1) jej treść nie odpowiada treści zaproszenia do składania ofert, w tym w szczególności gdy proponowane urządzenia nie spełniają wymagań opisanych w Opisie przedmiotu zamówienia (Załącznik nr 1 do niniejszego zaproszenia),
2) została złożona przez Wykonawcę podlegającego wykluczeniu,
3) Wykonawca nie potwierdził spełnienia warunków udziału w postępowaniu,
4) Wykonawca nie dołączył do oferty wymaganych dokumentów i nie uzupełnił ich na wezwanie Zamawiającego w określonym terminie,
5) nie zachowano zgodności z wymogami określonymi w Rozdziale VII – Przygotowanie i sposób złożenia oferty,
6) została złożona po terminie składania ofert określonym w zaproszeniu do składania ofert.

**XIV. Opis sposobu udzielania wyjaśnień do treści zaproszenia do składania ofert oraz sposób porozumiewania się Zamawiającego z wykonawcami**

1. Wykonawca może zwrócić się do Zamawiającego o wyjaśnienie treści zaproszenia do składania ofert. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania pod warunkiem, że wniosek o wyjaśnienie treści zaproszenia do składania ofert wpłynął do Zamawiającego nie później niż do końca dnia, w którym upływa połowa wyznaczonego terminu składania ofert. Jeżeli wniosek o wyjaśnienie treści zaproszenia wpłynął po upływie terminu składania wniosku lub dotyczy udzielonych wyjaśnień, Zamawiający może udzielić wyjaśnień albo pozostawić wniosek bez rozpoznania. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku, o którym mowa w zdaniu pierwszym.
2. Treść zapytań wraz z wyjaśnieniami Zamawiający przekazuje Wykonawcom, bez ujawniania źródła zapytania oraz zamieszcza je na stronie internetowej, na której upubliczniono zaproszenie do składania ofert.
3. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść zaproszenia do składania ofert. Dokonaną zmianę treści niniejszego zaproszenia Zamawiający udostępnia na stronie internetowej, na której upubliczniono zaproszenie do składania ofert.
4. Jeżeli w wyniku zmiany treści zaproszenia do składania ofert jest niezbędny dodatkowy czas na wprowadzenie zmian w ofertach, Zamawiający przedłuża termin składania ofert i informuje o tym Wykonawców oraz zamieszcza informację na stronie internetowej, na której upubliczniono zaproszenie do składania ofert.
5. Oświadczenia, wnioski, pytania, zawiadomienia oraz informacje Zamawiający i Wykonawcy przekazują pocztą elektroniczną.
6. Pytania należy kierować w formie elektronicznej na adres e-mail: zampub@powiatstargardzki.eu lub za pośrednictwem platformy https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl
7. Zamawiający urzęduje od poniedziałku do piątku w godzinach od 8:00 do 16:00.

**XV. Zmiana treści zaproszenia do składania ofert**

1. Zamawiający może przed wyznaczonym terminem składania ofert zmienić treść zaproszenia do składania ofert. Dokonaną zmianę Zamawiający upubliczni na stronie internetowej Zamawiającego, na stronie na której upubliczniono zaproszenie do składania ofert.
2. W wyniku zmiany treści zaproszenia do składania ofert, Zamawiający może przedłużyć termin składania ofert, o czas niezbędny na wprowadzenie przez Wykonawcę zmian w ofercie.
3. Zmiany treści zaproszenia do składania ofert oraz udzielone przez Zamawiającego wyjaśnienia są każdorazowo wiążące dla Wykonawców.

**XVI. Informacje o formalnościach, jakie zostaną dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia**

1. Zamawiający zawrze umowę z Wykonawcą, który przedłoży najkorzystniejszą ofertę z punktu widzenia kryteriów przyjętych w niniejszym zaproszeniu do składania ofert.
2. Umowa zostanie zawarta w formie pisemnej pod rygorem nieważności.
3. Zamawiający informuje wybranego Wykonawcę o miejscu i terminie zawarcia umowy.
4. Umowa w sprawie realizacji zamówienia zawarta zostanie z uwzględnieniem postanowień wynikających z treści niniejszego zaproszenia do składania ofert oraz danych zawartych w ofercie.
5. W przypadku gdy Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia, Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców oraz wybrać najkorzystniejszą ofertę albo unieważnić postępowanie.

**XVII. Zmiana treści umowy**

Zamawiający przewiduje możliwość zmiany postanowień zawartej umowy w następującym zakresie:

1. w przypadkach i na zasadach określonych przez Ministra Finansów, Funduszy i Polityki Regionalnej w „Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego

Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014-2020" – pkt 6.5.2 ppkt 20 lit. b, c, d,

2. zmiany terminu realizacji przedmiotu umowy, tj.:
   1) z powodu wystąpienia przeszkód o obiektywnym, nadzwyczajnym i niemożliwym do przewidzenia charakterze, w szczególności takich jak niedobory rynkowe, przedłużający się czas dostawy u producenta, itp.,
   2) z przyczyn leżących po stronie Zamawiającego, w szczególności wstrzymania terminu dostawy bądź niemożliwości realizacji umowy w wyniku działań osób trzecich;.

**XVIII. Unieważnienie postępowania**

1. Zamawiający unieważnia postępowanie, w przypadku:
   a) nie została złożona żadna oferta,
   b) żadna ze złożonych ofert nie odpowiada wymaganiom stawianym przez Zamawiającego,
   c) cena najkorzystniejszej oferty przewyższa kwotę, którą Zamawiający może przeznaczyć na sfinansowanie zamówienia, chyba że Zamawiający może zwiększyć tę kwotę do ceny najkorzystniejszej oferty,
   d) w przypadku, gdy jego dalsze prowadzenie lub zawarcie umowy nie będzie leżało w interesie publicznym lub gdy obarczone będzie wadą lub z innych przyczyn będzie zachodziła potrzeba zmiany warunków udzielenia lub realizacji zamówienia.
2. Zamawiający zastrzega sobie prawo unieważnienia postępowania o udzielenie zamówienia bez dokonania wyboru którejkolwiek ze złożonych ofert, na każdym jego etapie, bez uprzedniego informowania Wykonawców oraz bez podawania przyczyn takiego zakończenia postępowania.
3. Zamawiający nie przewiduje środków odwoławczych od rozstrzygnięcia Zamawiającego, podejmowanych w ramach postępowania o udzielenie zamówienia.

**XIX. Dodatkowe informacje**

1. Zaproszenie do składania ofert opublikowano w Bazie Konkurencyjności pod adresem: https://bazakonkurencyjnosci.funduszeeuropejskie.gov.pl oraz na stronie internetowej Zamawiającego pod adresem https://bip.powiatstargardzki.pl w zakładce Zamówienia publiczne poniżej 130 000 złotych
2. Informację o wyborze najkorzystniejszej oferty Zamawiający zamieści w Bazie Konkurencyjności oraz na stronie internetowej Zamawiającego wskazanej powyżej oraz przekaże Wykonawcom uczestniczącym w postępowaniu na adresy wskazane w Ofercie.
3. Jeżeli Zamawiający lub Wykonawca przekazuje korespondencję e-mailem, każda ze stron na żądanie drugiej niezwłocznie potwierdza fakt jej otrzymania. W przypadku przekazywania dokumentów e-mailem dowód prawidłowej transmisji danych oznacza, że Wykonawca otrzymał korespondencję w momencie jej przekazania przez Zamawiającego, niezależnie od ewentualnego potwierdzenia faktu jej otrzymania. Zamawiający nie ponosi odpowiedzialności za niesprawne działanie urządzeń Wykonawcy.

**XX. Klauzula Informacyjna**

1. Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), dalej „RODO", Zamawiający informuję, że:
   1) Administratorem Pani/Pana danych osobowych jest Starosta Stargardzki z siedzibą w Stargardzie, ul. Skarbowa 1, 73-110 Stargard, tel. 91 48 04 802/803,
   2) Inspektorem ochrony danych osobowych w Starostwie Powiatowym w Stargardzie jest Pan Tadeusz Ler, z którym można skontaktować się w sprawach ochrony swoich danych osobowych pod nr tel. 91 48 04 802/803, e-mail: iod@powiatstargardzki.pl, lub pisemnie na adres siedziby wskazany w ppkt 1),
   3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO, w celu związanym z postępowaniem o udzielenie zamówienia na „Dostawa dwóch zapór sieciowych wraz z licencjami", Nr WZ.7011.3.2023.WJ1,

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o ustawę z dnia 6 września 2001 r. – o dostępie do informacji publicznej,
5) Pani/Pana dane osobowe będą przechowywane, zgodnie z instrukcją kancelaryjną i jednolitym rzeczowym wykazem akt;
6) celem uzyskania Pani/Pana danych osobowych, bezpośrednio Pani/Pana dotyczących jest realizacja ustawowych zadań urzędu, ponieważ przetwarzanie jest niezbędne do wykonania zadania, które Administrator realizuje w interesie publicznym w ramach powierzonej władzy publicznej, a także do podjęcia czynności zmierzających do udzielenia niniejszego zamówienia oraz do zawarcia i wykonania umowy (podstawa art. 6 ust. 1 lit. b i lit. e RODO);
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO,
8) posiada Pani/Pan:
   a) na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
   b) na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych,
   c) 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,
   d) 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:
   a) w związku z art. 17 ust. 3 lit. b, d lub e RODO prawo do usunięcia danych osobowych,
   b) prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
   c) 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.

2. Zamawiający informuje, że:
   1) skorzystanie przez osobę, której dane osobowe dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 rozporządzenia 2016/679, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia ani zmianą postanowień umowy w sprawie zamówienia publicznego w zakresie niezgodnym z ustawą Prawo zamówień publicznych,
   2) wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 rozporządzenia 2016/679, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego,
   3) w przypadku, korzystania przez osobę, której dane osobowe są przetwarzane przez Zamawiającego, z uprawnienia, o których mowa w art. 15 ust. 1-3 rozporządzenia 2016/679, Zamawiający może żądać od osoby występującej z żądaniem dodatkowych informacji mających na celu sprecyzowanie nazwy lub daty zakończonego postępowania o udzielenie zamówienia publicznego.

**XX. Wykaz załączników**

1. Opis przedmiotu zamówienia – Załącznik nr 1
2. Projekt umowy – Załącznik nr 2
3. Oferta – Załącznik nr 3
4. Oświadczenie o braku podstaw do wykluczenia z postępowania oraz o spełnieniu warunków udziału w postępowaniu – Załącznik nr 4

Wicestarosta

Łukasz Wilkosz

Elektronicznie podpisany przez Łukasz Wilkosz
Data: 2023.05.22 15:06:39 +02'00'

**Załącznik nr 1**

# OPIS PRZEDMIOTU ZAMÓWIENIA

## I. URZĄDZENIE 1

### 1. Interfejsy, dysk, zasilanie

1) System realizujący funkcję Firewall musi dysponować minimum:
   a) 16 portami Gigabit Ethernet RJ-45.
   b) 8 gniazdami SFP 1 Gbps.
   c) 2 gniazdami SFP+ 10 Gbps.
   d) **Zamawiający wymaga dostarczenia 2 wkładek 10G SFP+ wielomodowych, duplex (LC) wytworzonych przez producenta oferowanego rozwiązania UTM**
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 dwa zasilania AC.

### 2. Parametry wydajnościowe

1) W zakresie Firewall'a obsługa nie mniej niż 1.5 mln. jednoczesnych połączeń oraz 56 tys. nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 18 Gbps dla pakietów 512 B.
3) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 64 B.
4) Przepustowość Stateful Firewall: nie mniej niż 20 Gbps dla pakietów 1518 B.
5) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 2.2 Gbps.
6) Wydajność szyfrowania IPSec VPN nie mniej niż 11 Gbps.
7) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 2.6 Gbps.
8) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus – minimum 1 Gbps.
9) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 1 Gbps.

### 3. 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 StatefulInspection.
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, Trafficshaping).
9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11) Analiza ruchu szyfrowanego protokołem SSL.
12) Analiza ruchu szyfrowanego protokołem SSH.

**4. 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:
   a) Translację jeden do jeden oraz jeden do wielu.
   b) 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.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Cisco ACI.
   d) Google Cloud Platform (GCP).
   e) Nuage Networks VSP.
   f) OpenStack.
   g) VMwarevCenter (ESXi).
   h) VMware NSX.

**5. 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 SafeSearch – przeciwdziałająca pojawieniu się niechcianych treści w wynikach wyszukiwarek takich jak: Google oraz Yahoo.
6) System musi umożliwiać zdefiniowanie czasu, który użytkownicy sieci mogą spędzać na stronach o określonej kategorii. Musi istnieć również możliwość określenia maksymalnej ilości danych, które użytkownik może pobrać ze stron o określonej kategorii.
7) Administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania.
8) W ramach systemu musi istnieć możliwość określenia, dla których kategorii url lub wskazanych ulr – system nie będzie dokonywał inspekcji szyfrowanej komunikacji.

## II. URZĄDZENIE 2

**1. Interfejsy, dysk, zasilanie**

1) System realizujący funkcję Firewall musi dysponować minimum 8 portami Gigabit Ethernet RJ-45 oraz minimum 2 portami współdzielonymi RJ-45/SFP.
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 20 interfejsów wirtualnych - definiowanych jako VLAN'y w oparciu o standard 802.1Q.
4) System musi być wyposażony w zasilanie AC.

**2. Parametry wydajnościowe**

1) W zakresie Firewall'a obsługa nie mniej niż 1,5 miliona jednoczesnych połączeń oraz 45 tys. nowych połączeń na sekundę.
2) Przepustowość Stateful Firewall: nie mniej niż 10 Gbps dla pakietów 512 B.

3) Przepustowość Firewall z włączoną funkcją Kontroli Aplikacji: nie mniej niż 1,8 Gbps.
4) Wydajność szyfrowania IPSec VPN nie mniej niż 6,5 Gbps.
5) Wydajność skanowania ruchu w celu ochrony przed atakami (zarówno clientside jak i serverside w ramach modułu IPS) dla ruchu Enterprise Traffic Mix - minimum 1,4 Gbps.
6) Wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami: IPS, Application Control, Antywirus - minimum 900 Mbps.
7) Wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http – minimum 715 Mbps.

**3. 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 StatefulInspection.
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, Trafficshaping).
9) Mechanizmy ochrony przed wyciekiem poufnej informacji (DLP).
10) Dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych. W ramach postępowania powinny zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego uwierzytelnienia administratorów lub w ramach połączeń VPN typu client-to-site.
11) Analiza ruchu szyfrowanego protokołem SSL także dla protokołu HTTP/2.
12) Funkcja lokalnego serwera DNS ze wsparciem dla DNS over TLS (DoT) oraz DNS over HTTPS (DoH) z możliwością filtrowania zapytań DNS na lokalnym serwerze DNS jak i w ruchu przechodzącym przez system.

**4. Polityka 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:

a) Translację jeden do jeden oraz jeden do wielu.
b) Dedykowany ALG (Application-Level Gateway) dla protokołu SIP.

3) W ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN.
4) Możliwość wykorzystania w polityce bezpieczeństwa zewnętrznych repozytoriów zawierających: kategorie url, adresy IP, nazwy domenowe, hash'e złośliwych plików.
5) 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.
   a) Amazon Web Services (AWS).
   b) Microsoft Azure
   c) Google Cloud Platform (GCP).
   d) OpenStack.
   e) VMware NSX.

**5. Funkcje SD-WAN**

1) System powinien umożliwiać wykorzystanie protokołów dynamicznego routingu przy konfiguracji równoważenia obciążenia do łączy WAN.

2) Reguły SD-WAN powinny umożliwiać określenie aplikacji jako argumentu dla kierowania ruchu.

**6. 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 SafeSearch – 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.

## III. ELEMENTY WSPÓLNE DLA OBU URZĄDZEŃ

**1. Wymagania ogólne**

Dostarczony system bezpieczeństwa musi zapewniać wszystkie wymienione poniżej funkcje sieciowe i bezpieczeństwa niezależnie od dostawcy łącza. Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej 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:

a) Firewall,
b) Ochrony w warstwie aplikacji,
c) Protokołów routingu dynamicznego.

**2. Redundancja, monitoring i wykrywanie awarii**

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

**3. Połączenia VPN**

1) System musi umożliwiać konfigurację połączeń typu IPSec VPN. W zakresie tej funkcji musi zapewniać:
   a) wsparcie dla IKE v1 oraz v2,
   b) obsługa szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/CounterMode(GCM),

c) obsługa protokołu Diffie-Hellman grup 19 i 20,
d) wsparcie dla Pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE,
e) tworzenie połączeń typu Site-to-Site oraz Client-to-Site,
f) monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności,
g) możliwość wyboru tunelu przez protokoły: dynamicznego routingu (np. OSPF) oraz routingu statycznego,
h) obsługa mechanizmów: IPSec NAT Traversal, DPD, Xauth,
i) Mmechanizm „Split tunneling" dla połączeń Client-to-Site.

2) System musi umożliwiać konfigurację połączeń typu SSL VPN. W zakresie tej funkcji musi zapewniać:
a) 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,
b) pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling" przy zastosowaniu dedykowanego klienta,
c) producent rozwiązania musi dostarczać oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPSec VPN lub SSL VPN.

**4. Routing i obsługa łączy WAN**

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

**5. Zarządzanie pasmem**

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

**6. Ochrona przed malware**

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

**7. 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.

**8. 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.

**9. Uwierzytelnianie użytkowników w ramach sesji**

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

**10. 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 dwuskładnikowego dla dostępu administracyjnego.
4) System musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow.
5) System musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację.
6) Element systemu pełniący funkcję Firewal musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall.
7) Element systemu realizujący funkcję firewall musi umożliwiać wykonanie szeregu zmian przez administratora w CLI lub GUI, które nie zostaną zaimplementowane zanim nie zostaną zatwierdzone.

**11. 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.

**12. Certyfikaty**

Poszczególne elementy oferowanego systemu bezpieczeństwa powinny posiadać certyfikacje ICSA lub EAL4 dla funkcji Firewall.

**13. Licencje**

W ramach postępowania powinny zostać dostarczone licencje upoważniające do korzystania z aktualnych baz funkcji ochronnych producenta i serwisów. Powinny one obejmować: 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 36 miesięcy.

**14. Warunki gwarancji**

1) Wykonawca udziela Zamawiającemu na przedmiot dostawy36 – miesięcznej gwarancji oraz rękojmi, liczonej od dnia podpisania protokołu odbioru.
2) Wykonawca zobowiązuje się w ramach gwarancji do napraw gwarancyjnych oraz usługi serwisowej dotyczących przedmiotu niniejszej umowy (z wyłączeniem licencji), które będą realizowane przez producenta sprzętu lub autoryzowany przez producenta podmiot.
3) Naprawa gwarancyjna będzie obejmować wymianę bądź naprawę urządzenia, które działa w sposób niewłaściwy z zastrzeżeniem, że Wykonawca odbierze urządzenie bez nośników pamięci, z siedziby Zamawiającego na własny koszt.
4) Zamawiający wymaga, aby naprawa urządzenianastąpiła w terminie do 14 dni kalendarzowych, od daty potwierdzenia zgłoszenia.
5) Zamawiający dopuszcza możliwość przedłużenia terminu naprawy określonego w ust. 4 o kolejne 14 dni z powodu trudności związanych z dostępem do elementów urządzenia podlegających wymianie. W takim przypadku Wykonawca zobowiązany jest poinformować o tym fakcie Zamawiającego niezwłocznie.
6) Usługa serwisowa dla każdego z urządzeń świadczona w ramach gwarancji będzie obejmować:
   a) dostarczenie urządzenia zastępczego w przypadku naprawy urządzenia poza siedzibą lub w siedzibie Zamawiającego w następnym dniu roboczym (NBD) liczonym od dnia potwierdzenia zasadności zgłoszeniaz zastrzeżeniem, że czas reakcji na zgłoszenie wynosi maksymalnie 1 godzinę, o takich samych parametrach na czas naprawy,
   b) usuwanie wszelkich nieprawidłowości oprogramowania wpływających na działanie urządzenia,
   c) dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7,
   d) pierwszą linię wsparcia w języku polskim w trybie 8x5.
7) Usługi serwisowe wymienione w ust. 14 pkt 6 lit a-d mają być świadczone przez okres 36 miesięcy.

**15. Pozostałe informacje**

1) Wymagania dotyczące wszystkich dostarczanych produktów:
   a) wszystkie elementy składowe produktów muszą być fabrycznie nowe nieużywane oraz nieeksploatowane na wystawach lub imprezach targowych, nie wycofane z produkcji, sprawne technicznie, bezpieczne, kompletne i gotowe do pracy, a także muszą spełniać wymagania techniczno-funkcjonalne wyszczególnione w opisie przedmiotu zamówienia,
   b) przedmiot zamówienia musi spełniać wszystkie wymogi dotyczące bezpieczeństwa obowiązujące w Polsce,

c) Zamawiający wymaga, aby każdy produkt dostarczony został w oryginalnym opakowaniu umożliwiającym jego identyfikację, bez konieczności naruszania opakowania. Uszkodzone i zniszczone opakowanie, upoważnia Zamawiającego do odmowy przyjęcia przedmiotu zamówienia.

2) Zamawiający jest obecnie w posiadaniu rozwiązań UTM FortiGate 100E o numerze seryjnym FG100ETK19037491 oraz FortiGate 80E o numerze seryjnym FGT80ETK19000176. Zakupione rozwiązania o parametrach zgodnych z poniższą specyfikacją mają zastąpić posiadane przez Zamawiającego urządzenia.

3) W przypadku wystąpienia w dokumentacji niniejszego postępowania opisów przedmiotu zamówienia, zawierających wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty dostarczane przez konkretnego Wykonawcę, w tym w szczególności jednoznacznych nazw urządzeń oraz oprogramowania i konkretnych typów katalogowych, wszystkie takie wskazania i nazwy każdorazowo należy czytać z klauzulą „lub równoważne" o takich samych lub nie gorszych parametrach technicznych, jakościowych, funkcjonalnych oraz estetycznych. Jeżeli w w/w dokumentach podano konkretne typy urządzeń i oprogramowania należy to traktować jako pomocnicze wskazanie minimalnego poziomu jakościowego (standardu).

**Załącznik nr 2**
**Projekt umowy**

**Umowa nr …….**

zawarta w dniu …… maja 2023 r. w Stargardzie pomiędzy:
Powiatem Stargardzkim z siedzibą w Stargardzie przy ul. Skarbowej 1, NIP 854-22-28-620, reprezentowanym przez:
.....
zwanym w dalszej części Umowy: „Zamawiającym”
a
.....
reprezentowanym przez:
.....
NIP: ……..REGON:……
zwanym, w dalszej części Umowy: „Wykonawcą”

łącznie zwanymi również Stronami

Umowa finansowana jest z funduszy przyznanych w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014 – 2020, Osi Priorytetowej V. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia REACT-EU, Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia dotycząca realizacji projektu grantowego „Cyfrowy Powiat”.

Wartość niniejszego zamówienia nie przekracza kwoty 130 000 zł, o której mowa w art. 2 ust. 1 pkt 1 ustawy – ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. z dnia 22 lipca 2022 r. (Dz.U. z 2022 r. poz. 1710 z późn. zm), w związku z tym do niniejszego postępowania stosuje się zasady określone w Wytycznych w zakresie kwalifikowalności wydatków w ramach Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego oraz Funduszu Spójności na lata 2014 – 2020.

**§1**

1. Przedmiotem umowy jest:
   a) dostawa dwóch urządzeń – zapór sieciowych wraz z licencjami w celu rozbudowy zabezpieczeń logicznych (firewall, systemy IDS, IPS),
   b) asysta przy konfiguracji dostarczonych urządzeń.

**§2**

1. Realizacja umowy nastąpi:
   1) w zakresie przedmiotu umowy określonego w §1ust. 1 pkt a w terminie do 20 czerwca 2023 r.,
   2) w zakresie przedmiotu umowy określonego w §1ust. 1pkt b w terminach 21–22 czerwca 2023 r.
2. Miejsce dostawy: siedziba Starostwa Powiatowego w Stargardzie, ul. Skarbowa 1, 73-110 Stargard. Przedmiot umowy zostanie dostarczony na koszt i ryzyko Wykonawcy.
3. Wykonawca dostarczy urządzenia fabrycznie nowe, kompletne, sprawne technicznie.
4. Urządzenia muszą spełniać wymagania techniczno-jakościowe, opisane w załączniku nr 1 do zaproszenia.
5. O terminie dostawy Wykonawca powiadomi Zamawiającego w formie elektronicznej e-mailem przynajmniej na jeden dzień przed terminem dostawy.
6. Dostawa będzie zrealizowana w dzień roboczy w godzinach 8-16.
7. Wykonanie dostawy potwierdzone zostanie podpisaniem protokołu odbioru, bez zastrzeżeń, potwierdzającego:
   1) dostarczenie urządzeń wraz z licencjami,
   2) dostarczenie haseł dla administratorów.

**§3**

1. Wykonawca udziela Zamawiającemu na przedmiot dostawy, o którym mowa w § 1 ust. 1 pkt a), 36 – miesięcznej gwarancji oraz rękojmi, liczonej od dnia podpisania protokołu odbioru.
2. Wykonawca zobowiązuje się w ramach gwarancji do napraw gwarancyjnych oraz usługi serwisowej dotyczących przedmiotu niniejszej umowy(z wyłączeniem licencji), które będą realizowane przez producenta sprzętu lub autoryzowany przez producenta podmiot.
3. Naprawa gwarancyjna będzie obejmować wymianę bądź naprawę urządzenia, które działa w sposób niewłaściwy z zastrzeżeniem, że Wykonawca odbierze urządzenie bez nośników pamięci, z siedziby Zamawiającego na własny koszt.
4. Zamawiający wymaga, aby naprawa urządzenia nastąpiła w terminie do 14 dni kalendarzowych, od daty potwierdzenia zgłoszenia.
5. Zamawiający dopuszcza możliwość przedłużenia terminu naprawy określonego w ust. 4 o kolejne 14 dni z powodu trudności związanych z dostępem do elementów urządzenia podlegających wymianie. W takim przypadku Wykonawca zobowiązany jest poinformować o tym fakcie Zamawiającego niezwłocznie.
6. Usługa serwisowa dla każdego z urządzeń świadczona w ramach gwarancji będzie obejmować:
   a) dostarczenie urządzenia zastępczego w przypadku konieczności naprawy urządzenia poza siedzibą lub w siedzibie Zamawiającego w następnym dniu roboczym (NBD) liczonym od dnia potwierdzenia zasadności zgłoszenia, z zastrzeżeniem, że czas reakcji na zgłoszenie wynosi maksymalnie 1 godzinę, o takich samych parametrach na czas naprawy,
   b) usuwanie wszelkich nieprawidłowości oprogramowania wpływających na prawidłowe działanie urządzenia,
   c) dostęp do aktualizacji oprogramowania oraz wsparcie techniczne w trybie 24x7,
   d) pierwszą linię wsparcia w języku polskim w trybie 8x5.
7. Usługi serwisowe wymienione w §3 ust. 6 pkt a-d mają być świadczone przez okres 36 miesięcy.

**§4**

1. Osobami wyznaczonymi do reprezentowania Zamawiającego w sprawach związanych z realizacją umowy będą: ……, tel.: ……, e-mail: …… oraz ……, tel.: ……, e-mail: ……
2. Osobami wyznaczonymi do kontaktów w sprawach związanych z realizacją umowy ze strony Wykonawcy będzie: ……, tel.: …… e-mail: ……
3. W związku z wykonywaniem niniejszej umowy Strony dopuszczają porozumiewanie się za pośrednictwem poczty elektronicznej za pośrednictwem adresów wskazanych w ust. 1 i 2.

**§5**

1. Zamawiający za prawidłowe wykonanie całości przedmiotu umowy określonego w § 1 zapłaci na rzecz Wykonawcy łączną kwotę …… zł netto (słownie: …… zł), powiększoną o wartość podatku VAT w wysokości ……., to jest brutto …… zł (słownie: ……..… zł), w tym za:
   1) urządzenie 1 – …….. (nazwa, model):
      a) cena brutto za urządzenie – …….. zł,
      b) cena brutto za licencję – …….. zł,
      c) cena brutto za usługę opisaną w §3 ust. 6 pkt d – …… zł
   2) urządzenie 2 – …….. (nazwa, model):
      a) cena brutto za urządzenie – …….. zł,
      b) cena brutto za licencję – …….. zł,
      c) cena brutto za usługę opisaną w §3 ust. 6 pkt d – …… zł
2. Łączna kwota brutto wynagrodzenia w ust. 1 zawiera wszystkie koszty związane z realizacją przedmiotu umowy, niezbędne do jego wykonania.
3. Płatność należności wynikającej z wystawionej faktury nastąpi przy zastosowaniu mechanizmu podzielonej płatności, o którym mowa w art. 108a ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j. Dz. U. z 2022 r. poz. 931 z późn. zm.).

4. Wykonawca oświadcza, że numer rachunku rozliczeniowego wskazany na fakturze, która będzie wystawiona w jego imieniu, jest rachunkiem, dla którego zgodnie z rozdziałem 3a ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439 z późn. zm.) prowadzony jest rachunek VAT.
5. Wykonawca wystawi fakturę w terminie do 7 dni od wykonania przedmiotu zamówienia, potwierdzonego podpisanym przez Zamawiającego protokołem odbioru.
6. Osobą upoważnioną do podpisania protokołu odbioru ze strony:
   1) Zamawiającego jest: …….
   2) Wykonawcy jest …….
7. Wynagrodzenie płatne będzie przelewem, na rachunek Wykonawcy, w terminie do 14 dni od otrzymania przez Zamawiającego prawidłowo wystawionej faktury.
8. Za datę zapłaty uznaje się dzień obciążenia rachunku Zleceniodawcy.
9. Dane do faktury:
   Nabywca: Powiat Stargardzki, ulica Skarbowa 1, 73-110 Stargard, NIP 854-22-28-620,
   Płatnik: Starostwo Powiatowe, ulica Skarbowa 1, 73-110 Stargard.

**§6**

1. Wykonawca zapłaci Zamawiającemu sumę kar umownych w przypadku zaistnienia następujących okoliczności:
   a) w wysokości 0,5% wartości wynagrodzenia, o którym mowa w §5 ust. 1 za każdy dzień opóźnienia dostawy licząc od terminu, o którym mowa w §2 ust. 1 pkt 1,
   b) w przypadku niedotrzymania terminu naprawy, określonego w §3 ust. 5 – w wysokości 0,5% wartości wynagrodzenia, o którym mowa w §5 ust. 1 za każdy dzień kalendarzowy opóźnienia,
   c) w przypadku niedotrzymania terminu dostawy urządzenia w następnym dniu roboczym, określonego w §3 ust. 6 pkt a – w wysokości 0,5% wartości wynagrodzenia, o którym mowa w §5 ust. 1 za każdy dzień kalendarzowy opóźnienia,
   d) w przypadku braku asysty przy konfiguracji, określonej w §1 pkt b – jednorazowo w wysokości 1% wartości wynagrodzenia, o którym mowa w §5 ust. 1,
   e) odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci karę umowną w wysokości 15% wynagrodzenia umownego brutto określonego §5 ust. 1.
2. Wykonawca wyraża zgodę na potrącenie kwoty kar umownych z należnego wynagrodzenia, o którym mowa w §5 ust. 1.
3. W przypadku zwłoki z zapłatą wynagrodzenia przez Zamawiającego, Wykonawca może naliczyć odsetki ustawowe za opóźnienie.
4. Zamawiający jest uprawniony do dochodzenia naprawienia szkody przewyższającej wartość naliczonych kar umownych do pełnej wysokości poniesionej szkody na zasadach ogólnych.
5. W przypadku niedostarczenia przedmiotu umowy w terminie z przyczyn zależnych od Wykonawcy Zamawiający może odstąpić od umowy poprzez złożenie oświadczenia na piśmie w ciągu 30 dni od upływu terminu dostarczenia, o którym mowa w §2 ust. 1 pkt 1.

**§7**

1. W ramach wynagrodzenia umownego określonego w treści § 5 Wykonawca udziela Zamawiającemu niezbędnych licencji pozwalających na wykorzystywanie oprogramowania wykorzystanego w celu wykonania przedmiotu umowy o którym mowa w § 1, a także pozwalającej na jego dalsze wykorzystywanie przez Zamawiającego w zakresie prowadzonej przez niego działalności.
2. Wykonawca ponosi w stosunku do Zamawiającego pełną odpowiedzialność za naruszenie praw autorskich jak i praw własności przemysłowej, w tym również za zapewnienie lub zapewnienie w niewłaściwym zakresie licencji o które mowa w ust. 1, o ile taki fakt miał związek z wykonywaniem przedmiotu umowy

**§ 8**

1. Zamawiający może odstąpić od niniejszej umowy w przypadkach przewidzianych w przepisach Kodeksu Cywilnego, a ponadto w razie wystąpienia przynajmniej jednej z następujących okoliczności:
   a) Wykonawca wykonuje przedmiot umowy wadliwie i pomimo wezwania przez Zamawiającego do zmiany sposoby wykonywania umowy nie zastosował się do złożonego wezwania,
   b) W przypadku niedostarczenia przedmiotu umowy w terminie z przyczyn zależnych od Wykonawcy Zamawiający może odstąpić od umowy poprzez złożenie oświadczenia na piśmie w ciągu 30 dni od upływu terminu dostarczenia, w którym mowa w §2 ust. 1 pkt 1
2. Odstąpienie od umowy przez Zamawiającego z przyczyn o których mowa w ust 1 i ust. punk a i b uznaje się za odstąpienie od umowy z przyczyn zależnych wyłącznie od Wykonawcy.
3. Zamawiający może złożyć oświadczenie w przedmiocie odstąpienia od umowy w terminie 21 dni licząc od dnia kiedy uzyskał informację o okolicznościach uzasadniających złożenia takiego oświadczenia.
4. W przypadku odstąpienia od umowy, gdy części przedmiotu umowy jest wykonana przez Wykonawcę, Zamawiający może według swojego wyboru te część zatrzymać płacąc odpowiednią część wynagrodzenia na rzecz Wykonawcy albo całość zawrócić Wykonawcy.

**§ 9**

1. Wszelkie zmiany niniejszej umowy wymagają formy pisemnej, pod rygorem nieważności.
2. W sprawach nieuregulowanych w umowie zastosowanie mają przepisy Kodeksu Cywilnego.
3. Spory wynikłe z realizacji niniejszej umowy rozstrzygane będą przez Sąd właściwy dla siedziby Zamawiającego.
4. Adresy Stron podane w niniejszej umowie są równocześnie adresami dla korespondencji. Strony powiadomią się wzajemnie o każdorazowej zmianie adresu pod rygorem uznania, że korespondencja skierowana pod ten adres została skutecznie doręczona.

**§ 10**

1. Integralną częścią Umowy są załączniki do Umowy, wymienione w ust. 2 pkt a-c
2. Dla celów interpretacji będą miały pierwszeństwo dokumenty zgodnie z następującą kolejnością:
   a) Umowa,
   b) Zaproszenie do składania ofert,
   c) Oferta Wykonawcy wraz z załącznikami stanowiącymi jej integralną część.

**§ 11**

Umowa została sporządzona w 3 jednobrzmiących egzemplarzach, z których jeden otrzymuje Wykonawca a dwa Zamawiający.

..... .....

Zamawiający Wykonawca

**Załącznik nr 3**

……..., dnia …..... 2023 r.

## Oferta

Ja (my), niżej podpisany(i)
….....
.....
.....
.....
działając w imieniu i na rzecz
nazwa firmy….....
siedziba ….....
adres e-mail: …….……
tel/fax ….....

W odpowiedzi na zaproszenie do składania ofert na **dostawę dwóch zapór sieciowych wraz z licencjami** składam(y) niniejszą ofertę i oferuję(my):

1. **łączną cenę za realizację przedmiotu zamówienia w wysokości …… zł netto** (słownie: ……..……..……..), co po powiększeniu o należny podatek VAT, w wysokości …….%, tj.……..…… zł, daje kwotę **……..... zł brutto** (słownie: ……..), w tym:
   1) za urządzenie 1 – …….. (producent, nazwa, model):
      a) cena brutto za urządzenie – …….. zł,
      b) cena brutto za licencję – …….. zł,
      c) cena brutto za usługę (pierwsza linia wsparcia w języku polskim (8x5) – …… zł.
   2) za urządzenie 2 – …….. (producent, nazwa, model):
      a) cena brutto za urządzenie – …….. zł,
      b) cena brutto za licencję – …….. zł,
      c) cena brutto za usługę (pierwsza linia wsparcia w języku polskim (8x5) – …… zł.
2. Zobowiązuję(my) się do udzielenia 36 miesięcznej gwarancji.
3. Zobowiązuję(my) się do realizacji przedmiotu zamówienia w terminie do 22 czerwca 2023 r.
4. Oświadczam(y), że osoby wyznaczone do realizacji przedmiotu zamówienia, wskazane poniżej, posiadają odpowiednie kwalifikacje i kompetencje określone w Dziale V ust. 1 pkt 2 lit. b:
   1) Imię i nazwisko ……, oznaczenie certyfikatu ……
   2) Imię i nazwisko ……, oznaczenie certyfikatu ……
5. Oświadczam(y), że zapoznaliśmy się z treścią zaproszenia do składania ofert i uznajemy się za związanych określonymi w nim wymaganiami i zasadami postępowania oraz że uzyskaliśmy wszelkie niezbędne informacje do przygotowania oferty.
6. Oświadczam(y), że *Projekt umowy* (Załącznik Nr 2) został przez nas zaakceptowany i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na warunkach w nim określonych.
7. Oświadczam(y), że uważamy się za związanych niniejszą ofertą przez okres 30 dni od daty wyznaczonej na składanie ofert.
8. Oświadczam(y), że: (niepotrzebne skreślić)
   ☐ oferta nie zawiera informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji.

□ oferta zawiera informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji. Informacje takie zawarte są w następujących dokumentach: ….....….....

Dokumenty/ informacje te stanowią tajemnicę przedsiębiorstwa, bowiem: ……

10. Na podstawie art. 6 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r., wyrażam zgodę na przetwarzanie moich danych osobowych przez administratora danych Powiat Stargardzki z siedzibą w Stargardzie, ul. Skarbowej 1, REGON 811684210, NIP 854-22-28-620w celu przeprowadzenia postępowania i wyboru najkorzystniejszej oferty, podaję dane osobowe dobrowolnie i oświadczam, że są one zgodne z prawdą.
11. Oświadczam(y), że zapoznaliśmy się z **Klauzulą Informacyjną** wynikającą z art. 13 RODO, zawartą w Dziale XIX zaproszenia oraz że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.

**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)**

12. Załącznikami do niniejszej oferty są:

1….....

2….....

3….....

4….....

5….....

_____

podpis osoby /osób/ upoważnionej

**Załącznik nr 4**

**Oświadczenie o braku podstaw do wykluczenia z postępowania oraz o spełnieniu warunków udziału w postępowaniu**

Ja (my), niżej podpisany(i)
.....
.....
.....
*(imię i nazwisko, stanowisko/podstawa do reprezentacji)*
działając w imieniu i na rzecz
.....
.....
*(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

Na potrzeby postępowania o udzielenie zamówienia na dostawę dwóch zapór sieciowych wraz z licencjami, oświadczam, co następuje:

☐ Oświadczam, że spełniam warunki udziału w postępowaniu określone przez Zamawiającego w Dziale V pkt 1 ppkt 2 lit. a-b zaproszenia do składania ofert.

……
*(data, podpis)*

☐ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie przesłanek określonych w Dziale V pkt 2 ppkt 1-9 zaproszenia do składania ofert.

……
*(data, podpis)*

☐ Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie przesłanek określonych w Dziale V pkt 2 ppkt 1-9, tj. ……..
*(podać mającą zastosowanie podstawę wykluczenia spośród wymienionych w Dziale V pkt 2 ppkt 1-9)*

……
*(data, podpis)*

**OŚWIADCZENIE DOTYCZĄCE PODANYCH INFORMACJI:**

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

……
*(data, podpis)*