SPECYFIKACJA WARUNKÓW ZAMÓWIENIA W POSTĘPOWANIU NA: **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”**

OR.272.10.2024.X

ZAMAWIAJĄCY:

Powiat Bytowski
ul. Ks. dr. Bolesława Domańskiego 2
77-100 Bytów

ZAMÓWIENIE OBEJMUJE:

32420000-3 - Urządzenia sieciowe
32422000-7 - Elementy składowe sieci
32510000-1 - Bezprzewodowy system telekomunikacyjny

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w oparciu o przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (tj. Dz. U. z 2024 poz. 1320 z późn. zm.), zwanej dalej ustawą Pzp.

Bytów, 05.12.2024 r.

SPIS TREŚCI:

I. NAZWA ORAZ ADRES ZAMAWIAJĄCEGO

Powiat Bytowski reprezentowany przez Zarząd Powiatu występujący w imieniu własnym z siedzibą przy ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów
NIP: 842 164 30 30
tel. 59 822 80 00
fax 59 822 80 01
Adres poczty elektronicznej: starostwo@powiatbytowski.pl
Adres strony internetowej Zamawiającego: powiatbytowski.pl
Adres strony internetowej prowadzonego postępowania: https://platformazakupowa.pl/

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 postępowaniem o udzielenie zamówienia będą udostępniane na stronie internetowej: **https://platformazakupowa.pl/**; **http://bip.powiatbytowski.pl/.**

III. TRYB UDZIELENIA ZAMÓWIENIA

Postępowanie o udzielenie zamówienia publicznego prowadzone jest w trybie podstawowym, na podstawie **art. 275 pkt 2** ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320 z późn. zm.) [zwanej dalej także „ustawa Pzp”].

IV. INFORMACJA, CZY ZAMAWIAJĄCY PRZEWIDUJE WYBÓR NAJKORZYSTNIEJSZEJ OFERTY Z MOŻLIWOŚCIĄ PROWADZENIA NEGOCJACJI

1. Zamawiający przewiduje wybór najkorzystniejszej oferty z możliwością prowadzenia negocjacji.
2. Negocjacje treści ofert:
1) nie mogą prowadzić do zmiany treści SWZ;
2) dotyczą wyłącznie tych elementów treści ofert, które podlegają ocenie w ramach kryteriów oceny ofert;
3) mają charakter poufny.
3. W przypadku skorzystania przez Zamawiającego z możliwości prowadzenia negocjacji:
1) może on zaprosić jednocześnie Wykonawców do negocjacji ofert złożonych w odpowiedzi na ogłoszenie o zamówieniu, jeżeli nie podlegały one odrzuceniu (przy czym Wykonawcy nie mają obowiązku uczestniczenia w negocjacjach);
2) w zaproszeniu do negocjacji wskazuje miejsce, termin i sposób prowadzenia negocjacji, a także kryteria oceny ofert, w ramach których będą prowadzone negocjacje w celu ulepszenia treści ofert;
3) informuje on równocześnie wszystkich Wykonawców, których oferty złożone w odpowiedzi na ogłoszenie o zamówieniu nie zostały odrzucone, o zakończeniu negocjacji oraz zaprasza ich do składania ofert dodatkowych (przy czym Wykonawcy nie mają obowiązku składania ofert dodatkowych).

4.Wykonawca może złożyć ofertę dodatkową, która zawiera nowe propozycje w zakresie treści oferty podlegających ocenie w ramach kryteriów oceny ofert wskazanych przez Zamawiającego w zaproszeniu do negocjacji.
5.Oferta dodatkowa nie może być mniej korzystna w żadnym z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu.
6.Oferta przestaje wiązać Wykonawcę w zakresie, w jakim złoży on ofertę dodatkową zawierającą korzystniejsze propozycje w ramach każdego z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji.
7.Oferta dodatkowa, która jest mniej korzystna w którymkolwiek z kryteriów oceny ofert wskazanych w zaproszeniu do negocjacji niż oferta złożona w odpowiedzi na ogłoszenie o zamówieniu, podlega odrzuceniu.
8. Wzór Formularza oferty dodatkowej stanowi **załącznik nr 5 do SWZ**.
9.Zamawiający nie przewiduje możliwości ograniczenia liczby wykonawców, których zaprosi do negocjacji ofert.
10.W przypadku, gdy Zamawiający nie prowadzi negocjacji, dokonuje wyboru najkorzystniejszej oferty spośród niepodlegających odrzuceniu ofert złożonych w odpowiedzi na ogłoszenie o zamówieniu.
11.Wymagania dotyczące sporządzania i przekazywania oferty określone w niniejszej SWZ mają odpowiednie zastosowanie do oferty dodatkowej.

V. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest dostawa sprzętu informatycznego w ramach konkursu grantowego „Cyberbezpieczny Samorząd".
Zakres rzeczowy zamówienia:
1) UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv - 1 kpl.
2) Sprzętowy appliance zapewniający szyfrowany kanał komunikacji – 1 szt.
3) Przełącznik sieciowy zarządzalny 48-portowy - 5 szt.
4) Przełącznik sieciowy zarządzalny 24-portowy - 3 szt.
5) Przełącznik sieciowy zarządzalny 24-portowy PoE – 1 szt.
6) Przełącznik sieciowy zarządzalny 8-portowy – 4 szt.
7) Punkt dostępowy AP – 6 szt.

2. Opis przedmiotu zamówienia za pomocą kodów CPV Wspólnego Słownika Zamówień:
32420000-3 - Urządzenia sieciowe,
32422000-7 - Elementy składowe sieci,
32510000-1 - Bezprzewodowy system telekomunikacyjny.

3. Szczegółowy opis przedmiotu zamówienia znajduje się w **załączniku nr 1 SWZ.**

ROZWIĄZANIA RÓWNOWAŻNE DLA ZAMÓWIENIA

1. Nazwy własne zawarte w dokumentacji są przykładowe. W przypadku wystąpienia w dokumentacji nazw własnych Zamawiający dopuszcza zastosowanie materiałów i produktów równoważnych pod warunkiem, że zaproponowane materiały i produkty będą odpowiadały pod względem parametrów

równoważności materiałom i produktom wskazanym przez Zamawiającego. W przypadku zaoferowania materiałów lub produktów równoważnych Wykonawca, zobowiązany jest złożyć wraz z ofertą opis materiałów i produktów równoważnych oraz wykazać, że spełniają one wymagania określone przez Zamawiającego.
2. W przypadku użycia w SWZ lub w załącznikach do SWZ odniesienia do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, o których mowa w art. 101 ust. 1 pkt 2 oraz ust. 3 ustawy Pzp, Zamawiający dopuszcza rozwiązania równoważne opisywanym. W przypadku zaoferowania rozwiązań równoważnych Wykonawca zobowiązany jest złożyć wraz z ofertą rozwiązań równoważnych oraz wykazać, że spełniają one wymagania określone przez Zamawiającego. Ilekroć w opisie przedmiotu zamówienia występują odniesienia do norm, europejskich ocen technicznych, specyfikacji technicznych i systemów referencji technicznych dodaje się po ich brzmieniu zwrot „lub równoważne".
3. W przypadku gdy w SWZ lub załącznikach zostały użyte znaki towarowe, oznacza to, że są podane przykładowo i określają jedynie minimalne oczekiwane parametry jakościowe oraz wymagany standard. Wykonawca może zastosować materiały lub urządzenia równoważne, lecz o parametrach technicznych i jakościowych podobnych lub lepszych, których zastosowanie w żaden sposób nie wpłynie na prawidłowe funkcjonowanie rozwiązań przyjętych w dokumentacji projektowej. Wykonawca, który zastosuje urządzenia lub materiały równoważne będzie obowiązany wykazać że zastosowane przez niego urządzenia i materiały spełniają wymagania określone przez Zamawiającego.

VI. OPIS CZĘŚCI ZAMÓWIENIA, JEŻELI ZAMAWIAJĄCY DOPUSZCZA SKŁADANIE OFERT CZĘŚCIOWYCH

1. Zamawiający nie dopuszcza możliwości składania ofert częściowych.
2. Powody niedokonania podziału zamówienia na części:

W ramach niniejszego zamówienia Zamawiający nie dokonał podziału zamówienia na części, ponieważ przedmiotem zamówienia jest dostawa podobnego asortymentu. Zamówienie dostępne jest dla małych i średnich przedsiębiorstw. Ponadto dostawy sprzętu objęte konkursem grantowym „Cyberbezpieczny Samorząd" zostały podzielone na części i każda z części stanowi przedmiot odrębnego postępowania.

VII. PODWYKONAWSTWO

1. Wykonawca może powierzyć wykonanie części zamówienia podwykonawcy (podwykonawcom).
2. Zamawiający nie zastrzega obowiązku osobistego wykonania przez Wykonawcę kluczowych części zamówienia.
3. Zamawiający wymaga, aby w przypadku powierzenia części zamówienia podwykonawcom, Wykonawca wskazał w ofercie części zamówienia, których wykonanie zamierza powierzyć podwykonawcom oraz podał (o ile są mu wiadome na tym etapie) nazwy (firmy) tych podwykonawców.

VIII. TERMIN WYKONANIA ZAMÓWIENIA

Wykonawca zobowiązany jest zrealizować przedmiot zamówienia w terminie **do 45 dni kalendarzowych od dnia zawarcia umowy.**

IX. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO TREŚCI TEJ UMOWY

1. Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy, określone zostały w **załączniku nr 6 do SWZ**.
2. Szczegółowe informacje dotyczące zmiany umowy bez konieczności przeprowadzania nowego postępowania o udzielenie zamówienia, zostały przewidziane w § 7 projektowanych postanowień umowy stanowiących **załącznik nr 6 do SWZ**.

X. WYMAGANIA DOTYCZĄCE WADIUM

1. **Wykonawca zobowiązany jest do wniesienia wadium w wysokości 2 000,00 złotych** (słownie: dwa tysiące złotych 00/100);
2. Wadium wnosi się przed upływem terminu składania ofert 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 Pzp.
3. Przedłużenie terminu związania ofertą jest dopuszczalne tylko z jednoczesnym przedłużeniem okresu ważności wadium albo, jeżeli nie jest to możliwe, z wniesieniem nowego wadium na przedłużony okres związania ofertą.
4. 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 dnia 9 listopada 2000 r. o utworzeniu Polskiej Agencji Rozwoju Przedsiębiorczości (t.j. Dz. U. z 2024 r. poz. 419).
5. Wadium wnoszone w pieniądzu wpłaca się na następujący numer rachunku bankowego:

Powiat Bytowski, ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów

PKO BP SA Oddział Bytów

Numer rachunku bankowego: 03 1020 4708 0000 7202 0004 4453

Tytułem: Wadium –„ DOSTAWA SPRZĘTU – CYBERBEZPIECZNY SAMORZĄD ”

6. O skuteczności wniesienia przelewem kwoty wadium decydować będzie data wpływu środków na rachunek bankowy Zamawiającego wskazany w powyższym ust. 5.
7. Jeżeli wadium jest wnoszone w formie gwarancji lub poręczenia, Wykonawca przekazuje Zamawiającemu oryginał gwarancji lub poręczenia, w postaci elektronicznej.
8. W przypadku, gdy Wykonawca wnosi wadium w formie gwarancji bankowej lub gwarancji ubezpieczeniowej albo poręczenia, z treści tych dokumentów musi w szczególności jednoznacznie wynikać zobowiązanie gwaranta (banku, ubezpieczyciela, poręczyciela) do zapłaty całej kwoty wadium nieodwołalnie i bezwarunkowo na pierwsze żądanie Zamawiającego (beneficjenta).
9. Zamawiający zwraca wadium niezwłocznie, nie później jednak niż w terminie 7 dni od dnia wystąpienia jednej z okoliczności:

1) upływu terminu związania ofertą;
2) zawarcia umowy w sprawie zamówienia publicznego;
3) unieważnienia postępowania o udzielenie zamówienia, z wyjątkiem sytuacji gdy nie zostało rozstrzygnięte odwołanie na czynność unieważnienia albo nie upłynął termin do jego wniesienia.
10. Zamawiający, niezwłocznie, nie później jednak niż w terminie 7 dni od dnia złożenia wniosku zwraca wadium Wykonawcy:
1) który wycofał ofertę przed upływem terminu składania ofert;
2) którego oferta została odrzucona;
3) po wyborze najkorzystniejszej oferty, z wyjątkiem Wykonawcy, którego oferta została wybrana jako najkorzystniejsza;
4) po unieważnieniu postępowania, w przypadku gdy nie zostało rozstrzygnięte odwołanie na czynność unieważnienia albo nie upłynął termin do jego wniesienia.
11. Zamawiający zwraca wadium wniesione w pieniądzu wraz z odsetkami wynikającymi z umowy rachunku bankowego, na którym było ono przechowywane, pomniejszone o koszty prowadzenia rachunku bankowego oraz prowizji bankowej za przelew pieniędzy na rachunek bankowy wskazany przez Wykonawcę.
12. Zamawiający zwraca wadium wniesione w innej formie niż w pieniądzu poprzez złożenie gwarantowi lub poręczycielowi oświadczenia o zwolnieniu wadium.
13. Zamawiający zatrzymuje wadium wraz z odsetkami, a w przypadku wadium wniesionego w formie gwarancji lub poręczenia o których mowa w art. 97 ust. 7 pkt 2-4 ustawy Pzp, występuje odpowiednio do gwaranta lub poręczyciela z żądaniem zapłaty wadium, jeżeli:
1) Wykonawca w odpowiedzi na wezwanie, o którym mowa w art. 107 ust. 2 lub art. 128 ust. 1 ustawy Pzp, z przyczyn leżących po jego stronie, nie złożył podmiotowych środków dowodowych lub przedmiotowych środków dowodowych potwierdzających okoliczności, o których mowa w art. 57 lub art. 106 ust. 1 ustawy Pzp, oświadczenia, o którym mowa w art. 125 ust. 1 ustawy Pzp, innych dokumentów lub oświadczeń lub nie wyraził zgody na poprawienie omyłki, o której mowa w art. 223 ust. 2 pkt 3 ustawy Pzp, co spowodowało brak możliwości wybrania oferty złożonej przez Wykonawcę jako najkorzystniejszej;
2) Wykonawca, którego oferta została wybrana odmówił podpisania umowy w sprawie zamówienia publicznego na warunkach określonych w ofercie;
3) zawarcie umowy w sprawie zamówienia publicznego stało się niemożliwe z przyczyn leżących po stronie Wykonawcy, którego oferta została wybrana.
Uwaga: Nie wniesienie wadium w wymaganym terminie oraz w wymaganej wysokości i formie skutkuje odrzuceniem Wykonawcy z postępowania na podstawie art. 226 ust. 1 pkt 14 ustawy Pzp.

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

Postępowanie prowadzone jest w języku polskim za pośrednictwem **platformazakupowa.pl** pod

adresem: **https://platformazakupowa.pl/transakcja/1029644**

1. W postępowaniu o udzielenie zamówienia komunikacja między Zamawiającym a Wykonawcami odbywa się drogą elektroniczną za pośrednictwem platformazakupowa.pl .
2. Zamawiający informuje, że instrukcje korzystania z platformazakupowa.pl dotyczące w szczególności logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz innych czynności podejmowanych w niniejszym postępowaniu przy użyciu platformazakupowa.pl znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje
a) W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między Zamawiającym a Wykonawcami w zakresie:
- przesyłania Zamawiającemu pytań do treści SWZ;
- przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia podmiotowych środków dowodowych;
- przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
- przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
- przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dot. treści przedmiotowych środków dowodowych;
- przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy - Prawo zamówień publicznych;
- przesyłania wniosków, informacji, oświadczeń Wykonawcy;
- przesyłania odwołania/inne;
odbywa się za pośrednictwem platformazakupowa.pl i formularza „Wyślij wiadomość do zamawiającego".
Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem platformazakupowa.pl poprzez kliknięcie przycisku „Wyślij wiadomość do zamawiającego" po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.
b) Zamawiający będzie przekazywał Wykonawcom informacje za pośrednictwem platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający będzie zamieszczał na platformie w sekcji „Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana za pośrednictwem platformazakupowa.pl do konkretnego Wykonawcy.
c) Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na platformazakupowa.pl przesłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.
d) Zamawiający, zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla

dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r. poz. 2452), określa niezbędne wymagania sprzętowo - aplikacyjne umożliwiające pracę na platformazakupowa.pl, tj.:
- stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
- komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych - MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje,
- zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer,
- włączona obsługa JavaScript,
- zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
- szyfrowanie na platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.
- oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany wg. czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

e) Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
- akceptuje warunki korzystania z platformazakupowa.pl określone w Regulaminie zamieszczonym na stronie internetowej pod linkiem w zakładce „Regulamin" oraz uznaje go za wiążący,
- zapoznał i stosuje się do Instrukcji składania ofert/wniosków,

f) Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z Instrukcją korzystania z platformazakupowa.pl, w szczególności za sytuację, gdy Zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu, ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy Pzp.

Zalecenia:

Formaty plików wykorzystywanych przez Wykonawców powinny być zgodne z „OBWIESZCZENIEM PREZESA RADY MINISTRÓW z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych".

1) Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf

2) W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego z formatów: .zip lub .7Z

3) Wśród formatów powszechnych a nie występujących w rozporządzeniu występują : .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.

4) Zamawiający zwraca uwagę na ograniczenia wielkości plików podpisywanych profilem zaufanym, który wynosi max 10MB, oraz na ograniczenie wielkości plików podpisywanych w aplikacji eDoApp służącej do składania podpisu osobistego, który wynosi max 5MB.

5) Ze względu na niskie ryzyko naruszenia integralności pliku oraz łatwiejszą weryfikację podpisu, Zamawiający zaleca, w miarę możliwości, przekonwertowanie plików składających się na ofertę na format .pdf i opatrzenie ich podpisem kwalifikowanym PAdES.

6) Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.
7) Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju. Podpisywanie różnymi rodzajami podpisów np. osobistym i kwalifikowanym może doprowadzić do problemów w weryfikacji plików.
8) Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.
9) Zaleca się, aby komunikacja z Wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza „Wyślij wiadomość do zamawiającego", nie za pośrednictwem adresu email.
10) Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.
11) Ofertę należy przygotować z należytą starannością dla podmiotu ubiegającego się o udzielenie zamówienia publicznego i zachowaniem odpowiedniego odstępu czasu do zakończenia przyjmowania ofert/wniosków. Sugerujemy złożenie oferty na 24 godziny przed terminem składania ofert/wniosków.
12) Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.
13) Jeśli Wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.
14) Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.
15) Zamawiający zaleca aby nie wprowadzać jakichkolwiek zmian w plikach po podpisaniu ich podpisem kwalifikowanym. Może to skutkować naruszeniem integralności plików co równoważne będzie z koniecznością odrzucenia oferty w postępowaniu.
3. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.
4. Dokumenty elektroniczne (inne niż oferta oraz załączniki do oferty) oraz cyfrowe odwzorowania dokumentów składane są przez Wykonawcę za pośrednictwem Formularza do komunikacji jako załączniki. Zamawiający dopuszcza również możliwość składania w/w dokumentów elektronicznych oraz cyfrowych odwzorowań dokumentów za pomocą poczty elektronicznej, na adres email: przetargi@powiatbytowski.pl. Datą ich przesłania będzie potwierdzenie dostarczenia wiadomości zawierającej dokument/informację z serwera pocztowego Zamawiającego.
5. Ofertę, oświadczenie o którym mowa w art. 125 ustawy Pzp, o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu (dalej „Oświadczenie"), składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
6. Oferty, Oświadczenia, podmiotowe środki dowodowe, zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, pełnomocnictwo, informacje oraz inne dokumenty przekazywane w postępowaniu sporządza się w postaci elektronicznej, w formatach danych określonych w przepisach wydanych na podstawie art. 18 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (t.j. Dz. U. z 2024 r. poz. 307), z zastrzeżeniem formatów, o których mowa w art. 66 ust. 1 ustawy Pzp, z uwzględnieniem rodzaju przekazywanych danych.
7. Dokumenty elektroniczne przekazuje się w postępowaniu przy użyciu środków komunikacji elektronicznej wskazanych przez Zamawiającego w rozdziale XI ust. 1 SWZ.

8. W przypadku gdy dokumenty elektroniczne w postępowaniu, przekazywane przy użyciu środków komunikacji elektronicznej, zawierają informacje stanowiące tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2022 r. poz. 1233), Wykonawca, w celu utrzymania w poufności tych informacji, przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
9. Podmiotowe środki dowodowe, przedmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski.
10. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania odpowiednio Wykonawcy, Wykonawców wspólnie ubiegających się o udzielenie zamówienia publicznego, podmiotu udostępniającego zasoby na zasadach określonych w art. 118 ustawy Pzp lub Podwykonawcy niebędącego podmiotem udostępniającym zasoby na takich zasadach, zwane dalej „dokumentami potwierdzającymi umocowanie do reprezentowania", zostały wystawione przez upoważnione podmioty inne niż Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub Podwykonawca, przekazuje się je jako dokument elektroniczny.
11. W przypadku gdy podmiotowe środki dowodowe, przedmiotowe środki dowodowe, inne dokumenty lub dokumenty potwierdzające umocowanie do reprezentowania, zostały wystawione przez upoważnione podmioty jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
12. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w powyższym ust. 11. dokonuje w przypadku:
- podmiotowych środków dowodowych oraz dokumentów potwierdzających umocowanie do reprezentowania - odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub Podwykonawca, w zakresie podmiotowych środków dowodowych lub dokumentów potwierdzających umocowanie do reprezentowania, które każdego z nich dotyczą;
- przedmiotowych środków dowodowych - odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
- innych dokumentów - odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia, w zakresie dokumentów, które każdego z nich dotyczą.
13. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w powyższym ust. 12 może dokonać również notariusz.
14. Przez cyfrowe odwzorowanie, należy rozumieć dokument elektroniczny będący kopią elektroniczną treści zapisanej w postaci papierowej, umożliwiający zapoznanie się z tą treścią i jej zrozumienie, bez konieczności bezpośredniego dostępu do oryginału.
15. Podmiotowe środki dowodowe oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty, oraz pełnomocnictwo przekazuje się w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
16. W przypadku gdy podmiotowe środki dowodowe oraz zobowiązanie podmiotu udostępniającego zasoby, przedmiotowe środki dowodowe, niewystawione przez upoważnione podmioty lub

pełnomocnictwo, zostały sporządzone jako dokument w postaci papierowej i opatrzone własnoręcznym podpisem, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej.
17. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w powyższym ust. 16 dokonuje w przypadku:
- podmiotowych środków dowodowych - odpowiednio Wykonawca, Wykonawca wspólnie ubiegający się o udzielenie zamówienia, podmiot udostępniający zasoby lub Podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
- przedmiotowego środka dowodowego, zobowiązania podmiotu udostępniającego zasoby - odpowiednio Wykonawca lub Wykonawca wspólnie ubiegający się o udzielenie zamówienia;
- pełnomocnictwa - mocodawca.
18. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, o którym mowa w powyższym ust. 17 może dokonać również notariusz.
19. W przypadku przekazywania w postępowaniu dokumentu elektronicznego w formacie poddającym dane kompresji, opatrzenie pliku zawierającego skompresowane dokumenty kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, jest równoznaczne z opatrzeniem wszystkich dokumentów zawartych w tym pliku odpowiednio kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
20. Sposób sporządzenia dokumentów elektronicznych, cyfrowych odwzorowań dokumentów oraz informacji 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).
21. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ.
22. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 2 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynął do Zamawiającego nie później niż na 4 dni przed upływem terminu składania ofert.
23. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie, o którym mowa w ust. 22, przedłuża termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych Wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia ofert.
24. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynął w terminie, o którym mowa w ust. 22, Zamawiający nie ma obowiązku udzielania wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
25. Przedłużenie terminu składania ofert, o którym mowa w ust. 23, nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
26. Zamawiający nie przewiduje innego sposobu komunikowania się z Wykonawcami niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

XII. WSKAZANIE OSÓB UPRAWNIONYCH DO KOMUNIKOWANIA SIĘ Z WYKONAWCAMI

Zamawiający wyznacza następujące osoby do kontaktu z Wykonawcami:

Kazimierz Cuppa – w zakresie przedmiotu zamówienia – Starostwo Powiatowe w Bytowie, Wydział Organizacyjno - Prawny, ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów, tel. (59)822 80 06
Renata Murglin, Monika Taraszewicz – w zakresie formalno-prawnym – Starostwo Powiatowe w Bytowie, Wydział Organizacyjno-Prawny, ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów, tel. (59)822 80 06

Kontakt z ww. osobami możliwy jest od poniedziałku do piątku w godz. 8.00-15.00.

XIII. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą od dnia upływu terminu składania ofert **do dnia 11.01.2025 r.**, przy czym pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą określonego w SWZ, Zamawiający przed upływem terminu związania ofertą zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XIV. OPIS SPOSOBU PRZYGOTOWANIA OFERTY

1. Oferta musi być przygotowana i złożona zgodnie z treścią formularza, który stanowi **załącznik nr 2 do SWZ**. Oferta powinna zawierać wszystkie wymagane oświadczenia i załączniki, o których mowa w SWZ.
2. Zamawiający zaleca wykorzystanie formularzy stanowiących załączniki do specyfikacji. Dopuszcza się dołączenie do oferty załączników opracowanych przez Wykonawcę, pod warunkiem, że ich treść będzie zgodna z formularzami opracowanymi przez Zamawiającego.
3. Oferta musi być podpisana przez osoby wskazane w dokumencie upoważniającym do występowania w obrocie prawnym lub posiadające stosowne pełnomocnictwo. Jeżeli osoba (osoby) podpisująca ofertę (reprezentująca Wykonawcę lub Wykonawców występujących wspólnie) działa na podstawie pełnomocnictwa, pełnomocnictwo to w formie oryginału lub notarialnie potwierdzonej kopii musi zostać dołączone do oferty.
4. Ofertę, Oświadczenia, podmiotowe środki dowodowe, przedmiotowe środki dowodowe, pełnomocnictwo, inne dokumenty składane elektronicznie muszą zostać podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, Wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo Podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.

5. Oferta powinna być:
- sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
- złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem platformazakupowa.pl,
- podpisana kwalifikowanym podpisem elektronicznym lub podpisem zaufanym lub podpisem osobistym przez osobę/osoby upoważnioną/upoważnione.

6. Podpisy kwalifikowane wykorzystywane przez Wykonawców do podpisywania wszelkich plików muszą spełniać wymogi „Rozporządzenia Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014.

7. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny Zamawiający wymaga dołączenia odpowiedniej ilości plików tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES.

8. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.

9. Wykonawca, za pośrednictwem platformazakupowa.pl może przed upływem terminu składania ofert wycofać ofertę. Sposób dokonywania wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje

10. Cena oferty musi zawierać wszystkie koszty, jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością.

11. Dokumenty i oświadczenia składane przez Wykonawcę powinny być sporządzone w języku polskim, chyba że w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, Wykonawca zobowiązany jest załączyć tłumaczenie na język polski.

12. Zgodnie z definicją dokumentu elektronicznego z art. 3 ust. 2 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne, opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego Wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia albo przez Podwykonawcę.

13. Maksymalny rozmiar jednego pliku przesyłanego za pośrednictwem dedykowanych formularzy do: złożenia, zmiany, wycofania oferty wynosi 150 MB natomiast przy komunikacji wielkość pliku to maksymalnie 500 MB.

14. Każdy z Wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe podlegać będą odrzuceniu.

15. Wykonawca poniesie wszelkie koszty związane z przygotowaniem i złożeniem oferty.

16. Zamawiający odrzuca ofertę w przypadkach określonych w ustawie Pzp.

17. **W przypadku podmiotów wspólnie ubiegających się o udzielenie zamówienia publicznego:** Wykonawcy wspólnie ubiegający się o udzielenie zamówienia ustanawiają pełnomocnika do

reprezentowania ich w postępowaniu albo do reprezentowania ich w postępowaniu i zawarcia umowy. Pełnomocnictwo należy dołączyć do oferty. Wszelką korespondencję w postępowaniu Zamawiający kieruje do pełnomocnika. Niniejsze zasady dotyczą składania oferty przez wspólników spółki cywilnej. Przed zawarciem umowy wykonawcy wspólnie ubiegający się o udzielenie zamówienia będą mieli obowiązek przedstawić Zamawiającemu kopię umowy regulującej współpracę tych wykonawców. W przypadku, o którym mowa w art. 117 ust. 4 ustawy Pzp , wykonawcy wspólnie ubiegający się o udzielenie zamówienia dołączają odpowiednio do oferty oświadczenie, z którego wynika, które roboty budowlane, dostawy lub usługi wykonają poszczególni wykonawcy - **załącznik nr 4 do SWZ.**

XV. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Oferta może być złożona tylko do upływu terminu składania ofert.
2. Termin składania ofert upływa dnia **13.12.2024 r. o godz. 12:00** Oferty złożone po terminie składania ofert zostaną odrzucone.
3. Ofertę wraz z załącznikami (wymaganymi dokumentami) należy umieścić na https://platformazakupowa.pl pod adresem: **https://platformazakupowa.pl/transakcja/1029644**

DO OFERTY NALEŻY ZAŁĄCZYĆ:

- Oświadczenie Wykonawcy składane na podstawie art. 125 ust. 1 ustawy Pzp dotyczące podstaw wykluczenia z postępowania **(załącznik nr 3 do SWZ)**. Informacje zawarte w oświadczeniu stanowią wstępne potwierdzenie, że Wykonawca nie podlega wykluczeniu w zakresie wskazanym w SWZ (Oświadczenie składają również każdy z Wykonawców wspólnie ubiegający się o udzielenie zamówienia),
- Oświadczenie składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych – dla Wykonawców wspólnie ubiegających się o udzielenie zamówienia (**załącznik nr 4 do SWZ**), o ile ma zastosowanie,
- Pełnomocnictwo, o którym mowa w rozdziale XIV ust. 3,
- Potwierdzenie wniesienia wadium, o którym mowa w rozdziale X.

4. **Ofertę oraz dokumenty składane wraz z nią składa się, pod rygorem nieważności, w formie elektronicznej lub w postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym**.
5. Aby złożyć ofertę wraz z załącznikami na platformazakupowa.pl należy:
- Wypełnić Formularz składania oferty lub wniosku i dołączyć wszystkie wymagane załączniki a następnie należy kliknąć przycisk „Przejdź do podsumowania".
6. Oferta lub wniosek składana elektronicznie musi zostać podpisana kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. W procesie składania oferty za pośrednictwem platformazakupowa.pl, Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem platformazakupowa.pl. Zalecane stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 1 oraz ust. 2 ustawy Pzp, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym.
7. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku

składania oferty poprzez kliknięcie przycisku „Złóż ofertę" i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
8. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje.
9. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych ofert lub innych składanych dokumentów lub oświadczeń.
10. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.
11. Do upływu terminu składania ofert Wykonawca może wycofać ofertę.
12. Po upływie terminu składania ofert Wykonawca nie może skutecznie dokonać zmiany ani wycofać złożonej oferty.
13. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
14. Zgodnie z art. 18 ust. 3 ustawy Pzp, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji jeżeli Wykonawca, nie później niż w terminie składania ofert, w sposób niebudzący wątpliwości zastrzegł, że nie mogą być one udostępniane oraz wykazał, załączając stosowne wyjaśnienia, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Pzp. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.

XVI. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu **13.12.2024 r. o godz. 12:30,** przy użyciu systemu teleinformatycznego, tj. za pośrednictwem platformazakupowa.pl.
2. W przypadku awarii systemu teleinformatycznego, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
3. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
4. Zamawiający, niezwłocznie po otwarciu ofert, udostępnia na stronie internetowej prowadzonego postępowania informacje o:
1) nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej albo miejscach zamieszkania Wykonawców, których oferty zostały otwarte;
2) cenach lub kosztach zawartych w ofertach.
5. Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl oraz na https://bip.powiatbytowski.pl
6. W przypadku ofert, które podlegają negocjacjom, Zamawiający udostępnia informacje, o których mowa w ust. 4 pkt 2), niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.

XVII. WARUNKI UDZIAŁU W POSTĘPOWANIU

Zamawiający określa następujące warunki udziału w postępowaniu dotyczące:

1)zdolności do występowania w obrocie gospodarczym;
- nie dotyczy

2)uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów;
- nie dotyczy

3)sytuacji ekonomicznej lub finansowej;
- nie dotyczy

4)zdolności technicznej lub zawodowej.
- nie dotyczy

XVIII. PODSTAWY WYKLUCZENIA O KTÓRYCH MOWA W ART. 108 UST. 1 USTAWY PZP

1. Z postępowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 ustawy Pzp, Wykonawcę:
1) 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 2023 r. poz. 2048 oraz z 2024 r. poz. 1166) 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 2024 r. poz. 930),
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. z 2021 r. poz. 1745),
g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296-307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270-277d Kodeksu karnego, lub przestępstwo skarbowe,
h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej,
- lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;

2) jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
3) wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
4) wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;
5) jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;
6) jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia.

XIX. PODSTAWY WYKLUCZENIA O KTÓRYCH MOWA W ART. 109 UST. 1 PKT 1 I 4 USTAWY PZP

1. Z postępowania o udzielenie zamówienia wyklucza się, z zastrzeżeniem art. 110 ust. 2 ustawy Pzp, Wykonawcę:
1) który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;
2) 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.

XX. PODSTAWY WYKLUCZENIA O KTÓRYCH MOWA W USTAWIE Z DNIA 13 KWIETNIA 2022 R. O SZCZEGÓLNYCH ROZWIĄZANIACH W ZAKRESIE PRZECIWDZIAŁANIA WSPIERANIU AGRESJI NA UKRAINĘ ORAZ SŁUŻĄCYCH OCHRONIE BEZPIECZEŃSTWA NARODOWEGO

Z postępowania o udzielenie zamówienia publicznego wyklucza się, na podstawie 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 (t.j. Dz. U. z 2024 r. poz. 507 z późn. zm.):

1) wykonawcę oraz uczestnika konkursu 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;

2) wykonawcę oraz uczestnika konkursu, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j. Dz. U. z 2023 r. poz. 1124, 1285, 1723, 1843) 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;

3) wykonawcę oraz uczestnika konkursu, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2023 r. poz. 120, 295, 1598) 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.

Wykluczenie następuje na okres trwania ww. okoliczności.

XXI. INFORMACJA O PODMIOTOWYCH ŚRODKACH DOWODOWYCH

1. Wykonawca, którego oferta została najwyżej oceniona, zostanie wezwany przez Zamawiającego do złożenia w wyznaczonym terminie, nie krótszym niż 5 dni od dnia wezwania, podmiotowych środków dowodowych, aktualnych na dzień ich złożenia.
2. Zamawiający informuje, iż Wykonawca jest obowiązany do złożenia **wraz z ofertą Oświadczenia**. Wzór oświadczenia stanowi **załącznik nr 3 do SWZ**.
3. W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, Oświadczenie, składa każdy z Wykonawców. Oświadczenie to potwierdza brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z Wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
4. **Na potwierdzenie braku podstaw wykluczenia Wykonawca, na wezwanie Zamawiającego, o którym mowa w rozdziale XXI ust. 1 składa następujące dokumenty:**

1) oświadczenia Wykonawcy, w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp, o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2024 r. poz. 594), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową lub wniosek o dopuszczenie do udziału w postępowaniu, albo oświadczenia o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Wzór oświadczenia stanowi **załącznik nr 8 do SWZ.**

2) oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, w zakresie podstaw wykluczenia z postępowania wskazanych przez

Zamawiającego w SWZ. Wzór oświadczenia stanowi **załącznik nr 7 do SWZ.**
5. Jeżeli Wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zastosowanie znajdzie § 4 Rozporządzenia Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy (Dz. U. z 2020 r. poz. 2415).
6. Jeżeli osoba reprezentująca Wykonawcę działa na podstawie pełnomocnictwa, pełnomocnictwo to w formie oryginału lub notarialnie potwierdzonej kopii musi zostać dołączone do oferty.

XXII. SPOSÓB OBLICZENIA CENY

1. Wykonawca poda cenę oferty w Formularzu Ofertowym sporządzonym według wzoru stanowiącego **załącznik nr 2 do SWZ**, jako cenę brutto z wyszczególnieniem stawki podatku od towarów i usług (VAT).
2. Cena oferty stanowi wynagrodzenie ryczałtowe.
3. Cena musi być wyrażona w złotych polskich (PLN). Zaokrąglenia cen w złotych należy dokonać do dwóch miejsc po przecinku według zasady, że trzecia cyfra po przecinku od 5 w górę powoduje zaokrąglenie drugiej cyfry po przecinku w górę o 1. Jeśli trzecia cyfra po przecinku jest niższa od 5 zostaje skreślona, a druga cyfra po przecinku nie ulegnie zmianie. Cenę oferty należy określić z należytą starannością, na podstawie opisu przedmiotu zamówienia z uwzględnieniem wszystkich kosztów związanych z realizacją zadania wynikających z zakresu dostawy, niezbędnych do wykonania zadania i doliczyć do powstałej kwoty inne składniki wpływające na ostateczną cenę. Cena winna uwzględniać także wszystkie koszty wynikające z opisu przedmiotu zamówienia zawartego w **Rozdziale V oraz w załączniku nr 1 do SWZ.**
4. Wykonawca poda w Formularzu Ofertowym stawkę podatku od towarów i usług (VAT) właściwą dla przedmiotu zamówienia, obowiązującą według stanu prawnego na dzień składania ofert. Określenie ceny ofertowej z zastosowaniem nieprawidłowej stawki podatku od towarów i usług (VAT) potraktowane będzie, jako błąd w obliczeniu ceny i spowoduje odrzucenie oferty, jeżeli nie ziszczą się ustawowe przesłanki omyłki (na podstawie art. 226 ust. 1 pkt 10 ustawy Pzp w związku z art. 223 ust. 2 pkt 3 ustawy Pzp).
5. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
6. W przypadku rozbieżności pomiędzy ceną ryczałtową podaną cyfrowo a słownie, jako wartość właściwa zostanie przyjęta cena ryczałtowa podana słownie.
7. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.

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

Zamawiający będzie stosować przy dokonywaniu wyboru najkorzystniejszej oferty następujące kryteria:

NAZWA KRYTERIUM OCENY OFERT:	WAGA (Wg.)
Cena brutto	**60 pkt**
Termin wykonania zamówienia	**40 pkt**

CENA BRUTTO (C):
Zamawiający przyjmuje cenę brutto jako kryterium oceny ofert, przypisując jej rangę **60 pkt**. Wartość punktowa powyższego kryterium obliczana będzie według następującego wzoru:

$$C = \frac{Cn}{Cb} \times 60 \text{ pkt}$$

gdzie:
C – ilość punktów za kryterium cena brutto
Cn – cena brutto oferty najkorzystniejszej (najniższa) spośród oferowanych
Cb – cena brutto oferty badanej

Obliczenia dokonywane będą do dwóch miejsc po przecinku, według zasady określonej w **Rozdziale XXII ust. 3**

TERMIN WYKONANIA ZAMÓWIENIA (T):
Zamawiający przyjmuje termin wykonania zamówienia jako kryterium oceny ofert, przypisując mu rangę **40 pkt**. Kryterium będzie rozpatrywane na podstawie terminu podanego przez Wykonawcę w Formularzu ofertowym. Termin ten liczony będzie od dnia zawarcia umowy. Wartość punktowa powyższego kryterium obliczana będzie według poniższej tabeli:

25 dni kalendarzowych i mniej	**40 pkt**
od 26 do 30 dni kalendarzowych	**30 pkt**
od 31 do 35 dni kalendarzowych	**20 pkt**
od 36 do 40 dni kalendarzowych	**10 pkt**
40 dni kalendarzowych i więcej	**0 pkt**

UWAGA!! Maksymalny termin wykonania zamówienia wynosi **45 dni kalendarzowych** na potrzeby oceny ofert.
UWAGA!!! W przypadku, gdy Wykonawca, nie zaznaczy w ofercie terminu wykonania zamówienia, Zamawiający do oceny oferty przyjmie 45 dni kalendarzowych i przyzna „0" punktów . W przypadku, gdy Wykonawca wskaże termin dłuższy niż 45 dni kalendarzowych, oferta zostanie odrzucona na podstawie art. 226 ust. 1 pkt 5.

Ilość punktów (P), jaką otrzyma dana oferta będzie równa sumie punktów z poszczególnych kryteriów:

$$P = C + T$$

1. Przy wyborze oferty Zamawiający będzie się kierował powyżej wskazanymi kryteriami.
2. Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.
3. Za najkorzystniejszą zostanie uznana oferta, która uzyskała najwyższą liczbę punktów, maksymalnie 100.

4. W toku badania i oceny ofert Zamawiający może żądać od Wykonawców wyjaśnień dotyczących treści złożonych przez nich ofert lub innych składanych dokumentów lub oświadczeń. Wykonawcy są zobowiązani do przedstawienia wyjaśnień w terminie wskazanym przez Zamawiającego.
5. Jeżeli zostanie złożona oferta, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług (t.j.: Dz. U. z 2024 r. poz. 361 z późn. zm.). dla celów zastosowania kryterium ceny Zamawiający dolicza do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałby obowiązek rozliczyć
6. W ofercie Wykonawca ma obowiązek:
1) poinformowania Zamawiającego, że wybór jego oferty będzie prowadził do powstania u Zamawiającego obowiązku podatkowego;
2) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
3) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym Zamawiającego, bez kwoty podatku;
4) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą Wykonawcy, będzie miała zastosowanie.
7. W przypadku, gdy Zamawiający skorzysta z możliwości negocjacji i Wykonawca na zaproszenie do złożenia oferty dodatkowej, złoży taką ofertę zawierającą nową, niższą cenę, ocenie podlegać będzie oferta Wykonawcy złożona w odpowiedzi na ogłoszenie o zamówieniu z uwzględnieniem zmiany ceny wynikającej z oferty dodatkowej.
8. Zamawiający wybiera najkorzystniejszą ofertę w terminie związania ofertą określonym w SWZ.
9. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę, którego oferta otrzymała najwyższą ocenę, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
10. W przypadku braku zgody, o której mowa w ust. 9, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą przesłanki do unieważnienia postępowania.

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

1. Zamawiający zawiera umowę w sprawie zamówienia publicznego, z uwzględnieniem art. 577 ustawy Pzp,
w terminie nie krótszym niż 5 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 10 dni, jeżeli zostało przesłane w inny sposób.
2. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu, o którym mowa w ust. 1, jeżeli w postępowaniu o udzielenie zamówienia złożono tylko jedną ofertę.
3. Wykonawca, którego oferta została wybrana jako najkorzystniejsza, zostanie poinformowany przez Zamawiającego o miejscu i terminie podpisania umowy.
4. Wykonawca, o którym mowa w ust. 1, ma obowiązek zawrzeć umowę w sprawie zamówienia na warunkach określonych w projektowanych postanowieniach umowy, które stanowią **załącznik nr 6 do SWZ**. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty, z uwzględnieniem ewentualnych nowych propozycji przedstawionych w ofercie dodatkowej.

5. Przed podpisaniem umowy Wykonawcy wspólnie ubiegający się o udzielenie zamówienia (w przypadku wyboru ich oferty jako najkorzystniejszej) przedstawią Zamawiającemu umowę regulującą współpracę tych Wykonawców.
6. Jeżeli Wykonawca, którego oferta została wybrana jako najkorzystniejsza, uchyla się od zawarcia umowy w sprawie zamówienia publicznego Zamawiający może dokonać ponownego badania i oceny ofert spośród ofert pozostałych w postępowaniu Wykonawców albo unieważnić postępowanie.

XXV. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy Pzp.
2. Odwołanie przysługuje na:
1) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
2) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy Pzp, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" ustawy Pzp.

XXVI. KLAUZULA INFORMACYJNA Z ART. 13 RODO

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 POWIAT BYTOWSKI z siedzibą: Starostwo Powiatowe w Bytowie ul. Ks. dr. B. Domańskiego 2, 77-100 Bytów, z którym można się kontaktować pisemnie, na adres siedziby, przez adres e-mail: starostwo@powiatbytowski.pl bądź telefonicznie, pod numerem: 59 822 80 00;
2) z inspektorem ochrony danych osobowych można się skontaktować pisemnie, na adres siedziby, przez adres e- mail: iod@powiatbytowski.pl bądź telefonicznie, pod numerem: 59 822 80 00;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego pn. **DOSTAWA SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO**

„CYBERBEZPIECZNY SAMORZĄD”, prowadzonym w trybie podstawowym. **art. 275 pkt 2** ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320 z późn. zm.) ;

4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 8 oraz art. 96 ust. 3 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (Dz. U. z 2024 r., poz. 1320 z późn. zm.), dalej „ustawa Pzp”;

5) Pani/Pana dane osobowe będą przechowywane przez okres określony w oparciu o uzasadniony interes realizowany przez administratora (dane przetwarzane są do momentu ustania przetwarzania w celach wynikających z wykonania umowy) zgodnie z Rozporządzeniem Prezesa Rady Ministrów z dnia 18 stycznia 2011 r. w sprawie instrukcji kancelaryjnej, jednolitych rzeczowych wykazów akt oraz instrukcji w sprawie organizacji i zakresu działania archiwów zakładowych (Dz. U. Nr 14, poz. 67 z późn. zm.)

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.

---

* Wyjaśnienie: skorzystanie z prawa do sprostowania nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego ani zmianą postanowień umowy w zakresie niezgodnym z ustawą Pzp oraz nie może naruszać integralności protokołu oraz jego załączników.

** Wyjaśnienie: prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

XXVII. INFORMACJE DODATKOWE

1) Informacje dotyczące ofert wariantowych, w tym informacje o sposobie przedstawiania ofert wariantowych oraz minimalne warunki, jakim muszą odpowiadać oferty wariantowe, jeżeli zamawiający wymaga lub dopuszcza ich składanie;

- nie dotyczy

2) Wymagania w zakresie zatrudnienia na podstawie stosunku pracy, w okolicznościach, o których mowa w art. 95;

- nie dotyczy

3) Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2, jeżeli zamawiający przewiduje takie wymagania;

- nie dotyczy

4) Informację o zastrzeżeniu możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94, jeżeli zamawiający przewiduje takie wymagania;

- nie dotyczy

5) Wymagania dotyczące zabezpieczenia należytego wykonania umowy, jeżeli zamawiający je przewiduje;

- nie dotyczy

6) Informację o przewidywanych zamówieniach, o których mowa w art. 214 ust. 1 pkt 7 i 8, jeżeli zamawiający przewiduje udzielenie takich zamówień;

- nie dotyczy

7) Informacje dotyczące przeprowadzenia przez wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2, jeżeli zamawiający przewiduje możliwość albo wymaga złożenia oferty po odbyciu wizji lokalnej lub sprawdzeniu tych dokumentów;

- nie dotyczy

8) Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między zamawiającym a wykonawcą, jeżeli zamawiający przewiduje rozliczenia w walutach obcych;

- nie dotyczy

9) Informacje dotyczące zwrotu kosztów udziału w postępowaniu, jeżeli zamawiający przewiduje ich zwrot;

- nie dotyczy

10) Informację o obowiązku osobistego wykonania przez wykonawcę kluczowych zadań, jeżeli zamawiający dokonuje takiego zastrzeżenia zgodnie z art. 60 i art. 121;

- nie dotyczy

11) Maksymalną liczbę wykonawców, z którymi zamawiający zawrze umowę ramową, jeżeli zamawiający przewiduje zawarcie umowy ramowej;

- nie dotyczy

12) Informację o przewidywanym wyborze najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230, jeżeli zamawiający przewiduje aukcję elektroniczną;

- nie dotyczy

13) Wymóg lub możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93;

- nie dotyczy

XXVIII. ZAŁĄCZNIKI DO SWZ

Integralną częścią niniejszej SWZ stanowią następujące załączniki:

Załącznik nr 1 - Opis przedmiotu zamówienia
Załącznik nr 2 - Formularz ofertowy wraz z wykazem sprzętu
Załącznik nr 3 - Oświadczenie wykonawcy składane na podstawie art. 125 ust. 1 ustawy Pzp dotyczące podstaw wykluczenia z postępowania
Załącznik nr 4 - Oświadczenie wykonawcy składane na podstawie art. 117 ust. 4 ustawy Pzp – dla podmiotów wspólnie ubiegających się o zamówienie
Załącznik nr 5 - Formularz oferty dodatkowej
Załącznik nr 6 - Projektowane postanowienia umowy
Załącznik nr 7 - Oświadczenie Wykonawcy o aktualności informacji zawartych w oświadczeniu o którym mowa w art. 125 ust. 1 ustawy Pzp w zakresie podstaw wykluczenia z postępowania
Załącznik nr 8 - Oświadczenie o przynależności lub braku przynależności do tej samej grupy kapitałowej z innym Wykonawcą, który złożył odrębną ofertę

Załącznik nr 1 do SWZ

1. UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv - 1 kpl.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv, fabrycznie nowe.**
System, k**onstrukcja**	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19”. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. Możliwość przeprowadzenia konfiguracji w trybie Zero Touch.
Pamięć operacyjna RAM	nie mniej niż 8 (GB)
Przestrzeń do przechowywania logów i raportów	nie mniej niż 120 GB
Liczba fizycznych interfejsów 1000BASE-T	nie mniej niż 8
Liczba fizycznych interfejsów 1000BASE-X	nie mniej niż 2
Liczba fizycznych interfejsów 10GBASE-X	nie mniej niż 4
Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q	nie mniej niż 512
Wydajność Firewall	nie mniej niż 30 000 Mbps
Wydajność Firewall IMIX	nie mniej niż 15 000 Mbps
Wydajność IPS	nie mniej niż 5 000 Mbps
Wydajność FW+IPS+AV	nie mniej niż 1 000 Mbps
Wydajność NGFW	nie mniej niż 5 000 Mbps
Liczba równoczesnych połączeń	nie mniej niż 6 000 000
Liczba nowych połączeń na sekundę	nie mniej niż 128 000
Wydajność IPsec VPN	nie mniej niż 15 000 Mbps

Nazwa komponentu	Wymagane minimalne parametry techniczne
Wydajność dla inspekcji ruchu SSL/TLS	nie mniej niż 2 000 Mbps
Liczba równoczesnych połączeń SSL/TLS	nie mniej niż 16 000
Liczba równoczesnych tuneli SSL VPN	nie mniej niż 2 000
Liczba równoczesnych tuneli IPsec VPN	nie mniej niż 2 000
Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.
Zapora sieciowa	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.
Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast. Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.
Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT

Nazwa komponentu	Wymagane minimalne parametry techniczne
Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet.
Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).
Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.
Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.
Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec.
Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza.

Nazwa komponentu	Wymagane minimalne parametry techniczne
	System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.
System prewencyjny i zaawansowanej ochrony	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.
Ochrona i kontrola web przed Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiążanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)
Ochrona i kontrola web - Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.
Filtr Web	Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.
Ochrona i kontrola aplikacji	Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.
Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sandbox do ochrony przez zadrożeniami typu Zero-Day. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.
Gwarancja	Min. 2 lata gwarancji oraz wsparcia technicznego . Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. Wsparcie i licencja na urządzenie, w tym na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Wdrożenie, szkolenie	Zamawiający wymaga podłączenia i zainstalowania we wskazanym miejscu UTM-a, Switch-y oraz AP. Zamawiający wymaga stworzenia przez Wykonawcę projektu segmentacji sieci oraz polityk bezpieczeństwa w myśl wytycznych Zamawiającego a opartych na wytycznych KRI i SZBI, CERT. Zamawiający po zaakceptowaniu projektów wymaga od Wykonawcy zaimplementowania i wdrożenia projektów na dostarczonych urządzeniach. Zamawiający wymaga szkolenia min. 8 godzin z wdrożonego rozwiązania w szczególności z zakresu polityk bezpieczeństwa, administracji i zarządzania.

2. Sprzętowy appliance zapewniający szyfrowany kanał komunikacji – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ systemu	**Sprzętowy appliance zapewniający szyfrowany kanał komunikacji z nadrzędnym rozwiązaniem klasy UTM/NGFW zaproponowanym w obecnym postępowaniu, fabrycznie nowy.**
Porty	min.: 1 porty 1 GbE/SFP WAN, 4 porty 1GbE LAN, 2 x port zasilania DC, 2 x USB 3.0, 1x Console (RJ-45 lub DB9)
Rodzaj urządzenia	switch zarządzalny z wbudowanym VPN z możliwością tunelowania ruchu w warstwie 2 z zaproponowanym urządzeniem UTM
Przepustowość	min. 250 Mb/s
WIFI / GSM	Możliwość rozbudowy urządzenia w zintegrowany modułu WIFI lub modułu GSM 3G/4G
Moc pracy	max. 9 W
Zarządzanie i utrzymanie	Rozwiązanie musi być w całości zarządzane przez nadrzędne rozwiązanie klasy UTM/NGFW. Plik konfiguracyjny pobierany musi być automatycznie z serwera provisioningu lub z pamięci USB Flash. Rozwiązanie cyklicznie sprawdzać powinno w/w lokalizacje pod kątem obecności nowej wersji konfiguracji. Aktualizacja oprogramowania (firmware) realizowana z poziomu nadrzędnego urządzenia UTM/NGFW. Urządzenie powinno pozwolić na zestawienie szyfrowanego kanału komunikacji z nadrzędnym UTM/NGFW (minimum AES-256). Rozwiązanie po stronie interfejsu WAN winno działać jako klient DHCP z opcją późniejszej zmiany adresu na adres statyczny. Urządzenie powinno obsługiwać modemy 3G/4G oferując przy tym mechanizm WAN Link Failover lub Load Balancing. Interfesjy LAN urządzenia powinny działać jako kolejne interfejsy nadrzędnego rozwiązania klasy UTM/NGFW. Filtrowanie ruchu realizowane być powinno na poziomie nadrzędnego urządzenia UTM/NGFW.
Gwarancja i wsparcie	Min. 2 lata gwarancji oraz wsparcia technicznego . Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Produkt posiadający licencje uprawniające na dożywotnią możliwość korzystania z wszystkich funkcji produktu;

3. Przełącznik sieciowy zarządzalny 48-portowy - 5 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**
Porty	min.: 48 porty 1GbE 4 porty SFP+ 10GbE
Rodzaj urządzenia	switch zarządzalny
Warstwa	zarządzanie na poziomie warstwy 2 i 3
Minimalny rozmiar tablicy MAC	32000
Przepustowość	min. 176Gb/s
Pamięć robocza	min. 512 MB
Pamięć bufora	min. 2 MB
Moc pracy	max. 60W
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzane przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.
Typ obudowy	RACK
Ilość VLAN	min 256
Gwarancja	1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;

4. Przełącznik sieciowy zarządzalny 24-portowy - 3 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**
Porty	min.: 24 porty 1GbE, 4 porty SFP+ 10GbE
Rodzaj urządzenia	switch zarządzalny
Warstwa	zarządzanie na poziomie warstwy 2 i 3
Minimalny rozmiar tablicy MAC	16000
Przepustowość	min. 128Gb/s
Pamięć robocza	min. 512 MB
Pamięć bufora	min. 1,5 MB
Moc pracy	max. 25W
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.
Typ obudowy	RACK
Ilość VLAN	min 256
Gwarancja	1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;

5. Przełącznik sieciowy zarządzalny 24-portowy PoE – 1 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**
Porty	min.: 24 porty 1GbE PoE, 4 porty SFP+ 10GbE
Rodzaj urządzenia	switch zarządzalny
Warstwa	zarządzanie na poziomie warstwy 2 i 3
Minimalny rozmiar tablicy MAC	16000
Przepustowość	min. 128Gb/s
Pamięć robocza	min. 512 MB
Pamięć bufora	min. 1,5 MB
PoE obciążenie portów w standardzie 802.3af/802.3at	24 porty (min. 15,4W) lub 13 protów (30W)
Moc pracy	max. 410W
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.
Typ obudowy	RACK
Ilość VLAN	min 256
Gwarancja	1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;

6. Przełącznik sieciowy zarządzalny 8-portowy – 4 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**
Porty	min.: 8 porty 1GbE 2 porty SFP 1GbE
Rodzaj urządzenia	switch zarządzalny
Warstwa	zarządzanie na poziomie warstwy 2 i 3
Minimalny rozmiar tablicy MAC	8000
Przepustowość	min. 20Gb/s
Pamięć robocza	min. 256 MB
Pamięć bufora	min. 512 KB
Moc pracy	max. 12W
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.
Ilość VLAN	min 256
Gwarancja	1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;

7. Punkt dostępowy AP – 6 szt.

Nazwa komponentu	Wymagane minimalne parametry techniczne
Typ	**Punkt dostępowy AP, fabrycznie nowy**
Porty	min.: 1GbE PoE+ (802.3at), gniazdo zasilania DC, port konsoli dostępu
Rodzaj urządzenia	Punkt dostępowy AP WIFI 6
Anteny wewnętrzne	Min. 2x2:2 dual radio (1 x 2.4 GHz, 1 x 5 GHz)
Obsługiwanie standardy 802.11	b, n, g, ax, ac
Szybkość transmisji danych 2,4 GHz	min. 574 Mbps
Szybkość transmisji danych 5 GHz	min. 1,2 Gbps
Uchwyt	Dedykowany uchwyt producenta urządzenia do zamocowania na ścianie lub suficie
Waga	max. 0,9 kg
Moc pracy	max. 18W
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.
Gwarancja	1. Min. 2 lata gwarancji oraz wsparcia technicznego . 2. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 3. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 4. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące
Dodatkowe wymagania	Zamawiający wymaga by Wykonawca wykonał przed dostarczeniem rozwiązania - projektu pokrycia i pojemności zasięgów WIFI z testami i pomiarami na obiekcie oraz miejscach wskazanych przez Zamawiającego. Przekazane mapy pokrycia sygnałem Zamawiającemu odbywa się w trakcie przekazania urządzeń. Zamawiający udostępni obiekt do dokonania wizji lokalnej wraz z pomiarami w uzgodnionym wcześniej terminie.

Załącznik nr 2 do SWZ

Powiat Bytowski
ul. Ks. dr. Bolesława Domańskiego 2
77-100 Bytów

FORMULARZ OFERTOWY

Ja/my niżej podpisani:

……..

(imię i nazwisko, stanowisko/podstawa reprezentacji)

działając w imieniu i na rzecz:

……..……
……..

(pełna nazwa Wykonawcy/Wykonawców w przypadku wspólnie ubiegających się o udzielenie zamówienia)

Adres:……....

Województwo:……..……

Kraj:……..……

Regon:……..……

NIP:……..……

Tel.:……..….

Adres skrzynki ePUAP……

Adres e-mail:…….. *(na które Zamawiający ma przesłać korespondencję)*

Wadium wniesione w pieniądzu należy zwrócić na rachunek bankowy: ……

Oświadczam, że rodzaj Wykonawcy to (informacja do celów statystycznych)*:

☐ *mikroprzedsiębiorstwo*, ☐ *małe przedsiębiorstwo*, ☐ *średnie przedsiębiorstwo*, ☐ *jednoosobowa działalność gospodarcza*, ☐ *osoba fizyczna nieprowadząca działalności gospodarczej*, ☐ *inny rodzaj*

Przystępując do postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”**, Składamy ofertę na realizację przedmiotu zamówienia w zakresie określonym w Specyfikacji Warunków Zamówienia na następujących warunkach:

cena netto za realizacje całego zamówienia wynosi: ……zł

(słownie złotych: ……..)

Podatek VAT…..%, ……..zł

cena brutto za realizacje całego zamówienia wynosi: ……zł

(słownie złotych: ……..)

Oświadczamy, że oferujemy następujący termin wykonania zamówienia:…….. dni**

Oświadczamy, że zapoznaliśmy się ze Specyfikacją Warunków Zamówienia oraz jej załącznikami i nie wnosimy do ich treści żadnych zastrzeżeń.

Oświadczamy, że uzyskaliśmy wszelkie informacje niezbędne do prawidłowego przygotowania i złożenia niniejszej oferty.

Informujemy, że zamierzamy/nie zamierzamy* powierzyć wykonanie części zamówienia podwykonawcom. Zakres prac powierzonych podwykonawcy:

Wykonawca powierzy podwykonawcom wykonanie następujących części zamówienia:		
	Wskazanie części zamówienia, których wykonanie Wykonawca zamierza powierzyć podwykonawcy	Nazwy (firmy) podwykonawców, jeżeli są znani
L.p		
1.		
2.		
3.		

Oświadczamy, że jesteśmy związani niniejszą ofertą przez okres wskazany w SWZ.

Oświadczamy, że zapoznaliśmy się z projektowanymi postanowieniami umowy, określonymi w **załączniku nr 6** do SWZ i zobowiązujemy się, w przypadku wyboru naszej oferty, do zawarcia umowy zgodnej z niniejszą ofertą, na warunkach w nich określonych.

Oświadczamy, że zapoznaliśmy się z klauzulą informacyjną zawartą w SWZ wynikającą z art. 13 ogólnego rozporządzenia o ochronie danych osobowych z dnia 27 kwietnia 2016 r. (t.j. Dz. U. z 2019 r. poz. 1781)

Oświadczamy, że wypełniliśmy 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[2].

Oświadczamy, że sposób reprezentacji spółki/konsorcjum* dla potrzeb niniejszego zamówienia jest następujący:

……

……

[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).

[2] 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)

Ofertę niniejszą składamy na …… stronach.

Załącznikami do niniejszej oferty są:

……

……

Miejscowość i data ……

(podpis)

Informacja dla Wykonawcy:

Formularz oferty musi być opatrzony przez osobę lub osoby uprawnione do reprezentowania firmy kwalifikowanym podpisem elektronicznym, podpisem zaufanych lub podpisem osobistym i przekazany Zamawiającemu wraz z dokumentem (-ami) potwierdzającymi prawo do reprezentacji Wykonawcy przez osobę podpisującą ofertę.

*** zakreślić właściwe**
**** w wyznaczonym miejscu proszę wskazać deklarowany termin wykonania zamówienia**
(UWAGA!!! W przypadku, gdy Wykonawca, nie zaznaczy w ofercie terminu wykonania zamówienia, Zamawiający do oceny oferty przyjmie 45 dni kalendarzowych i przyzna „0" punktów . W przypadku, gdy Wykonawca wskaże termin dłuższy niż 45 dni kalendarzowych, oferta zostanie odrzucona na podstawie art. 226 ust. 1 pkt 5.)

WYKAZ SPRZĘTU

1. UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv - 1 kpl.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	**Wymagane minimalne parametry techniczne**	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv, fabrycznie nowe.**	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
System, k**onstrukcja**	System ochrony sieci powinien zostać dostarczony w postaci komercyjnej platformy sprzętowej z zabezpieczonym systemem operacyjnym producenta rozwiązania. Rozwiązanie powinno być wyposażone w moduł kryptograficzny zgodny ze standardem FIPS 140-2. Rozwiązanie powinno wspierać następujące tryby pracy: routing (warstwa 3), bridge (warstwa 2), hybrydowy (część jako router, część jako bridge), TAP / Discover (sonda monitorująca) Rozwiązanie powinno ofertować możliwość budowy klastra wysokiej dostępności pracującego trybie Active-Passive lub Active-Active. System ochrony nie może posiadać ograniczeń co do ilości hostów w sieci chronionej. Rozwiązanie musi umożliwiać doposażenie o nadmiarowy zasilacz sieciowy dla zapewnienia ciągłości pracy (drugi zasilacz jako wyposażenie opcjonalne). Urządzenie w metalowej obudowie z możliwością montażu w szafie rack 19”. Wbudowany port konsolowy zgodny z RS-232 (RJ-45 i/lub micro-USB). Wbudowany port USB umożliwiający podłączenie modemów 3G/4G/LTE produkowanych przez firmy trzecie. Możliwość przeprowadzenia konfiguracji w trybie Zero Touch.	
Pamięć operacyjna RAM	nie mniej niż 8 (GB)	
Przestrzeń do przechowywania logów i raportów	nie mniej niż 120 GB	
Liczba fizycznych interfejsów 1000BASE-T	nie mniej niż 8	
Liczba fizycznych interfejsów 1000BASE-X	nie mniej niż 2	
Liczba fizycznych interfejsów 10GBASE-X	nie mniej niż 4	
Liczba wirtualnych interfejsów (VLAN) IEEE 802.1Q	nie mniej niż 512	
Wydajność Firewall	nie mniej niż 30 000 Mbps	
Wydajność Firewall IMIX	nie mniej niż 15 000 Mbps	
Wydajność IPS	nie mniej niż 5 000 Mbps	……
Wydajność FW+IPS+AV	nie mniej niż 1 000 Mbps	
Wydajność NGFW	nie mniej niż 5 000 Mbps	
Liczba równoczesnych połączeń	nie mniej niż 6 000 000	
Liczba nowych połączeń na sekundę	nie mniej niż 128 000	
Wydajność IPsec VPN	nie mniej niż 15 000 Mbps	
Wydajność dla inspekcji ruchu SSL/TLS	nie mniej niż 2 000 Mbps	
Liczba równoczesnych połączeń SSL/TLS	nie mniej niż 16 000	
Liczba równoczesnych tuneli SSL VPN	nie mniej niż 2 000	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Liczba równoczesnych tuneli IPsec VPN	nie mniej niż 2 000	
Zarządzanie	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelniania dwuskładnikowego w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. Wbudowany webowy graficzny interfejs administratora powinien oferować narzędzia diagnostyczne takie jak co najmniej: ping, traceroute, name lookup, route lookup czy packet capture w oparciu o Berkley Packet Filter. Interfejs graficzny administratora powinien zapewniać narzędzia do przechwytywania pakietów, wyświetlania otwartych połączeń sieciowych, wyświetlania tablicy ARP/NDP. Rozwiązanie powinno oferować możliwość definiowania profili administracyjnych określających dostęp do poszczególnych modułów konfiguracyjnych urządzenia na prawach: brak dostępu, dostęp tylko do odczytu lub pełen odczyt i zapis. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. System powinien oferować mechanizm blokady kolejnych połączeń w przypadku prób nieautoryzowanego dostępu do interfejsu do zarządzania. Liczba takich prób oraz czas blokady powinny być swobodnie definiowane przez administratora. Rozwiązanie powinno posiadać mechanizm informowania o aktualizacjach oprogramowania systemowego wraz z automatycznym procesem ich aplikowania (upgrade) i wycofywania (rollback). System powinien oferować możliwość zdefiniowania własnych obiektów typu sieć, usługa, host, harmonogram czasowy, użytkownik, grupa użytkowników, klient, serwer z możliwością wykorzystania ich do budowy polityk bezpieczeństwa. Dodawanie obiektów powinno być możliwe bezpośrednio podczas tworzenia dowolnej polisy bezpieczeństwa. System powinien oferować mechanizm pozwalający na śledzenie zmian w konfiguracji (tzw. changelog). Rozwiązanie powinno zapewniać elastyczne zarządzanie dostępem do usług administracyjnych per strefa zapory sieciowej. System powinien być wyposażony w mechanizm automatycznego powiadamiania za pośrednictwem protokołu SMTPS (STARTTLS lub SSL/TLS). Rozwiązanie powinno oferować monitorowanie stany pracy w oparciu o protokoły SNMP v1, v2c i v3 oraz biblioteki dostarczane i aktualizowane przez producenta. System musi oferować wsparcie dla co najmniej Netflow v5 (lub jego odpowiednika). System powinien zapewniać monitorowanie w czasie rzeczywistym stanu urządzenia (użycie CPU, RAM, HDD, obciążenie interfejsów sieciowych). Podobne statystyki powinny być dostępne również dla danych historycznych, z retencją do 12 miesięcy (celem śledzenia trendów obciążenia) w ramach webowego interfejsu graficznego urządzenia. System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta Wymagane jest aby rozwiązanie oferowało wbudowany mechanizm do automatycznego tworzenia szyfrowanych hasłem kopii zapasowych konfiguracji. Dostarczony system powinien posiadać udokumentowane API umożliwiające integrację z systemami firm trzecich.	
Zapora sieciowa	Wymagane jest aby zapora sieciowa działała w oparciu o mechanizm Stateful Packet Inspection. System powinien umożliwiać budowanie niezależnych stosów reguł dla protokołów IPv4 oraz IPv6. Rozwiązanie powinno umożliwiać budowanie polis w oparciu o takie obiekty jak sieć, usługa, użytkownik, grupa użytkowników lub czas. Rozwiązanie powinno zapewniać możliwość tworzenia polis w oparciu o relacje między strefami zapory sieciowej. Rozwiązanie powinno oferować możliwość definiowania własnych stref zapory sieciowej. System powinien umożliwiać blokowanie ruchu na podstawie kraju pochodzenia (geolokalizacja IP). System powinien pozwalać na filtrowanie widoku stosu reguł na bazie dowolnego ich składnika.	
Trasowanie ruchu	Rozwiązanie powinno oferować routing oparty o polityki SD-WAN wykorzystujące takie kryteria jak: interfejs, sieć, usługa, grupa aplikacji, użytkownik lub grupa użytkowników, brama główna, brama zapasowa czy load-balancing. Rozwiązanie powinno zapewniać rozkład ruchu pomiędzy kilkoma interfejsami WAN, z automatyczną diagnostyką łącz oraz automatycznym przełączaniem ruchu w przypadku awarii łącza. Przy podejmowaniu decyzji o przełączeniu ruchu na bramę zapasową poza sondowaniem przy użyciu protokołów ICMP czy TCP brane powinny być pod uwagę również takie kryteria jak jitter, opóźnienie czy utrata pakietów. Rozwiązanie powinno zapewniać obsługę routingu statycznego dla ruchu unicast i multicast.	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
	Rozwiązanie powinno zapewniać obsługę protokołów routingu dynamicznego (RIP, BGP, OSPF). Rozwiązanie powinno zapewniać obsługę Protocol Independent Multicast Sparse Mode (PIM-SM). Rozwiązanie powinno zapewniać możliwość przekierowania ruchu do nadrzędnych serwerów proxy (upstream/parent proxy) dla IPv4 i IPv6.	
Translacja adresów i portów	Rozwiązanie powinno pozwolić na definiowanie niezależnych od reguł zapory polis NAT. Rozwiązanie powinno pozwalać na tworzenie reguł NAT typu MASQ, SNAT, DNAT	
Kształtowanie pasma i jakość usług	System powinien zapewniać możliwość elastycznego kształtowania pasma (Traffic Shaping) dla sieci, użytkowników i aplikacji. Rozwiązanie powinno pozwalać na tworzenie limitów ilości danych dla użytkowników w kierunku upload, download lub total. Limity powinny być przyznawane cykliczne lub niecykliczne. System powinien mieć zaimplementowane mechanizmy optymalizujące ruch VoIP. Podczas klasyfikacji usług rozwiązanie powinno uwzględniać wartości Differentiated Services Field Codepoints (DSCP) zawarte w nagłówkach IPv4 jak i IPv6. Do kształtowania ruchu wykorzystywane powinny być polisy, którym nadać można odpowiedni priorytet.	
Podstawowa ochrona przed atakami DoS i DDoS	System powinien zapewniać ochronę przed atakami DoS czy DDoS (flood protection).	
Pozostałe	Rozwiązanie powinno oferować możliwość łączenia interfejsów w warstwie L2 (bridge) wraz z STP oraz przekazywaniem ruchu rozgłoszeniowego ARP. Rozwiązanie powinno oferować możliwość tworzenia wielu mostów (multiple bridge) oraz mostów zbudowanych z wielu portów (multiport bridge). System powinien oferować funkcjonalność serwera DHCP dla IPv4 oraz IPv6 i DHCP Relay. System powinien oferować wsparcie dla IEEE 802.3Q VLAN z możliwością konfiguracji niezależnych puli DHCP. Rozwiązanie powinno oferować możliwość agregowania linków fizycznych w oparciu o IEEE 802.3ad (LACP). System powinien oferować wsparcie dla usług Dynamic DNS takich jak np.. DynDNS, ZoneEdit, EasyDNS, DynAcces itp. Rozwiązanie powinno zapewniać wsparcie dla IPv6 wraz z tunelowaniem IP 6in4, 6to4, 4in6 oraz IPv6 rapid deployment (6rd). Rozwiązanie powinno obsługiwać ramki Ethernet o rozmiarze 9000 bajtów (tzw. ramki jumbo). Rozwiązanie powinno umożliwiać tworzenie interfejsów typu alias przypisanych do nadrzędnych interfejsów fizycznych.	
Uwierzytelnianie i obsługa użytkowników	Wymagane uwierzytelnianie użytkowników w trybach Transparent Proxy Authentication (NTLM/Kerberos), SSO (Single Sign On) lub przy użyciu agenta. Rozwiązanie powinno być wyposażone w lokalną bazę użytkowników. System powinien zapewniać możliwość uwierzytelniania w oparciu o takie usługi jak Active Directory, eDirectory, RADIUS, LDAP i TACACS+. Rozwiązanie powinno umożliwiać automatyczne uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w środowiskach opartych o Active Directory. System powinien umożliwiać uwierzytelnianie wieloskładnikowe za pomocą hasła jednorazowego zgodnie z RFC6238 (Time-Based One-Time Password Algorithm). Rozwiązanie powinno umożliwiać uwierzytelnianie i identyfikowanie użytkowników w trybie Single Sign On (SSO) w ramach Windows Terminal Server. System powinien oferować możliwość uwierzytelniania użytkowników za pośrednictwem agenta dostępnego dla platform Windows, Mac OS X, Linux, iOS, Android. Rozwiązanie powinno oferować Captive Portal i wykorzystywać go jako podstawowy mechanizm uwierzytelniania użytkowników w sieci. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny agenta do uwierzytelniania. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik instalacyjny klienta VPN co najmniej dla Windows i MacOS. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo pobrać plik z konfiguracją klienta SSL VPN dla Windows Mac OS, Linux, iOS, Android. Rozwiązanie powinno umożliwiać by uwierzytelnieni użytkownicy mogli samoobsługowo wyświetlić statystyk generowanego przez nich ruchu.	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Koncentrator VPN	System musi umożliwiać konfigurację połączeń typu IPsec site-to-site VPN dla IKE v1 oraz IKE v2. System musi obsługiwać połączenia IPsec szyfrowane przy użyciu AES256 z SHA512 wraz z grupami kluczy Diffie-Hellman: 19 (ecp256), 21 (ecp521) czy 31 (curve25519). System musi obsługiwac połączenia IPsec site-to-site VPN jak i IPsec client-to-site VPN oraz SSL client-to-site VPN. Rozwiązanie musi oferować mechanizmy monitorujące i utrzymujące stan aktywności tuneli IPsec site-to-site VPN. Rozwiązanie musi oferować mechanizmy IPsec VPN Failover i Failback. Urządzenie musi zapewniać możliwość tworzenia wirtualnych interfejsów tunelowych dla IPsec site-to-site VPN i przesyłania ruchu w oparciu o routing statyczny i protokoły routingu dynamicznego. Urządzenie musi oferować mechanizmy IPsec NAT Traversal, Dead Peer Detection oraz Xauth. Urządzenie musi oferować mechanizmy Full Tunnel oraz Split Tunnel dla połaczeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Producent musi dostarczać bezpłatnie oprogramowanie klienckie VPN, które umożliwia realizację połączeń IPsec client-to-site VPN jak i SSL client-to-site VPN. Urządzenie musi obsługiwać połączenia L2TP over IPsec.	
Logowanie i raportowanie	System musi umożliwiać monitorowanie logów ruchu w czasie rzeczywistym. System powinien umożliwiać składowanie oraz archiwizację logów. Logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu. Rozwiązanie musi zapewniać narzędzie do graficznej analizy logów. Rozwiązanie musi udostępniać narzędzie analizy incydentów bezpieczeństwa System powinien zapewniać monitoring ryzyka związanego z działaniem aplikacji sieciowych uruchamianych przez użytkowników np. klasyfikując ryzyko wg. skali. System powinien zapewniać przeglądanie logów przy zastosowaniu funkcji filtrujących. Rozwiązanie powinno umożliwiać wysyłanie raportów via email. Rozwiązanie powinno umożliwiać eksport raportów do plików PDF, HTML i CSV. Rozwiązanie powinno oferować możliwość wysyłania logów systemowych do co najmniej 3 serwerów syslog. System powinien zapewniać podgląd wykorzystania łącza internetowego w ujęciu dziennym, tygodniowym, miesięcznym lub rocznym dla wszystkich lub indywidualnego łącza. System powinien zapewniać podgląd w czasie rzeczywistym wykorzystania łącza i ilości wysyłanych danych w oparciu o użytkownika/adres IP lub aplikację. Rozwiązanie powinno oferować możliwość zanonimizowania danych w raportach. System powinien umożliwiać automatyczne tworzenie raportów według kryteriów i harmonogramów określonych przez administratora.	
System prewencyjny i zaawansowanej ochrony	Ochrona IPS musi opierać się co najmniej na analizie protokołów i bazie minimum 5000 sygnatur. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. Rozwiązanie powinno umożliwiać tworzenie własnych sygnatur IPS. Rozwiązanie powinno umożliwiać selektywne wskazywanie sygnatur i/lub grup sygnatur dla tworzonych przez administratora polis IPS. System ochrony powinien zapewniać wykrywanie, blokowanie i raportowanie prób połączeń z serwerami Command & Control / Botnet.	
Ochrona i kontrola web przed Malware	Rozwiązanie powinno działać jako Transparent Web Proxy zapewniając ochronę przed niebezpiecznymi treściami i szkodliwym oprogramowaniem dystrybuowanym przez HTTP, HTTPS i FTP. Rozwiązanie powinno wykorzystywać silnik antywirusowy pochodzący bezpośrednio od producenta rozwiązania. Wymagane jest aby system automatycznie aktualizował sygnatury zagrożeń. System powinien filtrować pliki na podstawie tak rozszerzeń jak i nagłówków MIME. Rozwiązanie musi zapewniać filtrowanie aktywnych treści takich jak ActiveX, apletów Java czy ciasteczek. Rozwiązanie musi przeprowadzać emulację skryptów Java. Rozwiązanie powinno przeprowadzać tzw. live-lookups t.j. w trybie rzeczywistym weryfikować bazę zagrożeń producenta. System powinien umożliwiać ręczną aktualizację przez pobraną wcześniej bazę sygnatur (Air Gap Pattern Updates)	
Ochrona i kontrola web - Inspecja ruchu SSL/TLS	Rozwiązanie musi umożliwiać inspekcji ruchu SSL wraz z walidacją certyfikatów. Rozwiązanie musi umożliwiać inspekcję ruchu TLS 1.3 bez negocjowania downgrade do TLS 1.2. Wymagane jest by inspekcja ruchu TLS przeprowadzana była niezależnie od użytego portu TCP. Wymagane jest by rozwiązanie umożliwiało blokowanie ruchu tunelowanego przez protokół QUIC (UDP:443). Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków inspekcji ruchu SSL/TLS z uwzględnieniem takich kryteriów jak co najmniej: strefa zapory, adres sieciowy, użytkownik lub grupa użytkowników, usługa czy kategoria web. Rozwiązanie musi umożliwiać tworzenie globalnych wyjątków inspekcji dla co najmniej: wyrażeń regularnych, kategorii stron, domen i subdomen.	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Filtr Web	Filtrowanie stron web powinno być oparte o predefiniowane kategorie z możliwością tworzenia własnych kategorii stron. Rozwiązanie powinno umożliwiać tworzenie granularnych polityk i wyjątków filtra Web z uwzględnieniem takich kryteriów jak co najmniej: użytkownik lub grupa użytkowników, kategoria stron czy harmonogram czasowy. Polityki filtrujące ruch Web powinny umożliwiać wybór akcji co najmniej: zablokuj, ostrzeż, zezwól. System powinien wyświetlać komunikat o przyczynie zablokowania dostępu do strony Web. Administrator powinien mieć możliwość modyfikowamoa treści komunikatu w tym dodania logo organizacji.	
Ochrona i kontrola aplikacji	Rozwiązanie powinno oferować bazę danych opisująca co najmniej 3000 aplikacji. Rozwiązanie powinno zapewniać automatyczną aktualizację sygnatur aplikacji. Rozwiązanie powinno umożliwiać wykrywanie i kontrolę mikro-aplikacji. Rozwiązanie powinno identyfikować aplikacje niezależnie od wykorzystywanego portu czy protokołu, na podstawie głębokiej analizy pakietów. Rozwiązanie powinno umożliwiać blokowanie kategorii aplikacji takich jak np. P2P, Instant Messenger, Proxy and Tunnel, Remote Access, Social Networking, Streaming Media itp. Rozwiązanie powinno umożliwiać tworzenie własnych grup aplikacji co najmniej na potrzeby polityk SD-WAN.	
Ochrona przed nieznanymi zagrożeniami	Rozwiązanie klasy Sandbox do ochrony przez zadrożeniami typu Zero-Day. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików wykonywalnych w tym .exe, .com, .dll. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików dokumentów w tym .doc, .docx, .docm, .rtf. Rozwiązanie umożliwiające dodatkową inspekcję i detonację plików .pdf. Rozwiązanie umożliwiające dodatkową inspekcję i detoancję archiwów w tym .zip, .bzip, .gzip, .rar, .tar, .lha, .lhz, .7z, .cab. Rozwiązanie nie może mieć ograniczeń co do liczby analizowanych plików. System zapewniający agresywną analizę behawioralna kodu uruchamianego w środowiskach testowych Windows i MacOS. System zapewniający analizę pamięci, ruchu sieciowego, operacji na dysku, operacji w rejestrze systemowym po detonacji kodu. System zapewniający ochronę przed exploitami i złośliwym kodem ransomware.	
Gwarancja	Min. 2 lata gwarancji oraz wsparcia technicznego . Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. Wsparcie i licencja na urządzenie, w tym na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Wdrożenie, szkolenie	Zamawiający wymaga podłączenia i zainstalowania we wskazanym miejscu UTM-a, Switch-y oraz AP. Zamawiający wymaga stworzenia przez Wykonawcę projektu segmentacji sieci oraz polityk bezpieczeństwa w myśl wytycznych Zamawiającego a opartych na wytycznych KRI i SZBI, CERT. Zamawiający po zaakceptowaniu projektów wymaga od Wykonawcy zaimplementowania i wdrożenia projektów na dostarczonych urządzeniach. Zamawiający wymaga szkolenia min. 8 godzin z wdrożonego rozwiązania w szczególności z zakresu polityk bezpieczeństwa, administracji i zarządzania.	

2. Sprzętowy appliance zapewniający szyfrowany kanał komunikacji – 1 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	**Wymagane minimalne parametry techniczne**	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ systemu	**Sprzętowy appliance zapewniający szyfrowany kanał komunikacji z nadrzędnym rozwiązaniem klasy UTM/NGFW zaproponowanym w obecnym postępowaniu, fabrycznie nowy.**	
Porty	min.: 1 porty 1 GbE/SFP WAN, 4 porty 1GbE LAN, 2 x port zasilania DC, 2 x USB 3.0, 1x Console (RJ-45 lub DB9)	
Rodzaj urządzenia	switch zarządzalny z wbudowanym VPN z możliwością tunelowania ruchu w warstwie 2 z zaproponowanym urządzeniem UTM	
Przepustowość	min. 250 Mb/s	
WIFI / GSM	Możliwość rozbudowy urządzenia w zintegrowany modułu WIFI lub modułu GSM 3G/4G	
Moc pracy	max. 9 W	
Zarządzanie i utrzymanie	Rozwiązanie musi być w całości zarządzane przez nadrzędne rozwiązanie klasy UTM/NGFW. Plik konfiguracyjny pobierany musi być automatycznie z serwera provisioningu lub z pamięci USB Flash. Rozwiązanie cyklicznie sprawdzać powinno w/w lokalizacje pod kątem obecności nowej wersji konfiguracji. Aktualizacja oprogramowania (firmware) realizowana z poziomu nadrzędnego urządzenia UTM/NGFW. Urządzenie powinno pozwolić na zestawienie szyfrowanego kanału komunikacji z nadrzędnym UTM/NGFW (minimum AES-256). Rozwiązanie po stronie interfejsu WAN winno działać jako klient DHCP z opcją późniejszej zmiany adresu na adres statyczny. Urządzenie powinno obsługiwać modemy 3G/4G oferując przy tym mechanizm WAN Link Failover lub Load Balancing. Interfesjy LAN urządzenia powinny działać jako kolejne interfejsy nadrzędnego rozwiązania klasy UTM/NGFW. Filtrowanie ruchu realizowane być powinno na poziomie nadrzędnego urządzenia UTM/NGFW.	
Gwarancja i wsparcie	Min. 2 lata gwarancji oraz wsparcia technicznego . Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji.	
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Produkt posiadający licencje uprawniające na dożywotnią możliwość korzystania z wszystkich funkcji produktu;	

3. Przełącznik sieciowy zarządzalny 48-portowy - 5 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**	
Porty	min.: 48 porty 1GbE 4 porty SFP+ 10GbE	
Rodzaj urządzenia	switch zarządzalny	
Warstwa	zarządzanie na poziomie warstwy 2 i 3	
Minimalny rozmiar tablicy MAC	32000	
Przepustowość	min. 176Gb/s	
Pamięć robocza	min. 512 MB	
Pamięć bufora	min. 2 MB	
Moc pracy	max. 60W	
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzane przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.	
Typ obudowy	RACK	
Ilość VLAN	min 256	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Gwarancja	5. Min. 2 lata gwarancji oraz wsparcia technicznego . 6. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 7. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 8. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;	

4. Przełącznik sieciowy zarządzalny 24-portowy - 3 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**	
Porty	min.: 24 porty 1GbE, 4 porty SFP+ 10GbE	
Rodzaj urządzenia	switch zarządzalny	
Warstwa	zarządzanie na poziomie warstwy 2 i 3	
Minimalny rozmiar tablicy MAC	16000	
Przepustowość	min. 128Gb/s	
Pamięć robocza	min. 512 MB	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Pamięć bufora	min. 1,5 MB	
Moc pracy	max. 25W	
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.	
Typ obudowy	RACK	
Ilość VLAN	min 256	
Gwarancja	5. Min. 2 lata gwarancji oraz wsparcia technicznego . 6. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 7. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 8. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;	

5. Przełącznik sieciowy zarządzalny 24-portowy PoE – 1 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**	
Porty	min.: 24 porty 1GbE PoE, 4 porty SFP+ 10GbE	
Rodzaj urządzenia	switch zarządzalny	
Warstwa	zarządzanie na poziomie warstwy 2 i 3	
Minimalny rozmiar tablicy MAC	16000	
Przepustowość	min. 128Gb/s	
Pamięć robocza	min. 512 MB	
Pamięć bufora	min. 1,5 MB	
PoE obciążenie portów w standardzie 802.3af/802.3at	24 porty (min. 15,4W) lub 13 protów (30W)	
Moc pracy	max. 410W	
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.	
Typ obudowy	RACK	
Ilość VLAN	min 256	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Gwarancja	5. Min. 2 lata gwarancji oraz wsparcia technicznego . 6. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 7. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 8. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;	

6. Przełącznik sieciowy zarządzalny 8-portowy – 4 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**Przełącznik sieciowy typu core switch, fabrycznie nowy.**	
Porty	min.: 8 porty 1GbE 2 porty SFP 1GbE	
Rodzaj urządzenia	switch zarządzalny	
Warstwa	zarządzanie na poziomie warstwy 2 i 3	
Minimalny rozmiar tablicy MAC	8000	
Przepustowość	min. 20Gb/s	
Pamięć robocza	min. 256 MB	
Pamięć bufora	min. 512 KB	
Moc pracy	max. 12W	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfjes administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.	
Ilość VLAN	min 256	
Gwarancja	5. Min. 2 lata gwarancji oraz wsparcia technicznego . 6. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 7. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 8. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Dokumentacja, inne	1. Zgodność z normami: CE; 2. Zestaw mocowań do montażu w szafie RACK;	

7. Punkt dostępowy AP – 6 szt.

Producent (wpisać) ……..

Model urządzenia (wpisać) ……

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Typ	**Punkt dostępowy AP, fabrycznie nowy**	
Porty	min.: 1GbE PoE+ (802.3at), gniazdo zasilania DC, port konsoli dostępu	

Nazwa komponentu	Wymagane minimalne parametry techniczne	**Parametry sprzętu oferowanego przez Wykonawcę** (jeżeli asortyment proponowany przez Wykonawcę posiada parametry takie same jak wskazane przez Zamawiającego wówczas wpisać **TAK**)
Rodzaj urządzenia	Punkt dostępowy AP WIFI 6	
Anteny wewnętrzne	Min. 2x2:2 dual radio (1 x 2.4 GHz, 1 x 5 GHz)	
Obsługiwanie standardy 802.11	b, n, g, ax, ac	
Szybkość transmisji danych 2,4 GHz	min. 574 Mbps	
Szybkość transmisji danych 5 GHz	min. 1,2 Gbps	
Uchwyt	Dedykowany uchwyt producenta urządzenia do zamocowania na ścianie lub suficie	
Waga	max. 0,9 kg	
Moc pracy	max. 18W	
Zarządzanie, zarządzanie zdalne z chmury	Rozwiązanie powinno być zarządzanie przez webowy graficzny interfejs administratora (Web GUI) działający w czasie rzeczywistym. Webowy graficzny interfejs administratora zabezpieczony protokołem HTTPS z certyfikatem self-signed z możliwością zmiany na podpisany przez zewnętrznego zaufanego wystawcę certyfikatów (External Trusted CA). Rozwiązanie powinno oferować mechanizm uwierzytelnianiania dwuskładnikowego przy połączeniu przez chmurę w oparciu o token sprzętowy lub programowy działający zgodnie z RFC6238 (Time-Based One-Time Password Algorithm) dla zabezpieczenia dostępu do Web GUI jak i VPN. System powinien oferować opcję automatycznego wylogowania sesji administratora po zdefiniowanym czasie bezczynności. System powinien oferować możliwość zdefiniowania polityki bezpieczeństwa dla haseł administratorów w zakresie minimalnej ilości znaków czy złożoności hasła. Rozwiązanie powinno oferować samoobsługowy portal dla użytkowników celem zmniejszenia liczby zadań wymagających udziału administratora, przy czym dostęp oparty winien być o mechanizm dwuskładnikowego uwierzytelniania zgodny z RFC6238 (Time-Based One-Time Password Algorithm). System powinien oferować możliwość integracji z centralnym systemem do zarządzania działającym w chmurze producenta.	
Gwarancja	5. Min. 2 lata gwarancji oraz wsparcia technicznego . 6. Telefoniczna infolinia/linia techniczna producenta przełącznika sieciowego. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki zostanie wskazany przez Wykonawcę w umowie. 7. Możliwość automatycznego pobierania nowego oprogramowania, aktualizacji, poprawek w okresie trwania gwarancji. 8. Wsparcie i licencja na zdalne zarządzania urządzeniami poprzez dedykowaną konsolę producenta rozwiązania - przez okres min. 24 miesiące	
Dodatkowe wymagania	Zamawiający wymaga by Wykonawca wykonał przed dostarczeniem rozwiązania - projektu pokrycia i pojemności zasięgów WIFI z testami i pomiarami na obiekcie oraz miejscach wskazanych przez Zamawiającego. Przekazane mapy pokrycia sygnałem Zamawiającemu odbywa się w trakcie przekazania urządzeń. Zamawiający udostępni obiekt do dokonania wizji lokalnej wraz z pomiarami w uzgodnionym wcześniej terminie.	

Załącznik nr 3 do SWZ

Zamawiający:
Powiat Bytowski
ul. Ks. Dr. Bolesława Domańskiego 2
77-100 Bytów

Wykonawca:

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

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

OŚWIADCZENIE WYKONAWCY
składane na podstawie art. 125 ust. 1 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp)
na potrzeby postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD"**

A. DOTYCZĄCE PODSTAW WYKLUCZENIA Z POSTĘPOWANIA:

(należy postawić znak „x" we właściwym okienku)
☐ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 i art. 109 ust. 1 pkt 1 i 4 ustawy Pzp.

☐ 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 i 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp). Jednocześnie oświadczam/my, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy Pzp podjąłem następujące środki naprawcze:
_____
_____

☐ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie 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 (t.j. Dz. U. z 2024 r. poz. 507 z późn. zm.).

B. 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.

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

Załącznik nr 4 do SWZ

OŚWIADCZENIE WYKONAWCÓW WSPÓLNIE UBIEGAJĄCYCH SIĘ O UDZIELENIE ZAMÓWIENIA

składane na podstawie art. 117 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (dalej jako: ustawa Pzp)

na potrzeby postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD"**

PODMIOTY W IMIENIU KTÓRYCH SKŁADANE JEST OŚWIADCZENIE:

_____
_____

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

_____
_____

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

reprezentowane przez:

_____

(imię, nazwisko, stanowisko/podstawa do reprezentacji)

Działając jako pełnomocnik podmiotów, w imieniu których składane jest oświadczenie oświadczam, że:

Wykonawca (nazwa i adres Wykonawcy):

_____

Zrealizuje następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

_____
_____

Wykonawca (nazwa i adres Wykonawcy):

_____

Zrealizuje następujący zakres świadczenia wynikającego z umowy o zamówienie publiczne:

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.

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

Załącznik Nr 5 do SWZ

FORMULARZ OFERTY DODATKOWEJ

Ja/my niżej podpisani:

……..

(imię i nazwisko, stanowisko/podstawa reprezentacji)

działając w imieniu i na rzecz:

……..
……..

(pełna nazwa Wykonawcy/Wykonawców w przypadku wspólnie ubiegających się o udzielenie zamówienia)

Adres:……....

Województwo:……..……

Kraj:……..……

Regon:……..……

NIP:……..……

Tel.:……..….

Adres skrzynki ePUAP……

Adres e-mail:…….... *(na które Zamawiający ma przesłać korespondencję)*

Oświadczam, że rodzaj Wykonawcy to (informacja do celów statystycznych)*:

☐ *mikroprzedsiębiorstwo*, ☐ *małe przedsiębiorstwo*, ☐ *średnie przedsiębiorstwo*, ☐ *jednoosobowa działalność gospodarcza*, ☐ *osoba fizyczna nieprowadząca działalności gospodarczej*, ☐ *inny rodzaj*

W odpowiedzi na zaproszenie do złożenia oferty dodatkowej do postępowania o udzielenie zamówienia publicznego na: **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”** składamy ofertę dodatkową na realizację przedmiotu zamówienia w zakresie określonym w Specyfikacji Warunków Zamówienia na następujących warunkach:

cena netto za realizacje całego zamówienia wynosi: ……zł

(słownie złotych: ……..)

Podatek VAT…..%, ……..zł

cena brutto za realizacje całego zamówienia wynosi: ……zł

(słownie złotych: ……..)

Oświadczamy, że oferujemy następujący termin wykonania zamówienia:…….. dni **

*** zakreślić właściwe**
**** w wyznaczonym miejscu proszę wskazać deklarowany termin wykonania zamówienia**
(UWAGA!!! W przypadku, gdy Wykonawca, nie wpisze w ofercie terminu wykonania zamówienia, Zamawiający do oceny oferty przyjmie termin wskazany w ofercie złożonej w odpowiedzi na ogłoszenie o zamówieniu)

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

Załącznik Nr 6 do SWZ

PROJEKTOWANE POSTANOWIENIA UMOWY

UMOWA NR …./OR/2024

Zawarta w dniu …… r. pomiędzy :

Powiatem Bytowskim, ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów, NIP: 842-164-30-30, REGON: 770979708

reprezentowanym przez:

……

……

przy kontrasygnacie Skarbnika Powiatu …….

zwanym dalej Zamawiającym

a

……
……
……

zwanym dalej Wykonawcą,

a łącznie zwanymi „Stronami" lub pojedynczo „Stroną".

W wyniku przeprowadzonego postępowania o udzielenie zamówienia publicznego w trybie podstawowym, na podstawie przepisów ustawy z dnia 11.09.2019 r. – Prawo zamówień publicznych (tj. Dz. U. z 2024 poz. 1320 z późn. zm.) na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD"**, zawarto umowę następującej treści:

§ 1

Przedmiot umowy

1. Przedmiotem umowy jest realizacja przez Wykonawcę na rzecz Zamawiającego zadania polegającego na dostawie sprzętu informatycznego w ramach konkursu grantowego „Cyberbezpieczny Samorząd" realizowanego w ramach FUNDUSZY EUROPEJSKICH NA ROZWÓJ CYFROWY 2021-2027 (FERC) Priorytet II: Zaawansowane usługi cyfrowe, Działanie 2.2. – Wzmocnienie krajowego systemu cyberbezpieczeństwa. Przedmiot umowy spełnia wymagania określone w ogłoszeniu o zamówieniu, specyfikacji warunków zamówienia wraz z załącznikami oraz jest zgodny z ofertą Wykonawcy.

2. Wykonawca oświadcza, że sprzęt będący przedmiotem umowy jest nieużywany, fabrycznie nowy, wolny od wad, wykonany w ramach bezpiecznych technologii. Dostarczony sprzęt będzie kompletny oraz będzie posiadał wymagane przepisami prawa certyfikaty.
3. Przekazanie sprzętu informatycznego zostanie potwierdzone protokołem odbioru.
4. Okres gwarancji, parametry dostarczanego sprzętu oraz warunki realizacji zamówienia określa załącznik nr 1 do Specyfikacji Warunków Zamówienia i oferta Wykonawcy. Okres gwarancji liczony będzie od dnia podpisania bez zastrzeżeń przez obie Strony protokołu odbioru.
5. Wykonawca oświadcza, że posiada odpowiednią wiedzę, doświadczenie i dysponuje stosowną bazą do wykonania przedmiotu umowy.

§ 2

Warunki rękojmi za wady oraz gwarancji

1. Wykonawca udziela rękojmi, na warunkach określonych w Kodeksie cywilnym oraz gwarancji jakości na działanie sprzętu na warunkach określonych w umowie oraz karcie gwarancyjnej.
2. Dostarczony w ramach niniejszej umowy sprzęt objęty będzie gwarancją jakości przez okres minimum 24 miesięcy, liczony od dnia podpisania bez zastrzeżeń protokołu odbioru przez Strony.
3. Gwarancji podlegają usterki, wady materiałowe i konstrukcyjne, a także nie spełnianie funkcji użytkowych sprzętu, deklarowanych przez Wykonawcę.
4. Wykonawca nie może odmówić wymiany towaru wadliwego na nowy, jeżeli był już on naprawiany lub gdy wada jest tego rodzaju, że nie rokuje doprowadzenia przedmiotu umowy do jakości, jaką powinien on posiadać w warunkach eksploatacji zgodnych z instrukcją obsługi.
5. Wykonawca zapewnia wymianę wadliwego elementu na nowy w przypadku 3-krotnej jego istotnej awarii. Za istotną awarię przyjmuje się każde uszkodzenie ograniczające funkcjonowanie elementu.
6. Wykonawca jest zwolniony z odpowiedzialności z tytułu gwarancji, jeżeli wykaże, że wady powstały z przyczyn leżących po stronie Zamawiającego, w szczególności z powodu niezgodnego z przeznaczeniem używania sprzętu lub niewłaściwej obsługi.
7. W czasie trwania gwarancji Wykonawca zapewni odbiór sprzętu, który uległ awarii z siedziby Zamawiającego nie później niż do następnego dnia roboczego, do godz. 15:30 od momentu otrzymania pisemnego lub telefonicznego zgłoszenia wady lub usterki przez Zamawiającego. Zgłoszenie awarii sprzętu zostanie każdorazowo przesłane drogą telefoniczną na nr …….. lub mailowo na adres……
8. Link do strony producenta na której znajduje się nr telefonu oraz adres mailowy na który można zgłaszać usterki:……...
9. Wykonawca zobowiązany jest do świadczenia usług gwarancyjnych na poniższych zasadach:
   1) Usługa gwarancyjna będzie świadczona przez producenta lub przez jego autoryzowany serwis,
   2) Wykonawca maksymalnie w ciągu 10 dni roboczych od momentu otrzymania zgłoszenia, dokona skutecznej naprawy sprzętu,

3) Jeśli czas usunięcia awarii będzie przekraczał 10 dni roboczych, Wykonawca niezwłocznie dostarczy Zamawiającemu na czas naprawy sprzęt zastępczy o nie gorszych parametrach technicznych wraz ze sterownikami umożliwiającymi korzystanie z tego urządzenia.

10. Wykonawca dokona odbioru, naprawy oraz zwrotu sprzętu na własny koszt i ryzyko. Wykonawca ponosi pełną odpowiedzialność za ewentualną utratę lub zniszczenie sprzętu po odebraniu go do naprawy z siedziby Zamawiającego.
11. Okres obowiązywania gwarancji będzie automatycznie wydłużany o czas naprawy lub wymiany sprzętu na nowy. Okres gwarancji wymienionego elementu sprzętu ponownie rozpoczyna swój bieg.

§ 3

Termin i warunki realizacji umowy

1. Sprzęt zostanie dostarczony w terminie…. dni kalendarzowych od dnia zawarcia umowy.
2. Wykonawca dostarczy przedmiot umowy do siedziby Zamawiającego, tj. Starostwa Powiatowego w Bytowie, ul. Ks. dr. B. Domańskiego 2, 77-100 Bytów.
3. Dostawa nastąpi w dni robocze w godzinach od 8:00 do 15:00.
4. Wykonawca zobowiązuję się wraz z dostawą dostarczyć:
   1) instrukcję w języku polskim;
   2) dokument gwarancyjny;
   3) deklaracje zgodności CE lub certyfikat CE (z wyłączeniem punktów dostępowych AP);
   4) dokumenty określające zasady świadczenia usług przez autoryzowany serwis w okresie gwarancyjnym i pogwarancyjnym.
5. Wykonawca na pięć dni przed zaplanowaną dostawą poinformuje Zamawiającego o gotowości dostawy sprzętu do siedziby Zamawiającego na adres wskazany w § 2 ust. 7 umowy. Strony uzgodnią termin dostawy oraz termin przeprowadzenia szkolenia.
6. Jeżeli w trakcie odbioru stwierdzona zostanie wada przedmiotu umowy, Zamawiający może odmówić jego odbioru, a Wykonawca zobowiązany będzie, w zależności od wyboru Zamawiającego, do wymiany wadliwego przedmiotu umowy na wolny od wad, w terminie uzgodnionym protokolarnie przez strony umowy, przy czym termin ten nie może być dłuższy niż 14 dni roboczych od dnia poinformowania Wykonawcy o stwierdzeniu wady. W przypadku stwierdzenia braków ilościowych w dostawie, Wykonawca jest zobowiązany do ich uzupełnienia w terminie uzgodnionym protokolarnie przez strony umowy, nie dłuższym jednak niż 7 dni roboczych od dnia stwierdzenia braków.
7. Ze strony Zamawiającego osobą upoważnioną do kontaktu i odbioru przedmiotu umowy jest ……. tel.:……., e-mail: …….
8. Ze strony Wykonawcy osobą upoważnioną do kontaktowania się z Zamawiającym jest …… tel.:……., e-mail: …….

§ 4

Wynagrodzenie za wykonanie umowy

1. Cena za przedmiot umowy, określona przez Wykonawcę w złożonej ofercie wynosi łącznie netto ….zł (słownie:…) z podatkiem VAT (%) w wysokości ….zł, łącznie brutto …zł (słownie:…).
2. Ceny za poszczególne elementy objęte zamówieniem kształtują się następująco:
   1) UTM - dwa urządzenia działające redundantnie w układzie aktiv - passiv - 1 kpl. ……...
   2) Sprzętowy appliance zapewniający szyfrowany kanał komunikacji – 1 szt……....
   3) Przełącznik sieciowy zarządzalny 48-portowy (cena za 5 szt.) ……
   4) Przełącznik sieciowy zarządzalny 24-portowy (cena za 3 szt.) ……
   5) Przełącznik sieciowy zarządzalny 24-portowy PoE – 1 szt. ……
   6) Przełącznik sieciowy zarządzalny 8-portowy (cena za 4 szt.) ……..
   7) Punkt dostępowy AP (cena za 6 szt.) ……
3. Wskazane w ust. 1 niniejszego paragrafu wynagrodzenie jest ostateczne i niezmienne do końca realizacji przedmiotu umowy oraz obejmuje wszelkie koszty poniesione przez Wykonawcę przy realizacji przedmiotu umowy z uwzględnieniem wszystkich opłat i podatków w tym podatku VAT. Cena musi obejmować koszty wydania i odebrania przedmiotu umowy, w szczególności koszty i opłaty związane z dostarczeniem przedmiotu umowy do siedziby Zamawiającego, opłaty za transport, załadunek, wyładunek, oraz dokumentację niezbędną do prawidłowego użytkowania przedmiotu umowy oraz realizację obowiązków spoczywających na Wykonawcy z tytułu rękojmi i gwarancji w tym serwis w okresie gwarancyjnym.

§ 5

Warunki płatności

1. Zapłata za dostarczony sprzęt, o którym mowa w § 1 nastąpi jednorazowo w terminie 14 dni od daty otrzymania oryginału faktury VAT wystawionej na Powiat Bytowski, ul. Ks. dr. Bolesława Domańskiego 2, 77-100 Bytów, NIP 842-164-30-30, wraz z podpisanym protokołem odbioru. Sporządzony protokół odbioru dostarczonego sprzętu, stwierdzać będzie jego zgodność z załącznikiem nr 1 do Specyfikacji Warunków Zamówienia i ofertą Wykonawcy. Faktura wraz z protokołem odbioru wystawiona zostanie przez Wykonawcę w dniu dostawy.
2. Należności określone na fakturze wynikające z niniejszej umowy zostaną przekazane przez Zamawiającego przelewem na konto Wykonawcy wskazane przez niego na fakturze. Równocześnie Wykonawca oświadcza, że numer rachunku bankowego, który zostanie wskazany na fakturze jest numerem rachunku bankowego Wykonawcy, otwartym w związku z prowadzoną działalnością gospodarczą oraz znajduję się w wykazie, o którym mowa w art. 96b ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług.

3. Wykonawca oświadcza, że jego firma jest zarejestrowanym, czynnym podatnikiem VAT, nie zawiesiła ani nie zaprzestała wykonywania działalności gospodarczej i zobowiązuje się do niezwłocznego powiadomienia o zmianach powyższego statusu.
4. Wykonawca oświadcza, że VAT wynikający z faktury zostanie terminowo rozliczony z organem podatkowym oraz, że nie posiada żadnych zaległości w zobowiązaniach w stosunku do Skarbu Państwa, które uniemożliwiłyby jego zapłatę.
5. Za dzień zapłaty uważany będzie dzień obciążenia rachunku Zamawiającego.

§ 6

Kary umowne

1. W wypadku niewykonania lub nienależytego wykonania umowy lub jej części Zamawiającemu przysługiwać będzie prawo do naliczenia Wykonawcy następujących kar umownych:
   a) w przypadku odstąpienia od umowy z przyczyn leżących po stronie Wykonawcy w wysokości 10% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy;
   b) w wysokości 0,5% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy, za każdy dzień zwłoki w dostawie sprzętu liczony od terminu wyznaczonego w § 3 ust. 1;
   c) za zwłokę w usunięciu wad i usterek stwierdzonych przy odbiorze lub zgłoszonych w okresie gwarancji i rękojmi w wysokości 1,0% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy za każdy dzień zwłoki,
   d) w wysokości 5% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy, za niedostarczenie certyfikatu o którym mowa w § 3 ust. 4 pkt 3.
2. Zamawiający zobowiązuje się zapłacić kary umowne w przypadku odstąpienia od umowy z przyczyn leżących po stronie Zamawiającego w wysokości 10% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy.
3. Łączna wartość kar umownych jakiej mogą dochodzić Strony nie może przekroczyć 20% wynagrodzenia umownego brutto określonego w § 4 ust. 1 umowy.
4. W sytuacji gdy kary umowne przewidziane w § 6 ust. 1 i 2 nie pokrywają poniesionych szkód, stronom przysługiwać będzie prawo żądania odszkodowania na zasadach ogólnych.
5. Wykonawca będzie zobowiązany do zapłaty należności wynikających z naliczenia kar umownych w terminie 14 dni od dnia otrzymania noty obciążeniowej.
6. Wykonawca wyraża zgodę na potrącenie kar umownych z należnego mu wynagrodzenia wynikającego z wystawionej faktury.

§ 7

Zmiany umowy

1. Zamawiający dopuszcza możliwość dokonywania wszelkich nieistotnych zmian umowy. Zmiana istotna niniejszej umowy wymaga formy pisemnej pod rygorem nieważności.

2. Zmiany istotnych postanowień umowy w stosunku do treści oferty mogą dotyczyć przedmiotu umowy w zakresie zmiany parametrów technicznych, wersji oprogramowania, modelu urządzenia w przypadku:
   e) jeżeli niezbędna jest zmiana sposobu wykonania zobowiązania, o ile zmiana taka jest korzystna dla Zamawiającego oraz konieczna w celu prawidłowej realizacji umowy,
   f) konieczności dostosowania postanowień do zmian powszechnie obowiązujących przepisów prawa z uwagi na brak możliwości realizacji umowy według pierwotnej jej treści lub z uwagi na rażącą stratę grożącą jednej ze stron.
3. Zmiany wysokości wynagrodzenia w stosunku do treści oferty mogą nastąpić w przypadku zmiany obowiązującej stawki podatku VAT – zmiany mogą nastąpić wyłącznie w przypadku i w terminie wejścia w życie ustawowej zmiany stawki VAT (zamiana ceny związana z ustawową zmianą wysokości VAT może obejmować wyłącznie zakres określony w specyfikacji i w ofercie, a jeszcze nie wykonany).
4. Strony umowy wnioskują o jej zmianę, jedna Strona przedkłada drugiej pisemne uzasadnienie konieczności wprowadzenia zmian do umowy.
5. Wszystkie powyższe postanowienia stanowią katalog zmian, na które Strony umowy mogą wyrazić zgodę. Nie stanowią jednocześnie zobowiązania do wyrażenia takiej zgody.
6. Wszystkie istotne zmiany treści umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy mogą być dokonywane wyłącznie w przypadkach określonych powyżej i wymagają pisemnego aneksu pod rygorem nieważności takiej zmiany.

§ 8

Podwykonawstwo

1. Wykonawca może powierzyć wykonanie części zamówienia będącego przedmiotem niniejszej umowy podwykonawcom.
2. Wykonawca na dzień zawarcia niniejszej umowy zgodnie z oświadczeniem złożonym w trakcie postępowania o udzielenie zamówienia, zamierza powierzyć niżej wskazanym podwykonawcom następujący zakres umowy:
   1) ….....…
   2) ….....
3. Wykonawca ponosi pełną odpowiedzialność za części przedmiotu umowy, którą wykonuje przy pomocy podwykonawców.
4. Wykonawca ponosi odpowiedzialność na zasadach ogólnych za jakość i terminowość prac, które realizuje przy pomocy podwykonawców.
5. W przypadku powierzenia wykonania części przedmiotu umowy podwykonawcom Wykonawca wraz z fakturą przedstawi Zamawiającemu pisemny wykaz podwykonawców z ich udziałem finansowym i rzeczowym oraz potwierdzenie zapłaty wymagalnego wynagrodzenia podwykonawcom w zakresie wszelkich zobowiązań wynikających z udziału podwykonawcy

w realizacji części umowy objętej fakturą. Brak potwierdzenia zapłaty wynagrodzenia podwykonawcom wstrzymuje dokonanie zapłaty faktury.

§ 9

Odstąpienie od umowy

1. Zamawiającemu przysługuje prawo odstąpienia od umowy:
   1) gdy Wykonawca pozostaje w zwłoce w terminie wykonania przedmiotu umowy, który został określony w § 3 ust. 1 i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami w terminie 7 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności.
   2) gdy Wykonawca nie realizuje zamówienia zgodnie z umową lub też nienależycie wykonuje swoje zobowiązania umowne i pomimo pisemnego lub przesłanego drogą elektroniczną wezwania otrzymanego od Zamawiającego nie przystąpił do realizacji umowy zgodnie z jej warunkami w terminie 7 dni od dnia stwierdzenia przez Zamawiającego danej okoliczności.
   3) w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu. W takim wypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu wykonania części umowy. § 6 ust. 2 nie ma zastosowania.
2. Odstąpienie od umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i winno zawierać uzasadnienie.

§ 10

Postanowienia końcowe

1. W sprawach nie uregulowanych niniejszą umową zastosowanie mają przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych i Kodeksu cywilnego.
2. Wszelkie spory mogące powstać na tle obowiązywania i realizowania niniejszej umowy rozstrzygane będą przez sąd powszechny właściwy dla miejsca położenia siedziby Zamawiającego.
3. Umowę sporządzono w czterech jednobrzmiących egzemplarzach, jeden egzemplarz dla Wykonawcy oraz trzy dla Zamawiającego.

§ 11

Integralną część umowy stanowią:

1. Specyfikacja Warunków Zamówienia.
2. Oferta Wykonawcy.

Zamawiający: **Wykonawca**

Załącznik nr 7 do SWZ

Zamawiający:
Powiat Bytowski
ul. Ks. Dr. Bolesława Domańskiego 2
77-100 Bytów

Wykonawca:
_____
(pełna nazwa/firma, adres, w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)
reprezentowany przez:
_____
(imię, nazwisko, stanowisko/podstawa do reprezentacji)

OŚWIADCZENIE WYKONAWCY [1]
o aktualności informacji zawartych w oświadczeniu o którym mowa w art. 125 ust. 1 Pzp w zakresie braku podstaw do wykluczenia z postępowania

na potrzeby postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD”**. Przystępując do udziału w ww. postępowaniu o udzielenie zamówienia publicznego oświadczam, że uczestniczę w postępowaniu jako:
(należy postawić znak „x” we właściwym okienku)

☐ Wykonawca samodzielnie ubiegający się o udzielenie zamówienia,
☐ Wykonawca ubiegający się o udzielenie zamówienia wspólnie z innymi Wykonawcami,

OŚWIADCZENIE DOTYCZĄCE PODSTAW WYKLUCZENIA
(należy postawić znak „x” we właściwym okienku)

☐ Oświadczam, że informacje zawarte w załączonym do oferty, złożonym przeze mnie oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp, w zakresie podstaw wykluczenia są nadal aktualne, a zatem:
☐ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 i art. 109 ust. 1 pkt 1 i 4 ustawy Pzp.
☐ Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. _____ ustawy Pzp (podać mająca zastosowanie podstawę wykluczenia spośród wymienionych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 4 ustawy Pzp). Jednocześnie oświadczam, że aktualnie są podjęte przeze mnie środki naprawcze, opisane w załączonym do mojej/naszej oferty oświadczeniu, o którym mowa w art. 125 ust. 1 ustawy Pzp.
☐ Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie 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 (t.j. Dz. U. z 2024 r. poz. 507 z późn. zm.).

☐ 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 przedstawieniu informacji.

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

[1] Zgodnie z art. 274 ust. 1 ustawy Pzp Wykonawca, składa oświadczenie na wezwanie Zamawiającego do złożenia podmiotowego środka dowodowego.

Załącznik nr 8 do SWZ

OŚWIADCZENIE [1]

o przynależności lub braku przynależności do tej samej grupy kapitałowej w zakresie art. 108 ust. 1 pkt 5 ustawy Pzp

na potrzeby postępowania o udzielenie zamówienia publicznego na **DOSTAWĘ SPRZĘTU INFORMATYCZNEGO W RAMACH KONKURSU GRANTOWEGO „CYBERBEZPIECZNY SAMORZĄD"**

Ja niżej podpisany

_____

(imię i nazwisko)

działając w imieniu i na rzecz:

_____

(pełna nazwa oraz adres siedziby Wykonawcy)

(należy postawić znak „x" we właściwym okienku)

☐ oświadczam, że nie należę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, z innym Wykonawcą, który złożył odrębną ofertę w niniejszym postępowaniu, w zakresie określonym art. 108 ust. 1 pkt 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych. W związku z powyższym, na dzień składania ofert nie podlegam wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 108 ust. 1 pkt 5 ustawy Pzp.

☐ oświadczam, że należę do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, z innym Wykonawcą, który złożył odrębną ofertę w niniejszym postępowaniu, w zakresie określonym art. 108 ust.1 pkt 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych oraz przedstawiamy dokumenty potwierdzające przygotowanie oferty w niniejszym postępowaniu niezależnie od Wykonawcy należącego do tej samej grupy kapitałowej.

Lista podmiotów należących do grupy kapitałowej Wykonawcy:

1. _____
2. _____

w związku z powyższym na dzień składania ofert nie podlegam wykluczeniu z postępowania o udzielenie zamówienia na podstawie art. 108 ust. 1 pkt 5 ustawy Pzp.

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