|  |
| --- |
| *Sygnatura sprawy:***11/ZP/21** |

|  |
| --- |
| SPECYFIKACJA WARUNKÓW ZAMÓWIENIA |
| ZAMAWIAJĄCY:Akademia Marynarki Wojennej**im. Bohaterów Westerplatte*****ul. inż. Śmidowicza 69******81-127 GDYNIA***www.amw.gdynia.pl |
|  |
| ZAPRASZA DO ZŁOŻENIA OFERTY W POSTĘPOWANIU LICENCJA NA SYSTEM OCHRONY ANTYWIRUSOWEJ. WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO. CERTYFIKAT SSL WILDCARD. SERWER USŁUG PULPITU ZDALNEGO.TRYB UDZIELENIA ZAMÓWIENIA**:** przetarg nieograniczonyPodstawa prawna: Ustawa z dnia 11.09.2019 r. - Prawo zamówień publicznych(Dz. U. z 2019 r. poz. 2019 z późn. zm.) |
|  |
|  **ZATWIERDZAM** **Rektor-komendant** **kontradmirał prof. dr hab. Tomasz SZUBRYCHT**dnia …… …………….. 2021 r**.**Opracowała: Sekcja Zamówień Publicznych |
| **ROZDZIAŁ 1** | **Nazwa oraz adres Zamawiającego, numer telefonu, adres poczty elektronicznej oraz strony internetowej prowadzonego postępowania** |  |
| Nazwa: | Akademia Marynarki Wojennej |
| Adres: | **ul. inż. Śmidowicza 69** |
|  | **81 – 127 GDYNIA** |
| Numer telefonu: | **261262537** |
| Godziny urzędowania: | **od godz. 7.30 do godz. 15.30** |
| NIP: | **586-010-46-93** |
| REGON: | **190064136** |
| Adres poczty elektronicznej: | przetargi@amw.gdynia.pl  |
| Adres strony internetowej:Adres strony internetowej prowadzonego postępowania | [www.amw.gdynia.pl](http://www.amw.gdynia.pl/)platforma zakupowahttps://platformazakupowa.pl/ |
| *Wykonawca zamierzający wziąć udział w postępowaniu o udzielenie zamówienia publicznego, zobowiązany jest posiadać konto na platformie zakupowej.**Zarejestrowanie i utrzymanie konta na platformie zakupowej oraz korzystanie z platformy jest bezpłatne.*

|  |  |
| --- | --- |
| **ROZDZIAŁ 2** | **Adres strony internetowej, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem o udzielenie zamówienia** |

platforma zakupowa<https://platformazakupowa.pl/>

|  |  |
| --- | --- |
| **ROZDZIAŁ 3** | **Tryb udzielenia zamówienia** |

 |

Postępowanie o udzielenie zamówienia prowadzone jest w **trybie nieograniczonym** na podstawie art. 132 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych oraz zgodnie z wymogami określonymi w niniejszej Specyfikacji Warunków Zamówienia, zwanej dalej „SWZ”.

|  |  |
| --- | --- |
| **ROZDZIAŁ 4** | **Opis przedmiotu zamówienia** |

1. Wspólny Słownik Zamówień (CPV):

 **Część I: CPV** 48760000-3 Pakiety oprogramowania do ochrony antywirusowej

 **CPV** 72000000-5 Usługi informatyczne

 **Część II**: **CPV** 48210000-3 Pakiety oprogramowania dla sieci

 **CPV** 48820000-2 Serwery

1. Przedmiotem zamówienia jest dostawa licencji na system ochrony antywirusowej i usługa wsparcia technicznego (część I) oraz dostawa Certyfikatu SSL Wildcard z roczną subskrypcją, licencji Microsoft zapewniających zdalny dostęp do serwerów Windows, licencji Microsoft – system operacyjny Windows Server Standard i serwera usług pulpitu zdalnego (część II) **(załącznik nr 2 do SWZ)**.
2. **Zamawiający informuje, że podstawą do wstępu cudzoziemców na teren Akademii przed przystąpieniem do realizacji umowy jest otrzymanie pozwolenia jednorazowego na wjazd w wyniku uzyskania pozytywnej opinii Dyrektora Zarządu Operacyjnego Służby Kontrwywiadu Wojskowego poprzez Szefa Agencji Bezpieczeństwa Wewnętrznego lub otrzymanie jednorazowego pozwolenia wydanego przez Dowództwo Generalne Rodzajów Sił Zbrojonych** *(wymóg uzyskania zgody SKW zgodnie z zasadami wynikającymi z decyzji nr 19/MON Ministra Obrony Narodowej z dnia 24.01.2017r. w sprawie organizowania współpracy międzynarodowej w resorcie obrony narodowej (Dz. Urz. MON poz. 18).*

**Zamawiający zastrzega, że procedura wyrażenia zgody na realizację umowy przez pracowników nie posiadających obywatelstwa polskiego może potrwać około miesiąca.
Z powyższego Wykonawcy nie przysługują żadne roszczenia związane ze zmianą terminu wykonania przedmiotu zamówienia.**

**Wykonawca przed przystąpieniem do realizacji Umowy zapozna się z procedurami wstępu na teren Akademii obowiązujących u Zamawiającego.**

|  |  |
| --- | --- |
| **ROZDZIAŁ 5** | **Informacje o przedmiotowych środkach dowodowych** |

Zamawiający przewiduje przedmiotowy środek dowodowy w postaci wypełnionego załącznika nr 1a ( parametry oferowane serwera).

|  |  |
| --- | --- |
| **ROZDZIAŁ 6** | **Termin wykonania zamówienia** |

Termin realizacji zamówienia: przewidywany termin realizacji zamówienia

**Część I:** 29.06.2021 r. – licencje

 01.07.2021 r. – 30.06.2022 r. – wsparcie techniczne

 **Część II:** 30.08.2021 r. – certyfikat, serwer i oprogramowanie

|  |  |
| --- | --- |
| **ROZDZIAŁ 7** | **Podstawy wykluczenia, o których mowa w art. 108 ust. 1** |

1. Z postępowania o udzielenie zamówienia wyklucza się z zastrzeżeniem art. 110 ust. 2 ustawy Prawo zamówień publicznych, Wykonawcę̨:

będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:

1. udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
2. handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
3. którym mowa w art. 228–230a, art. 250a Kodeksu karnego lub w art. 46 lub art. 48 ustawy z dnia 25 czerwca 2010 r. o sporcie,
4. 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,
5. charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
6. powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. poz. 769),
7. 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,
8. 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;
9. 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 1.1;
10. wobec którego wydano prawomocny wyrok sadu lub ostateczną decyzję administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba ze Wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postepowaniu 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;
11. wobec którego prawomocnie orzeczono zakaz ubiegania się̨ o zamówienia publiczne;
12. jeżeli Zamawiający może stwierdzić́, 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 postepowaniu, chyba że wykażą̨, że przygotowali te oferty lub wnioski niezależnie od siebie;
13. jeżeli, w przypadkach, o których mowa w art. 85 ust. 1 pzp, 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 być́ wyeliminowane w inny sposób niż̇ przez wykluczenie Wykonawcy z udziału w postępowaniu
o udzielenie zamówienia.
14. Wykonawca może zostać wykluczony przez Zamawiającego na każdym etapie postępowania o udzielenie zamówienia (art. 110 ust. 1 ustawy Prawo zamówień publicznych).

|  |  |
| --- | --- |
| **ROZDZIAŁ 8** | **Informacje o warunkach udziału w postępowaniu o udzielenie zamówienia** |

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy **spełniają warunki udziału w postępowaniu** dotyczące:
2. **zdolności do występowania w obrocie gospodarczym**

Opis spełnienia warunku:

Wykonawca musi posiadać zdolność do występowania w obrocie gospodarczym tj. być wpisanym do Krajowego Rejestru Sądowego lub Centralnej Ewidencji i Informacji

o Działalności Gospodarczej w zakresie art. 109 ust. 1 pkt 4 ustawy dnia 11.09.2019 r. - Prawo zamówień publicznych **(dotyczy części I i II)**.

1. **uprawnień do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów**

Opis spełnienia warunku:

Dokument wystawiony przez producenta lub dystrybutora oferowanego oprogramowania potwierdzający, że jest on autoryzowanym partnerem producenta oferowanego oprogramowania uprawnionym do sprzedaży licencji i wdrażania oferowanego oprogramowania **(dotyczy części I)**.

1. **sytuacji ekonomicznej lub finansowej**

Opis spełnienia warunku:

Zamawiający odstępuje od opisu sposobu dokonywania oceny spełnienia warunków w tym zakresie. Zamawiający nie dokona oceny spełnienia warunków udziału w postępowaniu.

1. **zdolności technicznej lub zawodowej**

Opis spełnienia warunku:

* + - * 1. **Wykonawca musi wykazać się doświadczeniem** **(załącznik nr 5) – dotyczy części I** tj. wykaz dostaw i usług wykonanych, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych, w okresie ostatnich 3 lat, a jeżeli okres prowadzenia działalności jest krótszy – w tym okresie, wraz z podaniem ich wartości, przedmiotu, dat wykonania i podmiotów, na rzecz których dostawy i usługi zostały wykonane lub są wykonywane, oraz załączeniem dowodów określających, czy te dostawy i usługi zostały wykonane lub są wykonywane należycie, przy czym dowodami, o których mowa, są referencje bądź inne dokumenty sporządzone przez podmiot, na rzecz którego dostawy i usługi zostały wykonane, a w przypadku świadczeń powtarzających się lub ciągłych są wykonywane, a jeżeli wykonawca z przyczyn niezależnych od niego nie jest w stanie uzyskać tych dokumentów – oświadczenie wykonawcy; w przypadku świadczeń powtarzających się lub ciągłych nadal wykonywanych referencje bądź inne dokumenty potwierdzające ich należyte wykonywanie powinny być wystawione w okresie ostatnich 3 miesięcy;

Za spełnienie tego warunku Zamawiający uzna wykonanie minimum 1 zamówienia obejmującego łącznie (nie dopuszcza się przedłożenia kilku dokumentów na cząstkowe zakresy wymienione poniżej) **na część I**:

• Dostarczenie licencji lub subskrypcji oprogramowania antywirusowego do ochrony serwerów i stacji roboczych z konsolą centralnego zarządzania dla minimum 500 urządzeń,

• Świadczenie wsparcia technicznego dla systemu ochrony antywirusowej ESET lub innego, oferowanego przez wykonawcę systemu antywirusowego w przypadku oferowania systemu równoważnego do ESET dla minimum 500 urządzeń

• Świadczenie wsparcia technicznego dla środowiska serwerowego opartego o Windows Serwer składającego się z minimum dwóch serwerów poczty Exchange 2010 skonfigurowanych w DAG, serwera plików, serwera wydruków, klastra środowiska wirtualnego Hyper-V, serwera backupu System Center Data Protection Manager 2012, kontrolerów domeny, serwerów fizycznych i macierzy dyskowych.

* + - * 1. **Wykonawca musi dysponować osobami** **(na część I załącznik nr 6)** **(dotyczy części I),** które zostaną skierowane przez wykonawcę do realizacji zamówienia publicznego, w szczególności odpowiedzialnych za świadczenie usług, kontrolę jakości lub kierowanie robotami budowlanymi, wraz z informacjami na temat ich kwalifikacji zawodowych, uprawnień, doświadczenia i wykształcenia niezbędnych do wykonania zamówienia publicznego, a także zakresu wykonywanych przez nie czynności oraz informacją o podstawie do dysponowania tymi osobami;.

Za spełnienie tego warunku zamawiający uzna dysponowanie przez wykonawcę osobami:

* Minimum 1 osobą, posiadającą certyfikat potwierdzający umiejętność instalowania
i konfigurowania oferowanego oprogramowania. Certyfikat musi być wystawiony przez producenta lub autoryzowanego dystrybutora oferowanego oprogramowania lub autoryzowany przez niego ośrodek szkoleniowy **(na część I załącznik nr 7).**
* Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Windows Serwer 2008 lub nowszego **(na część I załącznik nr 8).**
* Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Microsoft Exchange 2010 lub nowszego **(na część I załącznik nr 9).**
* Minimum 1 osobą posiadającą certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność wdrażania i administrowania środowiskiem wirtualnym opartym o Microsoft Hyper-V **(na część I załącznik nr 10).**
* Dysponować 1 osobą posiadającą certyfikat potwierdzający umiejętność świadczenia usług serwisowych zgodnie z ITIL (np. ITIL Foundation) **(na część I załącznik nr 11).**

2. Dysponować punktem serwisowym umożliwiającym dotarcie do siedziby Zamawiającego
 w ciągu 1 godziny od zgłoszenia serwisowego **(na część I załącznik nr 12).**

3. Dysponować portalem/systemem serwisowym w którym Zamawiający będzie mógł dokonywać zgłoszeń serwisowych i widzieć szczegóły ich realizacji **(na część I załącznik nr 13).**

**Ocena spełnienia warunku będzie dokonywana metodą 0-1, tj. spełnia/nie spełnia
w oparciu o dokument dołączony do oferty bądź po jego uzupełnieniu na wezwanie Zamawiającego.**

|  |  |
| --- | --- |
| **ROZDZIAŁ 9** | **Wykaz podmiotowych środków dowodowych** |

1. Oświadczenie o niepodleganiu wykluczeniu i spełnianiu warunków udziału w postępowaniu składane są na formularzu jednolitego europejskiego dokumentu zamówienia, w skrócie **„JEDZ”**, sporządzonym zgodnie ze wzorem standardowego formularza określonego w rozporządzeniu wykonawczym Komisji (UE) 2016/7 z dnia 5 stycznia 2016 r. ustanawiającym standardowy formularz jednolitego europejskiego dokumentu zamówienia (Dz. Urz. UE L 3 z 06.01.2016, str. 16).

W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, JEDZ składa każdy z Wykonawców.

Sporządzając oświadczenie JEDZ można skorzystać z nieodpłatnego narzędzia wspierającego Zamawiających i Wykonawców w stosowaniu standardowego formularza JEDZ w wersji elektronicznej, udostępnionego przez Urząd Zamówień Publicznych pod adresem http://espd.uzp.gov.pl/.

|  |  |
| --- | --- |
| **ROZDZIAŁ 10** | **Informacja o środkach komunikacji elektronicznej, przy użyciu których Zamawiający będzie komunikował się z Wykonawcami, oraz informacje o wymaganiach technicznych i organizacyjnych sporządzania, wysyłania i odbierania korespondencji elektronicznej** |

1. Postępowanie prowadzone jest w języku polskim w formie elektronicznej za pośrednictwem platformy zakupowej (dalej jako „Platforma”) pod adresem:

https://platformazakupowa.pl/

1. W celu skrócenia czasu udzielenia odpowiedzi na pytania preferuje się, aby komunikacja między Zamawiającym a Wykonawcami, w tym wszelkie oświadczenia, wnioski, zawiadomienia oraz informacje, przekazywane były w formie elektronicznej 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](http://platformazakupowa.pl/) poprzez kliknięcie przycisku „Wyślij wiadomość do Zamawiającego”, po których pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

1. Zamawiający będzie przekazywał wykonawcom informacje w formie elektronicznej za pośrednictwem [platformazakupowa.pl](http://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 w formie elektronicznej za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl/) do konkretnego Wykonawcy.
2. 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.
3. Zamawiający, zgodnie z art. 67 ustawy Prawo Zamówień Publicznych, określa wymagania techniczne i organizacyjne sporządzania, wysyłania i odbierania korespondencji elektronicznej, tj.:
	1. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s,
	2. komputer klasy PC lub MAC o następującej konfiguracji: pamięć RAM min. 2 GB, procesor Intel Pentium IV 2 GHZ lub nowszy, jeden z systemów operacyjnych - MS Windows wersja 7, Mac Os x 10.4, Linux, lub ich nowsze wersje,
	3. zainstalowana dowolna przeglądarka internetowa, w przypadku Internet Explorer minimalnie wersja 10.0,
	4. włączona obsługa JavaScript,
	5. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf,
	6. Platformazakupowa.pl działa według standardu przyjętego w komunikacji sieciowej - kodowanie UTF8,
	7. 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.
4. Wykonawca, przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
	1. akceptuje warunki korzystania z [platformazakupowa.pl](https://platformazakupowa.pl/) określone w Regulaminie zamieszczonym na stronie internetowej [pod linkiem](https://platformazakupowa.pl/strona/1-regulamin) w zakładce „Regulamin" oraz uznaje go za wiążący,
	2. zapoznał i stosuje się do Instrukcji składania ofert/wniosków dostępnej [pod linkiem](https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view).
5. **Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny
z Instrukcją korzystania z** [**platformazakupowa.pl**](http://platformazakupowa.pl/), w szczególności za sytuację, gdy Zamawiający zapozna się z treścią oferty przed upływem terminu otwarcia 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 określony w art. 221 Ustawy Prawo Zamówień Publicznych.

1. Zamawiający informuje, że instrukcje korzystania z [platformazakupowa.pl](http://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](http://platformazakupowa.pl/) znajdują się w zakładce „Instrukcje dla Wykonawców" na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
2. Zamawiający nie przewiduje sposobu komunikowania się z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej, wskazanych w SWZ.

|  |  |
| --- | --- |
| **ROZDZIAŁ 11** | **Informacja o sposobie komunikowania się Zamawiającego z Wykonawcami w inny sposób niż przy użyciu środków komunikacji elektronicznej w przypadku zaistnienia jednej z sytuacji określonych w art. 65 ust. 1, art. 66 i art. 69** |

Nie dotyczy.

|  |  |  |
| --- | --- | --- |
| **ROZDZIAŁ 12** | **Wskazanie osób uprawnionych do komunikowania się z Wykonawcami** |  |
|  |
| Sekcja Zamówień PublicznychAnna PARASIŃSKA, Beata ŁASZCZEWSKA-ADAMCZAK, Rafał FUDALA. |

|  |  |
| --- | --- |
| **ROZDZIAŁ 13** | **Termin związania ofertą** |

Wykonawca jest związany złożoną ofertą od dnia upływu terminu składania ofert do dnia **17.08.2021r.**

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 60 dni.

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

|  |  |
| --- | --- |
| **ROZDZIAŁ 14** | **Opis sposobu przygotowania oferty** |

1. Oferta, wniosek oraz przedmiotowe środki dowodowe (jeżeli były wymagane) składane elektronicznie muszą zostać podpisane elektronicznym kwalifikowanym podpisem w przypadku zamówień o wartości równej lub przekraczającej progi unijne. W procesie składania oferty, wniosku w tym przedmiotowych środków dowodowych na platformie, kwalifikowany podpis elektroniczny Wykonawca może złożyć bezpośrednio na dokumencie, który następnie przesyła do systemu[[1]](#footnote-1) przez[**platformazakupowa.pl**](https://platformazakupowa.pl/strona/1-regulamin) oraz dodatkowo dla całego pakietu dokumentów w kroku 2 **Formularza składania oferty lub wniosku** (po kliknięciu w przycisk **Przejdź do podsumowania**).
2. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio Wykonawca, podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, Wykonawcy wspólnie ubiegający się
o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą. Poprzez oryginał należy rozumieć dokument podpisany kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną/upoważnione. Poświadczenie za zgodność z oryginałem następuje w formie elektronicznej podpisane kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną/upoważnione.
3. Oferta musi być:
	1. sporządzona na podstawie załączników niniejszej SWZ w języku polskim,
	2. złożona przy użyciu środków komunikacji elektronicznej tzn. za pośrednictwem [platformazakupowa.pl](https://platformazakupowa.pl/),
	3. podpisana kwalifikowanym podpisem elektronicznym przez osobę/osoby upoważnioną /upoważnione.
4. Podpisy kwalifikowane wykorzystywane przez wykonawców do podpisywania wszelkich plików muszą spełniać “Rozporządzenie Parlamentu Europejskiego i Rady w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (eIDAS) (UE) nr 910/2014 - od 1 lipca 2016 roku”.
5. W przypadku wykorzystania formatu podpisu XAdES zewnętrzny Zamawiający wymaga dołączenia odpowiedniej ilości plików, czyli podpisywanych plików z danymi oraz plików XAdES.
6. Zgodnie z art. 18 ust. 3 ustawy Prawo zamówień publicznych, nie ujawnia się informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, wraz z przekazaniem takich informacji, zastrzegł, że nie mogą być one udostępniane oraz wykazał, że zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy Prawo zamówień publicznych. Na platformie w formularzu składania oferty znajduje się miejsce wyznaczone do dołączenia części oferty stanowiącej tajemnicę przedsiębiorstwa.
7. Wykonawca, za pośrednictwem [platformazakupowa.pl](https://platformazakupowa.pl/) może przed upływem terminu do składania ofert zmienić lub wycofać ofertę. Sposób dokonywania zmiany lub wycofania oferty zamieszczono w instrukcji zamieszczonej na stronie internetowej pod adresem:

<https://platformazakupowa.pl/strona/45-instrukcje>

1. Każdy z wykonawców może złożyć tylko jedną ofertę. Złożenie większej liczby ofert lub oferty zawierającej propozycje wariantowe spowoduje, że podlegać będzie odrzuceniu.
2. Ceny oferty muszą zawierać wszystkie koszty, jakie musi ponieść Wykonawca, aby zrealizować zamówienie z najwyższą starannością oraz ewentualne rabaty.
3. Dokumenty i oświadczenia składane przez Wykonawcę muszą być w języku polskim, chyba że
w SWZ dopuszczono inaczej. W przypadku załączenia dokumentów sporządzonych w innym języku niż dopuszczony, Wykonawca zobowiązany jest załączyć tłumaczenie na język polski.
4. Opatrzenie pliku zawierającego skompresowane dane kwalifikowanym podpisem elektronicznym jest jednoznaczne z podpisaniem oryginału dokumentu, z wyjątkiem kopii poświadczonych odpowiednio przez innego Wykonawcę ubiegającego się wspólnie z nim o udzielenie zamówienia, przez podmiot, na którego zdolnościach lub sytuacji polega Wykonawca, albo przez Podwykonawcę.
5. 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.
6. 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”.
7. Zalecenia:
8. *Zamawiający rekomenduje wykorzystanie formatów: .pdf .doc .xls .jpg (.jpeg) ze szczególnym wskazaniem na .pdf*
9. *W celu ewentualnej kompresji danych Zamawiający rekomenduje wykorzystanie jednego
z formatów:*
	* *.zip*
	* *.7Z*
10. *Wśród formatów powszechnych a NIE występujących w rozporządzeniu występują: .rar .gif .bmp .numbers .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.*
11. *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.*
12. *Pliki w innych formatach niż PDF zaleca się opatrzyć zewnętrznym podpisem XAdES. Wykonawca powinien pamiętać, aby plik z podpisem przekazywać łącznie z dokumentem podpisywanym.*
13. *Zamawiający zaleca aby w przypadku podpisywania pliku przez kilka osób, stosować podpisy tego samego rodzaju..*
14. *Zamawiający zaleca, aby Wykonawca z odpowiednim wyprzedzeniem przetestował możliwość prawidłowego wykorzystania wybranej metody podpisania plików oferty.*
15. *Komunikacja z Wykonawcami odbywała się tylko na Platformie za pośrednictwem formularza “Wyślij wiadomość do Zamawiającego”, nie za pośrednictwem adresu email.*
16. *Osobą składającą ofertę powinna być osoba kontaktowa podawana w dokumentacji.*
17. *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 kilka godzin przed terminem składania ofert/wniosków.*
18. *Podczas podpisywania plików zaleca się stosowanie algorytmu skrótu SHA2 zamiast SHA1.*
19. *Jeśli Wykonawca pakuje dokumenty np. w plik ZIP zalecamy wcześniejsze podpisanie każdego ze skompresowanych plików.*
20. *Zamawiający rekomenduje wykorzystanie podpisu z kwalifikowanym znacznikiem czasu.*
21. *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.*
22. Dokumenty stanowiące ofertę, które należy złożyć:
23. **Formularz ofertowy**- sporządzony według wzoru **(załącznik 1) - (dotyczy części I i II)**
24. **Wypełnioną tabelę (załącznik 1a) - (dotyczy części II)**
25. **Pełnomocnictwo** upoważniające do złożenia oferty, o ile ofertę składa pełnomocnik -**(dotyczy części I i II)** ;
26. **Pełnomocnictwo dla pełnomocnika** do reprezentowania w postępowaniu Wykonawców wspólnie ubiegających się o udzielenie zamówienia - dotyczy ofert składanych przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia **(dotyczy części I i II)** ;
27. **Oświadczenie podmiotu** udostępniającego zasoby, potwierdzające brak podstaw wykluczenia tego podmiotu oraz odpowiednio spełnianie warunków udziału w postępowaniu, w zakresie, w jakim wykonawca powołuje się na jego zasoby - sporządzony według wzoru **(załącznik nr 14) - (dotyczy części I).**
28. **Oświadczenie RODO** - sporządzone według wzoru **(załącznik nr 15) - (dotyczy części I i II)** .
29. Dokumenty i oświadczenia, które Wykonawca będzie zobowiązany złożyć na wezwanie Zamawiającego, którego oferta została najwyżej oceniona. Zamawiający wezwie wykonawcę, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni od dnia wezwania, aktualnych na dzień złożenia oświadczenia o braku podstaw do wykluczenia i następujących podmiotowych środków dowodowych:
30. **JEDZ - (dotyczy części I i II)**
31. **Odpis z Krajowego Rejestru Sądowego** lub informacja z Centralnej Ewidencji i Informacji o Działalności Gospodarczej, w zakresie art. 109 ust. 1 pkt 4 ustawy Pzp, sporządzonych nie wcześniej niż 3 miesiące przed jej złożeniem. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast ww. dokumentów składa dokument lub dokumenty wystawione w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, potwierdzające odpowiednio, że nie otwarto jego likwidacji, nie ogłoszono upadłości, jego aktywami nie zarządza likwidator lub sąd, nie zawarł układu z wierzycielami, jego działalność gospodarcza nie jest zawieszona ani nie znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury - **(dotyczy części I i II)**.
32. **Oświadczenie o przynależności** bądź braku przynależności do grupy kapitałowej **(załącznik nr 4) - (dotyczy części I i II).**
33. **Wykaz dostaw i usług** wraz z referencjami **(załącznik nr 5) - (dotyczy części I)**
34. **Wykaz osób (załącznik nr 6) - (dotyczy części I)**
35. **Oświadczenie o dysponowaniu osobami (załączniki nr 7-11) - (dotyczy części I)**
36. **Oświadczenie** o dysponowaniu punktem serwisowym **(załącznik nr 12) - (dotyczy części I)**.
37. **Oświadczenie** o dysponowaniu portalem/systemem serwisowym **(załącznik nr 13) - (dotyczy części I).**
38. Oferta, JEDZ w postępowaniu muszą być złożone w oryginale.
39. Zamawiający zaleca ponumerowanie stron oferty.
40. Pełnomocnictwo do złożenia oferty musi być złożone w oryginale w takiej samej formie, jak składana oferta (t.j. w formie elektronicznej lub postaci elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym). Dopuszcza się także złożenie elektronicznej kopii (skanu) pełnomocnictwa sporządzonego uprzednio w formie pisemnej, w formie elektronicznego poświadczenia sporządzonego stosownie do art. 97 § 2 ustawy z dnia 14 lutego 1991 r. - Prawo o notariacie, które to poświadczenie notariusz opatruje kwalifikowanym podpisem elektronicznym, bądź też poprzez opatrzenie skanu pełnomocnictwa sporządzonego uprzednio w formie pisemnej kwalifikowanym podpisem, podpisem zaufanym lub podpisem osobistym mocodawcy. Elektroniczna kopia pełnomocnictwa nie może być uwierzytelniona przez upełnomocnionego.
41. Oferty składane wspólnie (konsorcjum, spółka cywilna itp.)
42. Wykonawcy mogą wspólnie ubiegać się o udzielenie zamówienia.
43. Wykonawcy składający ofertę wspólną ustanawiają pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania w postępowaniu i zawarcia umowy.
44. Do oferty wspólnej Wykonawcy dołączają pełnomocnictwo.
45. Pełnomocnik pozostaje w kontakcie z Zamawiającym w toku postępowania i do niego Zamawiający kieruje informacje, korespondencję, itp.
46. Oferta wspólna, składana przez dwóch lub więcej Wykonawców, powinna spełniać następujące wymagania:
47. oferta wspólna powinna być sporządzona zgodnie z SWZ;
48. sposób składania dokumentów w ofercie wspólnej:
* dokumenty, dotyczące własnej firmy, takie jak np.: JEDZ składa każdy z Wykonawców składających ofertę wspólną we własnym imieniu;
* dokumenty wspólne takie jak np.: formularz ofertowy, formularz cenowy, dokumenty podmiotowe i przedmiotowe składa pełnomocnik Wykonawców w imieniu wszystkich Wykonawców składających ofertę wspólną;
1. kopie dokumentów dotyczących każdego z Wykonawców składających ofertę wspólną muszą być poświadczone za zgodność z oryginałem przez osobę lub osoby upoważnione do reprezentowania tych Wykonawców.
2. Przed podpisaniem umowy (w przypadku wygrania postępowania) Wykonawcy składający ofertę wspólną będą mieli obowiązek przedstawić Zamawiającemu umowę konsorcjum, zawierającą, co najmniej:
3. zobowiązanie do realizacji wspólnego przedsięwzięcia gospodarczego obejmującego swoim zakresem realizację przedmiotu zamówienia,
4. określenie zakresu działania poszczególnych stron umowy,
5. czas obowiązywania umowy, który nie może być krótszy, niż okres obejmujący realizację zamówienia oraz czas trwania gwarancji jakości i rękojmi.

|  |  |
| --- | --- |
| **ROZDZIAŁ 15** | **Sposób oraz termin składania ofert** |

1. Ofertę wraz z wymaganymi dokumentami należy umieścić na [platformazakupowa.pl](http://platformazakupowa.pl/) pod adresem: **https://platformazakupowa.pl/** w myśl Ustawy na stronie internetowej prowadzonego postępowania do dnia **19.05.2021r. o godz. 09:00**
2. Do oferty należy dołączyć wszystkie wymagane w SWZ dokumenty.
3. Po wypełnieniu Formularza składania oferty lub wniosku i dołączenia wszystkich wymaganych załączników należy kliknąć przycisk „Przejdź do podsumowania”.
4. Oferta lub wniosek składana elektronicznie musi zostać podpisana elektronicznym podpisem kwalifikowanym. W procesie składania oferty za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl/), Wykonawca powinien złożyć podpis bezpośrednio na dokumentach przesłanych za pośrednictwem [platformazakupowa.pl](http://platformazakupowa.pl/). Zalecamy stosowanie podpisu na każdym załączonym pliku osobno, w szczególności wskazanych w art. 63 ust. 1 oraz ust. 2 ustawy Prawo zamówień publicznych, gdzie zaznaczono, iż oferty, wnioski o dopuszczenie do udziału w postępowaniu oraz oświadczenie, o którym mowa w art. 125 ust. 1 tej ustawy sporządza się, pod rygorem nieważności, w postaci lub formie elektronicznej i opatruje się odpowiednio w odniesieniu do wartości postępowania kwalifikowanym podpisem elektronicznym.
5. Za datę złożenia oferty przyjmuje się datę jej przekazania w systemie (platformie) w drugim kroku składania oferty poprzez kliknięcie przycisku “Złóż ofertę” i wyświetlenie się komunikatu, że oferta została zaszyfrowana i złożona.
6. Szczegółowa instrukcja dla Wykonawców dotycząca złożenia, zmiany i wycofania oferty znajduje się na stronie internetowej pod adresem: <https://platformazakupowa.pl/strona/45-instrukcje>
7. Wykonawca po upływie terminu do składania ofert nie może wycofać złożonej oferty.

|  |  |
| --- | --- |
| **ROZDZIAŁ 16** | **Termin otwarcia ofert** |

* + 1. Otwarcie ofert nastąpi niezwłocznie po upływie terminu składania ofert, tj. **19.05.2021r. o godz. 09:15**
		2. Jeżeli otwarcie ofert następuje przy użyciu systemu teleinformatycznego, w przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert następuje niezwłocznie po usunięciu awarii.
		3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
		4. Zamawiający, najpóźniej przed otwarciem ofert, udostępnia na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
		5. **Otwarcie ofert jest niejawne.**
		6. 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.

1. Informacja zostanie opublikowana na stronie postępowania na platformazakupowa.pl w sekcji ,,Komunikaty” .
2. W przypadku ofert, które podlegają negocjacjom, Zamawiający udostępnia informacje, o których mowa w ust. 6 pkt 2, niezwłocznie po otwarciu ofert ostatecznych albo unieważnieniu postępowania.
3. Zgodnie z Ustawą Prawo Zamówień Publicznych Zamawiający nie ma obowiązku przeprowadzania jawnej sesji z otwarcia ofert, z udziałem wykonawców lub transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line a ma jedynie takie uprawnienie.

|  |  |
| --- | --- |
| **ROZDZIAŁ 17** | **Sposób obliczenia ceny** |

Cena oferty musi uwzględniać wszystkie zobowiązania wynikające z umowy, tj. wszystkie koszty i składniki związane z wykonaniem zamówienia oraz warunkami SWZ i uwzględniać cały zakres przedmiotu zamówienia (w tym podatki i narzuty). Cena oferty uwzględnia wszystkie zobowiązania, musi być podana w PLN cyfrowo i słownie, z wyodrębnieniem należnego podatku VAT - jeżeli występuje.

Cenę należy określić z dokładnością do dwóch miejsc po przecinku. Kwoty wykazane w ofercie zaokrągla się do pełnych groszy, przy czym końcówki poniżej 0,5 grosza pomija się, a końcówki 0,5 grosza i wyższe zaokrągla się do 1 grosza.

Cena ustalona przez Wykonawcę zostanie ustalona na okres ważności umowy i nie będzie podlegała zmianom.

Cenę za wykonanie przedmiotu zamówienia należy wpisać do „Formularza ofertowego” stanowiącego załącznik do niniejszej specyfikacji warunków zamówienia.

Wynagrodzenie za przedmiot umowy jest wynagrodzeniem ryczałtowym.

|  |  |
| --- | --- |
| **ROZDZIAŁ 18** | **Opis kryteriów oceny ofert, wraz z podaniem wag tych kryteriów, i sposobu oceny** |

Przy wyborze oferty Zamawiający będzie się kierował **następującymi kryteriami:**

**Część I**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Kryterium** | **Znaczenie kryterium (%)** | **Liczba możliwych do uzyskania punktów** |
| 1. | Cena oferty  | **90** | do 90 punktów |
| 2. | Polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę (oprócz Wykonawcy)  | **10** | do 10 punktów |

Cena – **90%**

sposób przyznania punktów

**Cn / Cb x 100 x 90% = ilość punktów**

gdzie:

Cn – najniższa cena spośród ofert nie odrzuconych

Cb – cena oferty badanej (rozpatrywanej)

100 – wskaźnik stały

90% – procentowe znaczenie kryterium „ceny”

Polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę (oprócz Wykonawcy) – **10%**

sposób przyznania punktów:

Polskojęzyczne wsparcie – 10 pkt

Brak polskojęzycznego wsparcia – 0 pkt

**Część II**

|  |  |  |  |
| --- | --- | --- | --- |
| **Lp.** | **Kryterium** | **Znaczenie kryterium (%)** | **Liczba możliwych do uzyskania punktów** |
| 1. | Cena oferty  | **95** | do 95 punktów |
| 2. | Gwarancja na serwer dłuższa niż 36 miesięcy  | **5** | do 5 punktów |

 Cena – **95%**

sposób przyznania punktów

**Cn / Cb x 100 x 95% = ilość punktów**

gdzie:

Cn – najniższa cena spośród ofert nie odrzuconych

Cb – cena oferty badanej (rozpatrywanej)

100 – wskaźnik stały

95% – procentowe znaczenie kryterium „ceny”

Gwarancja - **5%**

Gwarancja do 36 miesięcy -0 pkt

Gwarancja powyżej 36 miesięcy -5pkt

**Maksymalny okres gwarancji 60 miesięcy**

Zamawiający oceni oferty sumując punkty uzyskane z poszczególnych kryteriów.

Ocenie będą podlegać wyłącznie oferty nie podlegające odrzuceniu.

Za najkorzystniejszą zostanie uznana oferta z najwyższą liczbą punktów.

W sytuacji, gdy Zamawiający nie będzie mógł dokonać wyboru najkorzystniejszej oferty ze względu na to, że zostały złożone oferty o takiej samej ilości punktów, wezwie on Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez Zamawiającego ofert dodatkowych zawierających nową cenę. Wykonawcy, składając oferty dodatkowe, nie mogą zaoferować cen wyższych niż zaoferowane w uprzednio złożonych przez nich ofertach.

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.

Zamawiający wybiera najkorzystniejszą ofertę w terminie związania z ofertą określonym w SWZ.

1. Jeżeli termin związania ofertą upłynie przed wyborem najkorzystniejszej oferty, Zamawiający wezwie Wykonawcę̨, którego oferta otrzymała najwyższą ocenę̨, do wyrażenia, w wyznaczonym przez Zamawiającego terminie, pisemnej zgody na wybór jego oferty.
2. W przypadku braku zgody, o której mowa w ust. 7, oferta podlega odrzuceniu, a Zamawiający zwraca się o wyrażenie takiej zgody do kolejnego Wykonawcy, którego oferta została najwyżej oceniona, chyba że zachodzą̨ przesłanki do unieważnienia postępowania.

|  |  |
| --- | --- |
| **ROZDZIAŁ 19** | **Informacje o formalnościach, jakie muszą zostać dopełnione po wyborze oferty w celu zawarcia umowy w sprawie zamówienia publicznego** |

1. Zamawiający zawiera umowę̨ w sprawie zamówienia publicznego, z uwzględnieniem art. 577 ustawy Prawo zamówień publicznych, w terminie nie krótszym niż 10 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty, jeżeli zawiadomienie to zostało przesłane przy użyciu środków komunikacji elektronicznej, albo 15 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 ofertę̨.
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 do SWZ. Umowa zostanie uzupełniona o zapisy wynikające ze złożonej oferty.
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 postepowanie.

|  |  |
| --- | --- |
| **ROZDZIAŁ 20** | **Projektowane postanowienia umowy w sprawie zamówienia publicznego, które zostaną wprowadzone do treści tej umowy** |

1. Zamawiający wymaga, aby wybrany Wykonawca zawarł z nim umowę na warunkach określonych w projekcie umowy stanowiącym **załącznik nr 3** do SWZ.
2. Zamawiający zastrzega sobie, iż ostateczna treść umowy w stosunku do projektu umowy może ulec zmianie, jednakże wyłącznie w przypadku, gdy zmiana ta nie jest istotna w rozumieniu art. 454 ustawy Prawo Zamówień Publicznych i w zakresie przewidzianym w treści projektu umowy, zgodnie z art. 455 ust. 1 ustawy Prawo Zamówień Publicznych..
3. Zamawiający, zgodnie z art. 455 ust. 1 ustawy Prawo Zamówień Publicznych, przewiduje możliwość dokonania zmian postanowień zawartej umowy w sprawie zamówienia publicznego,
w sposób i na warunkach określonych w projekcie umowy.

|  |  |
| --- | --- |
| **ROZDZIAŁ 21** | **Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy** |

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówieniá oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów pzp.

2. Odwołanie przysługuje na:

2.1. niezgodna z przepisami ustawy czynność Zamawiającego, podjętą w postepowanių o udzielenie zamówienia, w tym na projektowane postanowienie umowy;

2.2. zaniechanie czynnoścí w postepowanių o udzielenie zamówienia, do której Zamawiający był obowiązany̨ na podstawie ustawy;

2.3. zaniechanie przeprowadzenia postępowania o udzielenie zamówienia lub zorganizowania konkursu na podstawie ustawy, mimo że zamawiający był do tego obowiązany.

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 któryḿ mowa w art. 519 ust. 1 pzp, stronom oraz uczestnikom postepowanią odwoławczego przysługuje skarga do sadu.̨ Skargę̨ wnosi się do Sadų Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.

5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX ustawy Prawo zamówień publicznych - „Środki ochrony prawnej”.

|  |  |
| --- | --- |
| **ROZDZIAŁ 22** | **Podstawy wykluczenia, o których mowa w art. 109 ust. 1, jeżeli Zamawiający je przewiduje** |

Zamawiający **przewiduje** podstawy wykluczenia, o których mowa w art. 109 ust. 1 ustawy Prawo zamówień publicznych.

Stosownie do treści art. 109 ust. 2 ustawy PZP, Zamawiający wykluczy z postępowania 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 ustawy PZP, chyba że wykonawca 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;
3. który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów;
4. który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej umowy w sprawie zamówienia publicznego lub umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady;
5. który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego
w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału
w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych;
6. który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia;
7. który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu
o udzielenie zamówienia.

W przypadkach, o których mowa w ust. 2 pkt 1–4, zamawiający może nie wykluczać wykonawcy, jeżeli wykluczenie byłoby w sposób oczywisty nieproporcjonalne, w szczególności gdy kwota zaległych podatków lub składek na ubezpieczenie społeczne jest niewielka albo sytuacja ekonomiczna lub finansowa wykonawcy, o którym mowa w ust. 2 pkt 2, jest wystarczająca do wykonania zamówienia.

|  |  |
| --- | --- |
| **ROZDZIAŁ 23** | **Opis części zamówienia, jeżeli Zamawiający dopuszcza składanie ofert częściowych** |

Zamawiający **dopuszcza** możliwość składania ofert częściowych.

|  |  |
| --- | --- |
| **ROZDZIAŁ 24** | **Liczba części zamówienia, na którą Wykonawca może złożyć ofertę, lub maksymalna liczbę części, na które zamówienie może zostać udzielone temu samemu Wykonawcy, oraz kryteria lub zasady, mające zastosowanie do ustalenia, które części zamówienia zostaną udzielone jednemu Wykonawcy, w przypadku wyboru jego oferty w większej niż maksymalna liczbie części** |

Wykonawca może złożyć ofertę na **dwie części** postępowania.

|  |  |
| --- | --- |
| **ROZDZIAŁ 25** | **Wymagania dotyczące wadium, w tym jego kwotę, jeżeli Zamawiający przewiduje obowiązek wniesienia wadium** |

Zamawiający **nie** **przewiduje** konieczności złożenia wadium.

|  |  |
| --- | --- |
| **ROZDZIAŁ 26** | **Informacje dotyczące zabezpieczenia należytego wykonania umowy, jeżeli Zamawiający je przewiduje** |

Zamawiający **nie wymaga** wniesienie zabezpieczenia należytego wykonania umowy.

|  |  |
| --- | --- |
| **ROZDZIAŁ 27** | **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** |

Zamawiający **nie dopuszcza** możliwości składania ofert wariantowych.

|  |  |
| --- | --- |
| **ROZDZIAŁ 28** | **Liczba Wykonawców, z którymi zamawiający zawrze umowę ramową, jeżeli zamawiający przewiduje zawarcie umowy ramowej.** |

Nie dotyczy

|  |  |
| --- | --- |
| **ROZDZIAŁ 29** | **Informacja o przewidywanych zamówieniach, o których mowa w art. 214 ust. 1 pkt 7 i 8, jeżeli zamawiający przewiduje udzielenie takich zamówień** |

Zamawiający **nie przewiduje** możliwości udzielenia zamówień z wolnej ręki o których mowa w art. 214 ust. 1 pkt 7 i 8 ustawy Prawo zamówień publicznych.

|  |  |
| --- | --- |
| **ROZDZIAŁ 30** | **Informacje dotyczące przeprowadzenia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia, o których mowa w art. 131 ust. 2 ustawy Prawo zamówień publicznych, jeżeli Zamawiający przewiduje możliwość albo wymaga złożenia oferty po odbyciu wizji lokalnej lub sprawdzeniu tych dokumentów** |

Zamawiający **nie wymaga** odbycia przez Wykonawcę wizji lokalnej lub sprawdzenia przez niego dokumentów niezbędnych do realizacji zamówienia.

|  |  |
| --- | --- |
| **ROZDZIAŁ 31** | **Informacje dotyczące walut obcych, w jakich mogą być prowadzone rozliczenia między Zamawiającym a wykonawcą, jeżeli Zamawiający przewiduje rozliczenia w walutach obcych** |

1. Zamawiający **nie przewiduje** możliwości prowadzenia rozliczeń w walutach obcych.
2. Rozliczenia między Zamawiającym a Wykonawcą będą prowadzone w złotych polskich (PLN).
3. Zamawiający nie przewiduje możliwości udzielenia zaliczek na poczet wykonania zamówienia.

|  |  |
| --- | --- |
| **ROZDZIAŁ 32** | **Informacje o uprzedniej ocenie ofert, zgodnie z art. 139, jeżeli zamawiający przewiduje odwróconą kolejność oceny.** |

Zamawiający **przewiduje** odwróconą kolejność oceny.

|  |  |
| --- | --- |
| **ROZDZIAŁ 33** | **Informacja o przewidywanym wyborze najkorzystniejszej oferty z zastosowaniem aukcji elektronicznej wraz z informacjami, o których mowa w art. 230 ustawy Prawo zamówień publicznych, jeżeli Zamawiający przewiduje aukcję elektroniczną** |

Zamawiający **nie przewiduje** aukcji elektronicznej.

|  |  |
| --- | --- |
| **ROZDZIAŁ 34** | **Informacje dotyczące zwrotu kosztów udziału w postępowaniu, jeżeli Zamawiający przewiduje ich zwrot** |

Zamawiający **nie przewiduje** zwrotu kosztów udziału w postępowaniu, z zastrzeżeniem art. 261.

|  |  |
| --- | --- |
| **ROZDZIAŁ 35** | **Informacje o zastrzeżeniu możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94, jeżeli Zamawiający przewiduje takie wymagania** |

Zamawiający **nie zastrzega** możliwości ubiegania się o udzielenie zamówienia wyłącznie wykonawców, o których mowa w art. 94 ustawy Prawo zamówień publicznych.

|  |  |
| --- | --- |
| **ROZDZIAŁ 36** | **Wymagania w zakresie zatrudnienia osób, o których mowa w art. 96 ust. 2 pkt 2, jeżeli Zamawiający przewiduje takie wymagania** |

Nie dotyczy.

|  |  |
| --- | --- |
| **ROZDZIAŁ 37** | **Informacje o zastrzeżeniu możliwości ubiegania się o udzielenie zamówienia wyłącznie przez wykonawców, o których mowa w art. 94, jeżeli Zamawiający przewiduje takie wymagania** |

Zamawiający **nie zastrzega** możliwości ubiegania się o udzielenie zamówienia wyłącznie wykonawców, o których mowa w art. 94 ustawy Prawo zamówień publicznych.

|  |  |
| --- | --- |
| **ROZDZIAŁ 38** | **Informację o obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań, jeżeli Zamawiający dokonuje takiego zastrzeżenia zgodnie z art. 60 i art. 121 ustawy Prawo zamówień publicznych** |

Zamawiający **nie zastrzega** obowiązku osobistego wykonania przez Wykonawcę kluczowych zadań.

|  |  |
| --- | --- |
| **ROZDZIAŁ 39** | **Wymóg lub możliwość złożenia ofert w postaci katalogów elektronicznych lub dołączenia katalogów elektronicznych do oferty, w sytuacji określonej w art. 93ustawy Prawo zamówień publicznych** |

Zamawiający **nie wymaga** złożenia oferty w postaci katalogu elektronicznego.

|  |  |
| --- | --- |
| **ROZDZIAŁ 40** | **Klauzula informacyjna z art. 13 RODO do zastosowania przez Zamawiających w celu związanym z postępowaniem o udzielenie zamówienia publicznego** |

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:

* administratorem Pani/Pana danych osobowych jest */****Akademia Marynarki Wojennej im. Bohaterów Westerplatte, ul. Inż. J. Śmidowicza 69, 81-127 Gdynia****/;*
* inspektorem ochrony danych osobowych w */nazwa zamawiającego/* jest Pan/~~Pani~~ */* ***mgr inż. Janusz Gawrych, kontakt: iod@amw.gdynia.pl, 261-262-644/ \*;***
* Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. cRODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego **11/*ZP/21*** prowadzonym
w trybie **przetargu nieograniczonego**
* 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 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r. poz. 1579 i 2018), dalej „ustawa Pzp”;
* Pani/Pana dane osobowe będą przechowywane, zgodnie z art. 97 ust. 1 ustawy Pzp, przez okres 4 lat od dnia zakończenia postępowania o udzielenie zamówienia, a jeżeli czas trwania umowy przekracza 4 lata, okres przechowywania obejmuje cały czas trwania umowy;
* 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;
* w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
* 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;
* 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**.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*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).*

***\* 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.*

|  |  |
| --- | --- |
| **ROZDZIAŁ 41** | **Załączniki** |

**Załącznik nr 1** Formularz ofertowy

**Załącznik nr 1a** Tabela

**Załącznik nr 2** Opis przedmiotu zamówienia

**Załącznik nr 3** Projekt umowy

**Załącznik nr 4** Oświadczenie o grupie kapitałowej

**Załącznik nr 5** Wykaz dostaw i usług

**Załącznik nr 6** Wykaz osób

**Załącznik nr 7-11** Oświadczenia o dysponowaniu osobami

**Załącznik nr 12** Oświadczenia o dysponowaniu punktem serwisowym

**Załącznik nr 13** Oświadczenia o dysponowaniu panelem serwisowym

**Załącznik nr 14** Oświadczenie o poleganiu na innych podmiotach

**Załącznik nr 15** Oświadczenie RODO

Gdynia, …...04.2021 r. Podpisy osób uprawnionych

**WNIOSKUJĄCY**

(odpowiedzialny za opis przedmiotu zamówienia, zawarcie i realizację umowy)**:**

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Marcin **SZULC**

**UZGODNIONO Z:**

(Sekcją Zamówień Publicznych w zakresie procedur Prawa zamówień publicznych)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Anna **PARASIŃSKA**

**UZGODNIONO Z:**

(Kanclerz AMW)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Marek **DRYGAS**

***ZAŁĄCZNIK NR 1***

 *wypełniony formularz winien być pierwszą stroną oferty*

**FORMULARZ OFERTOWY WYKONAWCY**

*DANE DOTYCZĄCE WYKONAWCY*Nazwa Wykonawcy (firmy)

................................................................................................................................................

Adres Siedziby Wykonawcy (firmy)

……………………................................................................................................................

Adres do korespondencji

………………………………………………………………………………………………

Nr telefonu/**e-mail** ………............../......................................./........................................NIP ....................................................................................................................REGON ..…...............................................................................................................

 **oświadczam, że jestem** (*należy wybrać z listy*)

* mikroprzedsiębiorstwem,
* małym przedsiębiorstwem,
* średnim przedsiębiorstwem,
* jednoosobową działalność gospodarcza,
* osoba fizyczna nieprowadząca działalności gospodarczej,
* inny rodzaj.

Jednostki centralne komputerów, serwery, zestawy komputerów stacjonarnych, drukarki oraz urządzenia do transmisji danych cyfrowych (w tym koncentratory, switche sieciowe, routery i modemy) objęte są „0” stawką VAT zgodnie z art. 83 ust. 1 pkt 26 Ustawy. Zamawiający będzie się ubiegał o formalną zgodę organu założycielskiego na **zakup serwera** **z 0 stawką podatku VAT** po wyborze najkorzystniejszej oferty. Spowodowane jest to wpisaniem wykonawcy w dokumencie potwierdzającym **zastosowanie 0 stawki podatku VAT.**

Niniejszym składamy ofertę w postepowaniu prowadzonym w trybie przetargu podstawowego na:

**Część I:**

* LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I  ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ
* WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO

**Część II:**

* CERTYFIKAT SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ
* SERWER USŁUG PULPITU ZDALNEGO

**Cena za wykonanie części I:**

cena netto PLN

(słownie: .....................................................................................................................................)

cena brutto PLN

(słownie: .....................................................................................................................................)

W tym:

* **Licencja wraz z roczną subskrypcją na system ochrony antywirusowej i antyspamowej zasobów sieci komputerowej (nazwa oprogramowania):**

…………….netto/……………brutto- zastosowano podatek VAT w wysokości .................%

* **Wsparcie techniczne systemu ochrony antywirusowej i antyspamowej oraz środowiska serwerowego i wirtualnego:**

…………….netto/……………brutto- zastosowano podatek VAT w wysokości .................%

Posiadamy polskojęzyczne wsparcie techniczne świadczone przez producenta albo autoryzowanego dystrybutora na Polskę – **TAK / NIE** ( niepotrzebne skreślić)

**Cena za wykonanie części II:**

cena netto PLN

(słownie: .....................................................................................................................................)

cena bruto PLN

(słownie: .....................................................................................................................................)

W tym:

* **Certyfikat ssl wildcard z roczną subskrypcją:**

…………….netto/……………brutto- zastosowano podatek VAT w wysokości .................%

* **Licencja Microsoft zapewniająca zdalny dostęp do serwerów Windows 50 szt.:**

…………….netto/……………brutto- zastosowano podatek VAT w wysokości .................%

* **Licencja Microsoft – system operacyjny Windows Server Standard 4 szt.:**

…………….netto/……………brutto- zastosowano podatek VAT w wysokości .................%

* **Serwer usług pulpitu zdalnego :**

…………….netto/brutto– (stawka VAT 0%)

Gwarancja na serwer wynosi: …………… lat

Zapewniamy następujące warunki świadczenia usług serwisowych:

|  |  |
| --- | --- |
| Czas reakcji serwisowej: | 1 godzina |
| Miejsce świadczenia usług serwisowych | AMW |
|  |
| Zgłaszanie potrzeb serwisowych – wskazanie minimum 2 kontaktów |
| Nazwiska osób "kontaktowych" | ……………………………………………………………………. |
| Maile | ……………………………………………………………………. |
| Telefony | ……………………………………………………………………. |
| Faksy | ……………………………………………………………………. |
| Inny sposób zgłaszania potrzeby serwisu – podać procedurę | …………………………………………………………………….……………………………………………………………………. |

1. oświadczamy, że wybór oferty:
* nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.
* będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie
z przepisami o podatku od towarów i usług. Powyższy obowiązek podatkowy będzie dotyczył ……………………………………… (*Wpisać nazwę /rodzaj towaru lub usługi, które będą prowadziły do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług)*objętych przedmiotem zamówienia.
1. oświadczamy, że oferujemy przedmiot zamówienia zgodny z wymaganiami i warunkami określonymi przez Zamawiającego w SWZ i potwierdzamy przyjęcie warunków umownych i warunków płatności zawartych w SWZ i we wzorze umowy stanowiącym załącznik do SWZ,
2. oferta liczy **........................** kolejno ponumerowanych kart,

***Uwaga! Wykonawca zobowiązany jest do wypełnienia miejsc wykropkowanych.***

***ZAŁĄCZNIK NR 1a***

**Dotyczy części II**

**Serwer usług pulpitu zdalnego o parametrach podanych poniżej**

|  |  |
| --- | --- |
| **Nazwa producenta i oznaczenie produktu oferowanego** |   |

|  |  |  |
| --- | --- | --- |
| **Parametr** | **Charakterystyka (wymagania minimalne)** | **Parametr oferowany** |
| **Obudowa** | Obudowa Rack o wysokości max 1U z możliwością instalacji do 4 dysków 3.5" wraz z kompletem wysuwanych szyn umożliwiających montaż w szafie rack i wysuwanie serwera do celów serwisowych oraz organizatorem do kabli. Obudowa wyposażona w kartę umożliwiającą dostęp bezpośredni poprzez urządzenia mobilne - serwer musi posiadać możliwość konfiguracji oraz monitoringu najważniejszych komponentów serwera przy użyciu dedykowanej aplikacji mobilnej min. (Android/ Apple iOS) przy użyciu jednego z protokołów NFC/ BLE/ WIFI. |  |
| **Płyta główna** | Płyta główna z możliwością zainstalowania minimum dwóch procesorów. Płyta główna musi być zaprojektowana przez producenta serwera i oznaczona jego znakiem firmowym. |  |
| **Chipset** | Dedykowany przez producenta procesora do pracy w serwerach dwuprocesorowych |  |
| **Procesor** | Zainstalowany jeden procesor ośmiordzeniowy, min. 2.1GHz, klasy x86 dedykowany do pracy z zaoferowanym serwerem umożliwiający osiągnięcie wyniku min. 65,1 w teście SPECint\_rate\_base2017 dostępnym na stronie www.spec.org  |  |
| **RAM** | 64GB DDR4 RDIMM 2667MT/s, na płycie głównej powinno znajdować się minimum 16 slotów przeznaczonych do instalacji pamięci. Płyta główna powinna obsługiwać do 512GB pamięci RAM. |  |
| **Zabezpieczenia pamięci RAM** | Memory Rank Sparing, Memory Mirror, Failed DIMM isolation, Memory Address Parity Protection, Memory Thermal Throttling |  |
| **Gniazda PCI** | Min. jeden slot PCIe Gen 3 o prędkości min. x16 pełnej wysokości. |  |
| **Interfejsy sieciowe** | Wbudowane minimum 2 porty typu Gigabit Ethernet Base-T. |  |
| **Napęd optyczny** | Wbudowany DVD +/- RW SATA |  |
| **Dyski twarde** | Możliwość instalacji dysków SATA, SAS, SSD.Zainstalowane 2 dyski min. 960GB SSD vSAS 12Gb/s 512e 2,5"Możliwość zainstalowania wewnętrznego modułu dedykowanego dla hypervisora wirtualizacyjnego, wyposażonego w 2 jednakowe nośniki typu flash o pojemności minimum 32GB z możliwością konfiguracji zabezpieczenia RAID 1 z poziomu BIOS serwera, rozwiązanie nie może powodować zmniejszenia ilości wnęk na dyski twarde. |  |
| **Kontroler RAID** | Sprzętowy kontroler dyskowy, posiadający min. 2GB nieulotnej pamięci cache, możliwe konfiguracje poziomów RAID: 0, 1, 5, 6, 10, 50, 60. Wsparcie dla dysków samoszyfrujących. |  |
| **Wbudowane porty** | min. 1 port USB 2.0, 1 port micro-USB oraz min. 3 porty USB 3.0, 4 porty RJ45, 2 porty VGA (1 na przednim panelu obudowy, drugi na tylnym), min. 1 port RS232. |  |
| **Video** | Zintegrowana karta graficzna umożliwiająca wyświetlenie rozdzielczości min. 1920x1200 |  |
| **Wentylatory** | Redundantne |  |
| **Zasilacze** | Redundantne, Hot-Plug maksymalnie 550W. |  |
| **Bezpieczeństwo** | Zintegrowany z płytą główną moduł TPM.Wbudowany czujnik otwarcia obudowy współpracujący z BIOS i kartą zarządzającą. |  |
| **System operacyjny** | Brak systemu operacyjnego. |  |
| **Karta Zarządzania** | Niezależna od zainstalowanego na serwerze systemu operacyjnego posiadająca dedykowany port Gigabit Ethernet RJ-45 i umożliwiająca:* zdalny dostęp do graficznego interfejsu Web karty zarządzającej;
* zdalne monitorowanie i informowanie o statusie serwera (m.in. prędkości obrotowej wentylatorów, konfiguracji serwera);
* szyfrowane połączenie (TLS) oraz autentykacje i autoryzację użytkownika;
* możliwość podmontowania zdalnych wirtualnych napędów;
* wirtualną konsolę z dostępem do myszy, klawiatury;
* wsparcie dla IPv6;
* wsparcie dla WSMAN (Web Service for Management); SNMP; IPMI2.0, SSH, Redfish;
* możliwość zdalnego monitorowania w czasie rzeczywistym poboru prądu przez serwer;
* możliwość zdalnego ustawienia limitu poboru prądu przez konkretny serwer;
* integracja z Active Directory;
* możliwość obsługi przez dwóch administratorów jednocześnie;
* wsparcie dla dynamic DNS;
* wysyłanie do administratora maila z powiadomieniem o awarii lub zmianie konfiguracji sprzętowej.
* możliwość bezpośredniego zarządzania poprzez dedykowany port USB na przednim panelu serwera
* możliwość zarządzania do 50 serwerów bezpośrednio z konsoli karty zarządzającej pojedynczego serwera
* karta powinna posiadać możliwość wyposażenia we wbudowaną wewnętrzną pamięć SD lub USB o pojemności 16GB do przechowywania sterowników i firmware'ów komponentów serwera, umożliwiająca szybką instalację wspieranych systemów operacyjnych.

Dodatkowe oprogramowanie umożliwiające zarządzanie poprzez sieć, spełniające minimalne wymagania:* wsparcie dla serwerów, urządzeń sieciowych oraz pamięci masowych;
* możliwość zarządzania dostarczonymi serwerami bez udziału dedykowanego agenta;
* wsparcie dla protokołów – WMI, SNMP, IPMI, WSMan, Linux SSH;
* możliwość oskryptowywania procesu wykrywania urządzeń;
* możliwość uruchamiania procesu wykrywania urządzeń w oparciu o harmonogram;
* szczegółowy opis wykrytych systemów oraz ich komponentów;
* możliwość eksportu raportu do CSV, HTML, XLS;
* grupowanie urządzeń w oparciu o kryteria użytkownika;
* automatyczne skrypty CLI umożliwiające dodawanie i edycję grup urządzeń;
* szybki podgląd stanu środowiska;
* podsumowanie stanu dla każdego urządzenia;
* szczegółowy status urządzenia/elementu/komponentu;
* generowanie alertów przy zmianie stanu urządzenia;
* filtry raportów umożliwiające podgląd najważniejszych zdarzeń;
* integracja z service desk producenta dostarczonej platformy sprzętowej;
* możliwość przejęcia zdalnego pulpitu;
* możliwość podmontowania wirtualnego napędu;
* kreator umożliwiający dostosowanie akcji dla wybranych alertów;
* możliwość importu plików MIB;
* przesyłanie alertów „as-is” do innych konsol firm trzecich;
* aktualizacja oparta o wybranie źródła bibliotek (lokalna, on-line producenta oferowanego rozwiązania);
* możliwość instalacji sterowników i oprogramowania wewnętrznego bez potrzeby instalacji agenta;
* możliwość automatycznego generowania i zgłaszania incydentów awarii bezpośrednio do centrum serwisowego producenta serwerów;
* moduł raportujący pozwalający na wygenerowanie następujących informacji: nr seryjny sprzętu, konfiguracja poszczególnych urządzeń, wersje oprogramowania wewnętrznego, obsadzenie slotów PCIe i gniazd pamięci, informację o maszynach wirtualnych, aktualne informacje o stanie gwarancji, adresy IP kart sieciowych
 |  |
| **Certyfikaty** | Serwer musi być wyprodukowany zgodnie z normą ISO-9001:2008 oraz ISO-14001. Serwer musi posiadać deklaracja CE.Oferowany serwer musi znajdować się na liście Windows Server Catalog i posiadać status „Certified for Windows” dla systemów Microsoft Windows 2012, Microsoft Windows 2012 R2, Windows Server 2016 i nowszych. |  |
| **Warunki gwarancji** | Minimum trzy lata gwarancji realizowanej w miejscu instalacji sprzętu, z czasem reakcji do następnego dnia roboczego od przyjęcia zgłoszenia, możliwość zgłaszania awarii w trybie 365x7x24 poprzez ogólnopolską linię telefoniczną producenta. W przypadku awarii dyski twarde pozostają własnością zamawiającego.Możliwość rozszerzenia gwarancji przez producenta do siedmiu lat. |  |
| **Dokumentacja użytkownika** | Zamawiający wymaga dokumentacji w języku polskim lub angielskim.Możliwość telefonicznego sprawdzenia konfiguracji sprzętowej serwera oraz warunków gwarancji po podaniu numeru seryjnego bezpośrednio u producenta lub jego przedstawiciela. |  |

***ZAŁĄCZNIK NR 2***

1. **Opis przedmiotu zamówienia:**

**Część I:**

**Dostawa: Licencji na system ochrony antywirusowej**

**Licencja** wraz z roczną subskrypcją od 29.06.2021 r. na kompletny system ochrony antywirusowej i antyspamowej z centralnym zarządzaniem dla wszystkich urządzeń komputerowych w łącznej ilości 1200 sztuk obejmujący:

* Ochronę antywirusową i antyspamową dla sieci komputerowej składającej się z komputerów i serwerów z systemami operacyjnymi: Windows XP, Windows Vista, Windows 7, Windows 8, Windows 10, Linux, Mac OS, Windows 2003 R2 Server, Windows 2008 R2 Server, Windows 2012 R2 Server, Windows 2016 Server, Windows 2019 Server;
* Ochronę urządzeń mobilnych (tablety i smartfony);
* Ochronę antywirusową i antyspamową dla kontrolerów domeny Windows Server 2016, klastra Hyper-V systemu Windows Server 2008 R2, klastra Hyper-V systemu Windows Server 2016, Windows 2019 Server, serwera plików, drukarek, systemu Microsoft Exchange 2016 (dwa serwery w DAG), serwera kopii zapasowych Microsoft DPM 2016, serwera FTP, WSUS, serwerów aplikacji;
* System centralnego zarządzania ochroną antywirusową i antyspamową sieci komputerowej;

Zamawiający informuje, że aktualnie używa systemu antywirusowego ESET Endpoint Security.Wykonawca może zaoferować inne oprogramowanie spełniające kryteria podane w specyfikacji pod warunkiem wykonania do dnia 29.06.2021 r. dodatkowo pełnego wdrożenia obejmującego usługi:

* Opracowanie projektu migracji systemu antywirusowego wraz z procedurami deinstalacyjnymi aktualnego oprogramowania dla systemów operacyjnych Windows, Linux i Mac OS.
* Odinstalowanie aktualnie zainstalowanego systemu antywirusowego ESET ze stacji roboczych w domenie i poza nią, serwerów i serwera poczty elektronicznej.
* Zainstalowanie oraz skonfigurowanie dostarczonego oprogramowania antywirusowego i antyspamowego na wszystkich komputerach i serwerach zamawiającego, w tym na serwerze poczty elektronicznej.
* Sporządzenie dokumentacji powdrożeniowej.

**Usługa: Wsparcie techniczne**

Wsparcie techniczne środowiska serwerowego oraz systemu ochrony antywirusowej i antyspamowej składającego się z:

* + - serwerów i macierzy dyskowych,
		- domeny Active Directory,
		- środowiska wirtualnego Microsoft Hyper-V,
		- środowiska do zarządzania wirtualizacją Microsoft SCVMM
		- środowiska systemu poczty Microsoft Exchange
		- środowiska kopii zapasowych Microsoft System Center DPM .

W skład fizycznego środowiska serwerowego wchodzą:

* 2 kontrolery domeny z systemami Windows 2016 Serwer,
* 2 serwery Microsoft Exchange 2016 pracujące w klastrze DAG,
* 2 serwery kopii zapasowych jeden z systemem Microsoft DPM 2016 z systemem Windows Server 2016, drugi z systemem Microsoft DPM 2019 z systemem Windows Server 2016
* klaster dwuwęzłowy Hyper-V maszyn wirtualnych z systemami Windows 2008 R2 wraz z macierzami dyskowymi
* klaster trzywęzłowy Hyper-V maszyn wirtualnych z systemami Windows 2019 wraz z macierzami dyskowymi
* serwer z konsolą do zarządzania maszynami wirtualnymi Microsoft SCVMM 2012 R2 oparty na systemie Windows Server 2012 R2.

Na platformie wirtualnej pracują następujące maszyny wirtualne:

* serwery aplikacji Windows oraz Linux,
* serwer do zarządzania drukowaniem z systemem Windows 2003 R2 Server, Windows Server 2016
* serwer plików z systemem Windows Server 2016
* serwer do zarządzania aktualizacjami WSUS z systemem Windows Server 2019,
* serwer ochrony antywirusowej i antyspamowej z konsolą do zarządzania ERA 7.2 oparty na systemie Windows Server 2012 R2,
* serwer FTP z systemem Windows 2008 R2 Server
* serwer zarządzania macierzami Dell z systemem Windows Server 2012 R2.

**Część II: Dostawa**

1. **Certyfikatu** **SSL Wildcard z roczną subskrypcją o parametrach** nie gorszych niż:
* zgodność ze standardem X.509 v.3 (RFC5280),
* zabezpieczony funkcją skrótu SHA2,
* obsługa siły szyfrowania połączeń do 256 bitów,
* wsparcie dla SGC (Server Gated Cryptography),
* obsługa kluczy o długości 4096 bitów i więcej,
* minimalna długość kluczy kryptograficznych: RSA lub DSA 2048 bit, EC 571 bit: NIST K-571 oraz NIST B-571,
* wydany przez CERTUM PCC posiadający aktualny certyfikat zgodności ze standardami [WebTrust](http://www.certum.pl/certum/certum%2Cpz_o_webtrust.xml),
* możliwa weryfikacja statusu certyfikatu przy pomocy list CRL oraz protokołu OCSP.
1. **Licencji Microsoft zapewniających zdalny dostęp do serwerów Windows:** WinRmtDsktpSvcsCAL Sngl License/SoftwareAssurancePack Academic OLP 1License NoLevel UsrCAL – **50 licencji**
2. **Licencji Microsoft – system operacyjny Windows Server Standard**

WindowsServerSTDCORE Sngl License/SoftwareAssurancePack Academic OLP 2Licenses NoLevel CoreLic – **4 licencje**

1. **Serwer usług pulpitu zdalnego o minimalnych parametrach podanych w załączniku nr 1a**

Parametry/wymagania techniczne i jakościowe odnoszące się do przedmiotu zamówienia

**Oprogramowanie antywirusowe**

**Ochrona stacji roboczych - Windows**

1. Pełne wsparcie dla systemu Windows 7/Windows 8/Windows 8.1/Windows 10.

2. Wsparcie dla 32- i 64-bitowej wersji systemu Windows.

3. Wersja programu dostępna co najmniej w języku polskim oraz angielskim.

4. Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.

5. Pomoc w programie (help) i dokumentacja do programu dostępna w języku polskim oraz angielskim.

6. Skuteczność programu potwierdzona nagrodami VB100 i AV-comparatives.

**Ochrona antywirusowa i antyspyware**

1. Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.
2. Wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
3. Wbudowana technologia do ochrony przed rootkitami.
4. Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.
5. Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.
6. Możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie” lub według harmonogramu.
7. System ma posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
8. Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
9. Skanowanie „na żądanie” pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
10. Możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie” i według harmonogramu.
11. Możliwość skanowania dysków sieciowych i dysków przenośnych.
12. Skanowanie plików spakowanych i skompresowanych.
13. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
14. Administrator ma mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
15. Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
16. Brak konieczności ponownego uruchomienia (restartu) komputera po instalacji programu.
17. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
18. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
19. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
20. Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
21. Wbudowany konektor dla programów MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
22. Skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu MS Outlook, Outlook Express, Windows Mail i Windows Live Mail.
23. Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP „w locie” (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego, zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).
24. Automatyczna integracja skanera POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
25. Możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
26. Skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
27. Blokowanie możliwości przeglądania wybranych stron internetowych. Program musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
28. Możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
29. Automatyczna integracja z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
30. Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
31. Program ma zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
32. Musi istnieć możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
33. Administrator ma mieć możliwość zdefiniowania portów TCP, na których aplikacja będzie realizowała proces skanowania ruchu szyfrowanego.
34. Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.
35. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
36. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
37. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
38. Program ma posiadać wbudowane dwa niezależne moduły heurystyczne – jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
39. Musi być możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (bez ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
40. Do wysłania próbki zagrożenia do laboratorium producenta, aplikacja nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
41. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
42. Musi być też możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
43. Program ma mieć możliwość zabezpieczenia konfiguracji programu hasłem, w taki sposób, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
44. Powinna być też możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji program musi pytać o hasło.
45. Hasło do zabezpieczenia konfiguracji programu oraz deinstalacji musi być takie samo.
46. Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
47. Program ma mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
48. Po instalacji programu, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
49. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
50. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
51. Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
52. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.
53. Program musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
54. Program ma umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
55. Program ma posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
56. W momencie podłączenia zewnętrznego nośnika, aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
57. Administrator ma posiadać możliwość takiej konfiguracji programu, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem użytkownika.
58. Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (HIPS).
59. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
	* + tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
		+ tryb interaktywny, w którym to program pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
		+ tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
		+ tryb uczenia się, w którym program uczy się aktywności systemu i użytkownika oraz tworzy odpowiednie reguły w czasie określonym przez użytkownika. Po wygaśnięciu tego czasu program musi samoczynnie przełączyć się w tryb pracy oparty na regułach,
		+ tryb inteligentny, w którym program będzie powiadamiał wyłącznie o szczególnie podejrzanych zdarzeniach.
60. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
61. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
62. Oprogramowanie musi posiadać zaawansowany skaner pamięci.
63. Program musi być wyposażony w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
64. Program ma być wyposażony we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
65. Funkcja, generująca taki log, ma posiadać przynajmniej 9 poziomów filtrowania wyników pod kątem tego, które z nich są podejrzane dla programu i mogą stanowić zagrożenie bezpieczeństwa.
66. Program ma posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
67. Ma być automatyczna, inkrementacyjna aktualizacja silnika detekcji.
68. Ma istnieć możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
69. Ma być możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
70. Program musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
71. Program musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
72. Program musi być wyposażony w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
73. Program ma być wyposażony tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne, zapora sieciowa).
74. Aplikacja musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
75. W momencie wykrycia trybu pełnoekranowego, aplikacja ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań aplikacji.
76. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
77. Program ma być wyposażony w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, pracy zapory osobistej, modułu antyspamowego, kontroli stron internetowych i kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
78. Wsparcie techniczne do programu ma być świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.
79. Program musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
80. Program musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
81. Możliwość podejrzenia informacji o licencji, która znajduje się w programie.
82. W trakcie instalacji program ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
83. W programie musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
84. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej.
85. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
86. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
87. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
88. Program musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
89. Musi być możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji ma być w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
90. Program musi posiadać możliwość definiowana stanów aplikacji, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
91. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
92. Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
93. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
94. Aplikacja musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
95. Administrator ma mieć możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
96. Program musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść”.
97. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
98. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
99. Program ma posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
100. Administrator musi posiadać możliwość zastosowania reguł dla kontroli dostępu do stron w zależności od zdefiniowanego przedziału czasowego.
101. Program ma mieć wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych*.*
102. Program musi umożliwiać ochronę przed dołączeniem komputera do sieci botnet.
103. Program ma posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.

**Ochrona przed spamem**

1. Ochrona antyspamowa dla programów pocztowych MS Outlook, Outlook Express, Windows Mail oraz Windows Live Mail.
2. Program ma umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
3. Automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
4. Możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
5. Możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
6. Możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
7. Możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
8. Program ma domyślnie współpracować z folderem „Wiadomości-śmieci”, dostępnym w programie Microsoft Outlook.
9. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana”
10. Program ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana”.
11. Program musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

**Administracja zdalna**

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI” oraz „Golden Master Image”.
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.
21. Administrator musi posiadać możliwość instalacji modułu do zarządzania urządzeniami mobilnymi – MDM.
22. Serwer administracyjny musi posiadać możliwość sprawdzenia lokalizacji dla urządzeń z systemami iOS.
23. Serwer administracyjny musi posiadać możliwość wdrożenia urządzenia z iOS z wykorzystaniem programu DEP.
24. Serwer administracyjny musi posiadać możliwość konfiguracji polityk zabezpieczeń takich jak: ograniczenia funkcji urządzenia, blokadę usuwania aplikacji, konfigurację usługi Airprint, konfigurację ustawień Bluetooth, Wi-Fi, VPN dla urządzeń z systemem iOS 10 oraz 11.
25. Serwer administracyjny musi posiadać możliwość lokalizacji urządzeń mobilnych przy wykorzystaniu Google maps, Bing maps, OpenStreetMap.
26. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
27. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
28. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
29. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający, serwer proxy, moduł zarządzania urządzeniami mobilnymi.
30. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux, Android.
31. Serwer administracyjny musi pozwalać na zarządzanie urządzeniami z systemem iOS.
32. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
33. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
34. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
35. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
36. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
37. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
38. W przypadku braku zainstalowanego produktu zabezpieczającego na urządzeniu mobilnym z systemem Android, musi istnieć możliwość jego pobrania ze sklepu Google Play.
39. Administrator musi posiadać możliwość utworzenia listy autoryzowanych urządzeń mobilnych, które mogą zostać podłączone do serwera centralnej administracji.
40. Serwer administracyjny musi posiadać możliwość zablokowania, odblokowania, wyczyszczenia zawartości, zlokalizowania oraz uruchomienia syreny na zarządzanym urządzaniu mobilnym. Funkcjonalność musi wykorzystywać połączenie internetowe, a nie komunikację za pośrednictwem wiadomości SMS.
41. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
42. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi.
43. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
44. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
45. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
46. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
47. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
48. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.
49. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
50. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
51. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
52. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
53. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
54. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
55. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
56. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
57. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
58. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
59. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
60. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
61. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
62. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
63. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
64. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
65. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
66. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
67. Serwer administracyjny musi być wyposażony w mechanizm importu oraz eksportu szablonów raportów.
68. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
69. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF, CSV oraz PS.
70. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
71. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
72. Powiadomienia mailowe mają być wysyłane w formacie HTML.
73. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.
74. Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
75. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
76. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
77. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
78. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
79. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
80. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
81. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
82. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
83. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
84. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: antyspam, firewall, HIPS, kontrola dostępu do urządzeń, kontrola dostępu do stron internetowych.
85. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
86. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
87. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.
88. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
89. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
90. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
91. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
92. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
93. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
94. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

**Zakres czynności do wykonania w ramach wsparcia technicznego:**

1. Identyfikacja potencjalnych problemów w działaniu serwerów na bazie logów
i dzienników zdarzeń oraz podjęcie czynności naprawczych.
2. Optymalizacja konfiguracji systemów na bazie monitoringu wydajności serwerów.
3. Instalacja i testowanie poprawek zbiorczych wydawanych przez Microsoft
dla serwerów i systemów objętych wsparciem technicznym.
4. Zmiany w konfiguracjach zadań tworzenia kopii zapasowych serwerów mające
na celu usuwanie nieprawidłowości.
5. Optymalizacja działania kontrolerów domeny poprzez weryfikację: ustawień zasad grup w GPO i dystrybucji zasad grup do użytkowników, replikacji danych usług katalogowych, poprawności rozwiązywania nazw DNS.
6. Odnawianie certyfikatów oraz weryfikacja poprawności działania serwera certyfikatów.
7. Utworzenie arkusza bazy wiedzy rozwiązywanych problemów

**Serwer WSUS:**

1. Weryfikacja procedur aktualizacji oprogramowania Microsoft na serwerze i stacjach roboczych.
2. Weryfikacja poprawności pobierania aktualizacji oprogramowania serwera WSUS z witryny Microsoft.
3. Rozwiązywanie problemów dotyczących stacji, na których występują błędy aktualizacji.
4. Instalacja nowych wersji i poprawek WSUS.

**System antywirusowy i antyspamowy dla serwerów i stacji roboczych:**

* 1. Aktualizacja oprogramowania do aktualnych wersji.
	2. Weryfikacja procedur ochrony przed wirusami.
	3. Nadzór nad sprawną i bezawaryjną pracą serwera antywirusowego;
	4. Weryfikacja poprawności pobierania aktualizacji sygnatur i oprogramowania antywirusowego.
	5. Optymalizacja dystrybucji sygnatur wirusów pobranych na serwery i stacje klienckie.
	6. Weryfikacja stacji, na których występują błędy aktualizacji, usuwanie nieprawidłowości w tym zakresie.

**Serwer poczty elektronicznej Exchange 2016:**

1. Identyfikacja potencjalnych problemów w działaniu serwerów poprzez weryfikację: dzienników zdarzeń, stanu logów i sprawdzenie poprawności funkcjonowania usług serwera poczty oraz podjęcie czynności naprawczych .
2. Pomoc w rozwiązywanie problemów z dostępnością systemu pocztowego za pomocą przeglądarek z sieci wewnętrznej i zewnętrznej.
3. Optymalizacja struktury logicznej (nazewnictwo skrzynek użytkowników, list dystrybucyjnych) i fizycznej (np. ilość skrzynek w grupach magazynowania) systemu poczty
4. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera poczty dystrybuowanych przez producenta systemu firmę Microsoft.
5. Pomoc w rozwiązywaniu problemów związanych z przesyłaniem poczty.

**System antywirusowy i antyspamowy dla serwera poczty elektronicznej Exchange:**

1. Konfiguracja reguł filtrowania poczty pod względem wirusów, robaków i spamu oraz reguł filtrowania treści wiadomości i załączników.
2. Konfiguracja treści powiadomień w zależności od przesyłanych komunikatów.
3. Instalacja i testowanie poprawek do oprogramowania antywirusowego dla serwera poczty dystrybuowanych przez producenta systemu.

**System kopii zapasowych Microsoft SCDPM**

* 1. Weryfikacja poprawności wykonywania zadań kopii zapasowych systemu Exchange
	2. Optymalizacja zadań kopii zapasowych
	3. Odtwarzanie na żądanie skrzynek użytkowników z okresu objętego ochroną
	4. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera kopii zapasowych dystrybuowanych przez producenta systemu firmę Microsoft.
	5. Rozwiązywanie problemów związanych z działaniem serwera.

**System zarządzania maszynami wirtualnymi Microsoft SCVMM**

1. Identyfikacja potencjalnych problemów w działaniu serwera poprzez weryfikację: dzienników zdarzeń, stanu logów i sprawdzenie poprawności funkcjonowania usług oraz podjęcie czynności naprawczych.
2. Instalacja i testowanie poprawek zbiorczych (tzw. Service Pack) do serwera SCVMM dystrybuowanych przez producenta systemu firmę Microsoft.
3. Rozwiązywanie problemów związanych z zarządzaniem maszynami wirtualnymi.

**Środowisko wirtualne Hyper-V:**

1. Utrzymanie ciągłości pracy maszyn wirtualnych (reakcja na awarie), w tym usuwanie problemów sprzętowych i oprogramowania.
2. Optymalizacja konfiguracji węzłów klastra do pracy z macierzami.
3. Przygotowanie procedur archiwizacji i odtwarzania maszyn wirtualnych.
4. Optymalizacja działania maszyn wirtualnych.
5. Przygotowanie szablonów maszyn wirtualnych dla wybranych systemów operacyjnych.

**W ramach wsparcia technicznego zamawiający wymaga od Wykonawcy następujących usług:**

* Stałej wizyty serwisowej, trwającej minimum 8 godzin, realizowanej raz w miesiącu w ustalonym dniu każdego miesiąca. Celem wizyty ma być kontrola działania wszystkich systemów objętych umową i rozwiązywanie bieżących problemów. Dokładny zakres czynności do wykonania jest opisany powyżej. Łączna ilość czasu poświęconego na planowane wizyty serwisowe ma wynosić 12 dni roboczych rocznie.
* Wsparcia-serwisu w zakresie usuwania awarii i problemów związanych z działaniem ww. środowiska serwerowego.

Czas reakcji Wykonawcy na zgłoszony problem – maksymalnie 1 godzina od zgłoszenia w każdym dniu roku, o każdej porze.

 „Reakcja” – przybycie serwisanta do siedziby Zamawiającego i przystąpienie do usuwania awarii. Na świadczenie wsparcia-serwisu przeznaczonych ma być minimum 18 dni roboczych rocznie.

* Wykonawca dołączy informację o sposobie zgłaszania problemów i adresie punktu serwisowego, umożliwiającego dotarcie do siedziby Zamawiającego w ciągu 1 godziny od zgłoszenia awarii.
* Świadczenie wsparcia przez 12 miesięcy od 01.07.2021 r.

***ZAŁĄCZNIK NR 3***

***Część I***

 **UMOWA nr ………..………projekt**

zawarta w dniu ………………… r. w Gdyni pomiędzy:

**Akademią Marynarki Wojennej im. Bohaterów Westerplatte,** ul. Śmidowicza 69, 81-127 Gdynia, **NIP: 586-010-46-93,**

reprezentowaną przez: *:*

**Rektora-Komendanta AMW- kontradmirała prof. dr hab. Tomasza Szubrychta,**

zwaną dalej **Zamawiającym,**

a

firmą:

**………………………………………………………………………………………………**

wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej w dniu ……., pod numerem **NIP: ………….., REGON …………….** reprezentowaną przez **………………………………** ,

zwaną dalej **Wykonawcą**,

zwanymi dalej łącznie Stronami, a każdy indywidualnie Stroną,

o następującej treści:

**§1**

1. W wyniku wyboru oferty Wykonawcy, w postępowaniu o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego na podstawie art. 129 ust. 1 pkt 1 oraz art. 132 i nast. ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych,** o nr ………………………, w dniu ……………., Wykonawca zrealizuje na rzecz Zamawiającego następujące świadczenia:
2. udzielenie LICENCJI WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I  ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ I EWENTUALNE WDROŻENIE W PRZYPADKU OFEROWANIA INNEGO ANTYWIRUSA;
3. usługę WSPARCIA TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ  ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO,

zgodnie z ofertą złożoną w postępowaniu przetargowym.

**§2**

Wykonawca oświadcza, że:

1. Jest uprawniony oraz posiada niezbędne kwalifikacje do pełnej realizacji przedmiotu Umowy.
2. Realizowany przedmiot Umowy może być wykorzystywany bez naruszania praw własności osób trzecich, w tym praw patentowych i praw autorskich.
3. Realizowany przedmiot Umowy spełnia normy przewidziane prawem polskim.

**§3**

1. Realizacja przedmiotu Umowy w przedmiocie dostawy licencji i opcjonalnie świadczenia usługi wdrożeniowej systemu antywirusowego zostanie zakończona do dnia 29.06.2021 r.
2. Wsparcie techniczne realizowane będzie w terminie od dnia 01.07.2021 r. do dnia 30.06.2022 r.
3. Odbiór przedmiotu Umowy tytułem dostarczenia licencji nastąpi na podstawie protokołu przekazania/odbioru podpisanego przez obie Strony.
4. Wykonawca ma obowiązek osobistego wykonania całości zamówienia.
5. W przypadku przekroczenia terminu określonego w ust. 1 i 2 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% ceny określonej w § 4 ust. 1 za każdy dzień opóźnienia, nie więcej jednak niż 20% ceny.
6. Za odstąpienie od Umowy z przyczyn niezależnych od Zamawiającego Wykonawca zapłaci karę umowną w wysokości 5% wartości niewykonanego zakresu Umowy.
7. Za każde opóźnienie w usunięciu wad przedmiotu zamówienia, ujawnionych w okresie gwarancji – Wykonawca zapłaci karę umowną w wysokości 0,5% wartości przedmiotu Umowy za każdy dzień opóźnienia liczonego od dnia wyznaczonego na ich usunięcie, nie więcej jednak niż 10% ceny.
8. Zamawiający zastrzega sobie prawo potrącenia równowartości naliczonych kar umownych z wynagrodzenia Wykonawcy wynikającego z wystawionej przez Wykonawcę faktury.
9. Jeżeli szkoda spowodowana niewykonaniem lub nienależytym wykonaniem Umowy przekroczy wartość zastrzeżonych kar umownych, bądź wynika z innych tytułów niż zastrzeżone, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego do pełnej wysokości szkody.
10. Łączna wysokość kar umownych, których może dochodzić każda ze stron wynosi 40% ceny określonej w § 4 ust. 1 niniejszej Umowy.

**§4**

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy kwotę brutto w łącznej wysokości **………………………………..zł**

*(słownie: ………………………………………………………………………….. zł …… groszy).*

1. Zapłata nastąpi zgodnie z ofertą, po wykonaniu przedmiotu umowy w następujących transzach:
2. tytułem dostarczenia licencji – kwota ……. zł, płatna po podpisaniu przez Zamawiającego protokołu zdawczo/odbiorczego;
3. tytułem usługi wsparcia technicznego – kwota ………. zł, płatna w 12-tu równych miesięcznych ratach na podstawie wystawionych faktur VAT.
4. Ww. płatności realizowane będą przelewem w terminie 30 dni od doręczenia prawidłowo wystawionej faktury VAT, z konta Zamawiającego:

**SANTANDER BANK POLSKA SA**

**95 1500 1881 1210 2003 3251 0000**

na konto **Wykonawcy** w:

……………………………………………………………………………………………

przy czym za dzień zapłaty Strony Umowy przyjmują datę obciążenia rachunku **Zamawiającego**.

**§5**

**Wykonawca** deklaruje następujące warunki serwisu:

|  |  |
| --- | --- |
| Czas reakcji serwisowej: | 1 godz. |
| Miejsce świadczenia usług serwisowych | AMW |
|  |
| Zgłaszanie potrzeb serwisowych – wskazanie minimum 2 kontaktów |
| Nazwiska osób "kontaktowych" |  |
| e-maile |  |
| Telefony |  |
| Faksy |  |
| Inny sposób zgłaszania potrzeby serwisu – wg załączonej procedury |  |

**§6**

Uprawnienia z tytułu rękojmi nie są wyłączone.

**§7**

Wszystkie zmiany Umowy wymagają zgody obu Stron w formie pisemnej pod rygorem nieważności, z uwzględnieniem art. 455 Prawa zamówień publicznych.

**§8**

**Wykonawca** nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osoby trzecie bez uprzedniej pisemnej zgody **Zamawiającego**.

**§9**

W sprawach nie uregulowanych niniejszą Umową będą miały zastosowanie odpowiednie przepisy ustawy Prawo zamówień publicznych oraz kodeksu cywilnego.

**§10**

1. Zakres świadczenia **Wykonawcy** wynikający z Umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
2. Umowa jest nieważna w części wykraczającej poza określenie przedmiotu zamówienia zawartego w specyfikacji istotnych warunków zamówienia.
3. Zakazuje się zmian postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub w specyfikacji istotnych warunków zamówienia oraz określił warunki takiej zmiany.
4. Zamawiający może odstąpić od umowy:
5. 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;
6. jeżeli zachodzi co najmniej jedna z następujących okoliczności:
	1. dokonano zmiany umowy z naruszeniem art. 454 i art. 455,
	2. Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108,
	3. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.
7. Z zastrzeżeniem przepisów odrębnych, Umowa podlega unieważnieniu w przypadkach określonych w art. 457 Prawa zamówień publicznych.
8. Strony zgodnie oświadczają, iż tryb przewidziany w ustawie z dnia 11.09.2019 Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) i aktach wykonawczych do tej ustawy został zachowany.
9. Zamawiający, zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t. j. Dz. U. z 2021 r. poz. 424), oświadcza iż posiada status dużego przedsiębiorcy.
10. Strony zgodnie oświadczają, że zmiany: stawki podatku od towarów i usług oraz podatku akcyzowego, wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę, zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub ubezpieczenie zdrowotne, zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (Dz. U. poz. 2215 oraz z 2019 r. poz. 1074 i 1572) - nie będą miały wpływu na koszty wykonania zamówienia przez Wykonawcę.

**§11**

1. W czasie wykonywania niniejszej Umowy oraz w okresie gwarancji (rękojmi), **Wykonawca** jest zobowiązany do pisemnego powiadamiania Zamawiającego :
* o zmianie siedziby Wykonawcy,
* o upadłości Wykonawcy,
* o wszczęciu postępowania układowego,
* o ogłoszeniu likwidacji,
* o zawieszeniu działalności,
* o zmianie w zakresie rejestracji działalności Wykonawcy.
1. O wystąpieniu powyższych okoliczności, Wykonawca zobowiązany jest powiadomić Zamawiającego najpóźniej w terminie 3 dni od ich zaistnienia pod rygorem naliczenia kary umownej w wysokości 1 % ceny określonej w § 4 ust. 1.

**§12**

1. Spory wynikłe na tle realizacji niniejszej Umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
2. W przypadku rozbieżności pomiędzy zapisami Umowy, a treścią załączników do niej, pierwszeństwo zachowują postanowienia Umowy.

**§13**

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy oraz dwa dla Zamawiającego.

------------------------ -------------------------

 **Wykonawca Zamawiający**

***Część II***

 **UMOWA nr ………..………projekt**

zawarta w dniu ………………… r. w Gdyni pomiędzy:

**Akademią Marynarki Wojennej im. Bohaterów Westerplatte,** ul. Śmidowicza 69, 81-127 Gdynia, **NIP: 586-010-46-93,**

reprezentowaną przez: *:*

**Rektora-Komendanta AMW- kontradmirała prof. dr hab. Tomasza Szubrychta,**

zwaną dalej **Zamawiającym,**

a

firmą:

**………………………………………………………………………………………………**

wpisaną do Centralnej Ewidencji i Informacji o Działalności Gospodarczej w dniu ……., pod numerem **NIP: ………….., REGON …………….** reprezentowaną przez **………………………………** ,

zwaną dalej **Wykonawcą**,

zwanymi dalej łącznie Stronami, a każdy indywidualnie Stroną,

o następującej treści:

**§1**

1. W wyniku wyboru oferty Wykonawcy, w postępowaniu o udzielenie zamówienia publicznego w trybie **przetargu nieograniczonego na podstawie art. 129 ust. 1 pkt 1 oraz art. 132 i nast. ustawy z dnia 11.09.2019 r. - Prawo zamówień publicznych,** o nr ………………………, w dniu ……………., Wykonawca zrealizuje na rzecz Zamawiającego następujące świadczenia:
2. dostawę CERTYFIKATU SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ
3. dostawę SERWERA USŁUG PULPITU ZDALNEGO,

zgodnie z ofertą złożoną w postępowaniu przetargowym.

**§2**

Wykonawca oświadcza, że:

1. Jest uprawniony oraz posiada niezbędne kwalifikacje do pełnej realizacji przedmiotu Umowy.
2. Realizowany przedmiot Umowy może być wykorzystywany bez naruszania praw własności osób trzecich, w tym praw patentowych i praw autorskich.
3. Realizowany przedmiot Umowy spełnia normy przewidziane prawem polskim.

**§3**

1. Certyfikat, serwer wraz z oprogramowaniem dostarczone zostaną do dnia 30.08.2021 r.
2. Odbiór przedmiotu Umowy tytułem dostarczenia certyfikatu oraz serwera z oprogramowaniem nastąpi na podstawie protokołu przekazania/odbioru podpisanego przez obie Strony.
3. Wykonawca ma obowiązek osobistego wykonania całości zamówienia.
4. W przypadku przekroczenia terminu określonego w ust. 1 Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1% ceny określonej w § 4 ust. 1 za każdy dzień opóźnienia, nie więcej jednak niż 20% ceny.
5. Za odstąpienie od Umowy z przyczyn niezależnych od Zamawiającego Wykonawca zapłaci karę umowną w wysokości 5% wartości niewykonanego zakresu Umowy.
6. Za każde opóźnienie w usunięciu wad przedmiotu zamówienia, ujawnionych w okresie gwarancji – Wykonawca zapłaci karę umowną w wysokości 0,5% wartości przedmiotu Umowy za każdy dzień opóźnienia liczonego od dnia wyznaczonego na ich usunięcie, nie więcej jednak niż 10% ceny.
7. Zamawiający zastrzega sobie prawo potrącenia równowartości naliczonych kar umownych z wynagrodzenia Wykonawcy wynikającego z wystawionej przez Wykonawcę faktury.
8. Jeżeli szkoda spowodowana niewykonaniem lub nienależytym wykonaniem Umowy przekroczy wartość zastrzeżonych kar umownych, bądź wynika z innych tytułów niż zastrzeżone, Zamawiający zastrzega sobie prawo dochodzenia odszkodowania uzupełniającego do pełnej wysokości szkody.
9. Łączna wysokość kar umownych, których może dochodzić każda ze stron wynosi 40% ceny określonej w § 4 ust. 1 niniejszej Umowy.

**§4**

1. Zamawiający zobowiązuje się zapłacić Wykonawcy za przedmiot umowy kwotę brutto **………………………………..zł**

*(słownie: ………………………………………………………………………….. zł …… groszy).*

1. Zapłata nastąpi zgodnie z ofertą, po wykonaniu przedmiotu umowy. Kwota płatna po podpisaniu przez Zamawiającego protokołu zdawczo/odbiorczego;
2. Ww. płatności realizowane będą przelewem w terminie 30 dni od doręczenia prawidłowo wystawionej faktury VAT, z konta Zamawiającego:

**SANTANDER BANK POLSKA SA**

**95 1500 1881 1210 2003 3251 0000**

na konto **Wykonawcy** w:

……………………………………………………………………………………………

przy czym za dzień zapłaty Strony Umowy przyjmują datę obciążenia rachunku **Zamawiającego**.

**§5**

Uprawnienia z tytułu rękojmi nie są wyłączone.

**§6**

Wszystkie zmiany Umowy wymagają zgody obu Stron w formie pisemnej pod rygorem nieważności, z uwzględnieniem art. 455 Prawa zamówień publicznych.

**§7**

**Wykonawca** nie może przenieść praw i obowiązków wynikających z niniejszej Umowy na osoby trzecie bez uprzedniej pisemnej zgody **Zamawiającego**.

**§8**

1. Zakres świadczenia **Wykonawcy** wynikający z Umowy jest tożsamy z jego zobowiązaniem zawartym w ofercie.
2. Umowa jest nieważna w części wykraczającej poza określenie przedmiotu zamówienia zawartego w specyfikacji istotnych warunków zamówienia.
3. Zakazuje się zmian postanowień zawartej Umowy w stosunku do treści oferty, na podstawie której dokonano wyboru Wykonawcy, chyba że Zamawiający przewidział możliwość dokonania takiej zmiany w ogłoszeniu o zamówieniu lub w specyfikacji istotnych warunków zamówienia oraz określił warunki takiej zmiany.
4. Zamawiający może odstąpić od umowy:
	1. 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;
	2. jeżeli zachodzi co najmniej jedna z następujących okoliczności:
		1. dokonano zmiany umowy z naruszeniem art. 454 i art. 455,
		2. Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108,
		3. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.
5. Z zastrzeżeniem przepisów odrębnych, Umowa podlega unieważnieniu w przypadkach określonych w art. 457 Prawa zamówień publicznych.
6. Strony zgodnie oświadczają, iż tryb przewidziany w ustawie z dnia 11.09.2019 Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 2019 z późn. zm.) i aktach wykonawczych do tej ustawy został zachowany.
7. Zamawiający, zgodnie z art. 4c ustawy z dnia 8 marca 2013 r. o przeciwdziałaniu nadmiernym opóźnieniom w transakcjach handlowych (t. j. Dz. U. z 2021 r. poz. 424), oświadcza iż posiada status dużego przedsiębiorcy.

**§9**

1. W czasie wykonywania niniejszej Umowy oraz w okresie gwarancji (rękojmi), **Wykonawca** jest zobowiązany do pisemnego powiadamiania Zamawiającego :
* o zmianie siedziby Wykonawcy,
* o upadłości Wykonawcy,
* o wszczęciu postępowania układowego,
* o ogłoszeniu likwidacji,
* o zawieszeniu działalności,
* o zmianie w zakresie rejestracji działalności Wykonawcy.
1. O wystąpieniu powyższych okoliczności, Wykonawca zobowiązany jest powiadomić Zamawiającego najpóźniej w terminie 3 dni od ich zaistnienia pod rygorem naliczenia kary umownej w wysokości 1 % ceny określonej w § 4 ust. 1. W przypadku zaistnienia okoliczności, o których mowa w ust. 1.

**§10**

1. Spory wynikłe na tle realizacji niniejszej Umowy będzie rozstrzygał sąd powszechny właściwy dla siedziby Zamawiającego.
2. W przypadku rozbieżności pomiędzy zapisami Umowy, a treścią załączników do niej, pierwszeństwo zachowują postanowienia Umowy.
3. W sprawach nie uregulowanych niniejszą Umową będą miały zastosowanie odpowiednie przepisy ustawy Prawo zamówień publicznych oraz kodeksu cywilnego.

**§11**

Umowę sporządzono w trzech jednobrzmiących egzemplarzach, jeden dla Wykonawcy oraz dwa dla Zamawiającego.

 ---------------------------- -------------------------

 **Wykonawca Zamawiający**

***ZAŁĄCZNIK NR 4***

*Wykonawca:*

*………………………………….*

*…………………………………..*

*reprezentowany przez:*

*……………………………………*

*…………………………………….*

*(imię, nazwisko, stanowisko/podstawa do*

*reprezentacji)*

**OŚWIADCZENIE[[2]](#footnote-2)**

**O PRZYNALEŻNOŚCI / BRAKU PRZYNALEŻNOŚCI**

**DO GRUPY KAPITAŁOEJ**

Na potrzeby postępowania o udzielenie zamówienia publicznego pn.

***Część I:***

***• LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ***

***• WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO***

***Część II:***

***• CERTYFIKAT SSL WILDCARD Z ROCZNĄ SUBSKRYPCJĄ***

***• SERWER USŁUG PULPITU ZDALNEGO***

 ***numer referencyjny: 11/ZP/21***, prowadzonego w trybie przetargu nieograniczonego, na podstawie ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2019 r. poz. 2019 ze zm.), oświadczam/y, że:

**- należę[[3]](#footnote-3)\*** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, 1571 i 1667), co następujący Wykonawca, który złożył odrębną ofertę, w postępowaniu:

…………………………………………………………………………………………

…………………………………………………………………………………………

lub

**- nie należę \*** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2019 r. poz. 369, 1571 i 1667), co inny Wykonawca, który złożył odrębną ofertę, w postępowaniu.

Data, miejscowość oraz podpis(-y):

***ZAŁĄCZNIK NR 5***

**WYKAZ USŁUG ZGODNY Z WARUNKAMI SWZ**

**ANTYWIRUS - WSPARCIE**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Odbiorca(dokładna nazwa i adresi tel. kontaktowy) | Data wykonania(czas trwania umowy od - do) | Przedmiotwykonywanej usługi | Wartość |
|  |  |  |  |  |
|  |  |  |  |  |
|   |  |  |  |  |
|  |  |  |  |  |

 **UWAGA !!!**

W załączeniu dokumenty potwierdzające należyte wykonanie usług wyszczególnionych
w powyższym wykazie.

***ZAŁĄCZNIK NR 6***

**WYKAZ OSÓB SKIEROWANYCH DO REALIZACJI ZAMÓWIENIA ZGODNY
Z WARUNKIEM SWZ**

**ANTYWIRUS - WSPARCIE**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Lp. | Imię i Nazwisko | Posiadane kwalifikacje | Wykształcenie | Wykonywane czynności | Doświadczenie | Podstawa do dysponowania |
|  |  |  |  |  |  |  |

***ZAŁĄCZNIK NR 7***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

**OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany

…………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………………….

……………………………………………………………………………………….

…………………………………………………….………………………………….

z siedzibą w ………….……………………………………………………………………………..

**Oświadczam, że:**

Pani/Pan …………………………… posiada certyfikat potwierdzający umiejętność instalowania i konfigurowania oferowanego oprogramowania. Certyfikat musi być wystawiony przez producenta lub autoryzowanego dystrybutora oferowanego oprogramowania lub autoryzowany przez niego ośrodek szkoleniowy.

***ZAŁĄCZNIK NR 8***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

 **OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany

…………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………………….

……………………………………………………………………………………….

…………………………………………………….………………………………….

z siedzibą w ………….……………………………………………………………………………..

**Oświadczam, że:**

Pani/Pan …………………………… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Windows Serwer 2008 lub nowszego.

***ZAŁĄCZNIK NR 9***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

**OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany

…………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………………….

……………………………………………………………………………………….

…………………………………………………….………………………………….

z siedzibą w ………….……………………………………………………………………………..

**Oświadczam, że:**

Pani/Pan …………………………… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność instalowania i konfigurowania systemu Microsoft Exchange 2010 lub nowszego.

***ZAŁĄCZNIK NR 10***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

 **OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany

…………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………………….

……………………………………………………………………………………….

…………………………………………………….………………………………….

z siedzibą w ………….……………………………………………………………………………..

**Oświadczam, że:**

Pani/Pan …………………………… posiada certyfikat potwierdzający ukończenie szkolenia obejmującego umiejętność wdrażania i administrowania środowiskiem wirtualnym opartym o Microsoft Hyper-V

***ZAŁĄCZNIK NR 11***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

**OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany

…………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………………….

……………………………………………………………………………………….

…………………………………………………….………………………………….

z siedzibą w ………….……………………………………………………………………………..

**Oświadczam, że:**

Pani/Pan …………………………… posiada certyfikat potwierdzający umiejętność świadczenia usług serwisowych zgodnie z ITIL (np. ITIL Foundation)

***ZAŁĄCZNIK NR 12***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

**OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany ……………………………………………………………………………….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): …………..……..…….………

…………………………………………………………………………..……………………

…………………………………………………….………………….………………………

z siedzibą w ………….……………………………………………………………………………………

**Oświadczam, że:**

Dysponujemy punktem serwisowym umożliwiającym dotarcie do siedziby Zamawiającego
w ciągu 1 godziny od zgłoszenia serwisowego.

***ZAŁĄCZNIK NR 13***

………………………., dn. ……………………

(pieczęć adresowa Wykonawcy)

**OŚWIADCZENIE**

Przystępując do postępowania w sprawie udzielenia zamówienia publicznego 11/ZP/21 na usługę
i dostarczenie:

**Część I:**

**LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

Ja, niżej podpisany …………………………………………………………………….……….................

(imię i nazwisko)

w imieniu reprezentowanej przeze mnie firmy (nazwa firmy): ………………………

………………………………………………………….……………………………

……………………………………………………...………………………………

z siedzibą w ………….………………………………………………..………………………………

**Oświadczam, że:**

Dysponujemy portalem/systemem serwisowym w którym Zamawiający będzie mógł dokonywać zgłoszeń serwisowych i widzieć szczegóły ich realizacji

***ZAŁĄCZNIK NR 14***

*(Pieczęć firmowa Wykonawcy)*

**OŚWIADCZENIE**

**(dotyczy gdy Wykonawca w celu potwierdzenia spełnienia warunków udziału
w postępowaniu polega na zdolnościach innych podmiotów)**

Oświadczam, iż podmiotem, na którego zasoby powołujemy się na zasadach określonych w art. 118 ustawy PZP, w celu wykazania spełnienia warunków udziału w postępowaniu, jest\*:

……………………………………………………………………..………………………

*(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*

*\* niepotrzebne skreślić*

**PISEMNE ZOBOWIĄZANIE PODMIOTU DO ODDANIA DO DYSPOZYCJI WYKONAWCY NIEZBĘDNYCH ZASOBÓW NA OKRES KORZYSTANIA Z NICH PRZY WYKONYWANIU ZAMÓWIENIA ZGODNIE Z ART. 118 USTAWY PZP**

|  |  |
| --- | --- |
| Nazwa  | ...................................................................... |
| Adres  | ...................................................................... |

Ja (My) niżej podpisany (ni)

………………………………………………………………………………………………….

działając w imieniu i na rzecz : ……………………………………………………………………………………………………………………………………………………………………………………………………

oświadczam(y), że w postępowaniu 11/ZP/21 na:

**Część I:**

**• LICENCJA WRAZ Z ROCZNĄ SUBSKRYPCJĄ NA SYSTEM OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ZASOBÓW SIECI KOMPUTEROWEJ**

**• WSPARCIE TECHNICZNE SYSTEMU OCHRONY ANTYWIRUSOWEJ I ANTYSPAMOWEJ ORAZ ŚRODOWISKA SERWEROWEGO I WIRTUALNEGO**

zobowiązuję (zobowiązujemy) się udostępnić swoje zasoby Wykonawcy:

………………………………………………………………………………………………………………………………………………………………………………….

(pełna nazwa Wykonawcy i adres/siedziba Wykonawcy)

W celu oceny, czy ww. Wykonawca będzie dysponował moimi zasobami w stopniu niezbędnym dla należytego wykonania zamówienia oraz oceny, czy stosunek nas łączący gwarantuje rzeczywisty dostęp do moich zasobów podaję:

1. zakres moich zasobów dostępnych Wykonawcy:

…………………………………………………………………………………………………………………………………………………………………………………………

……………………………………………………………………………………………

1. sposób wykorzystania moich zasobów przez Wykonawcę przy wykonywaniu zamówienia:

……………………………………………………………………………………………

……………………………………………………………………………………………

………………………………………………………………………………………….

1. charakteru stosunku, jaki będzie mnie łączył z Wykonawcą:

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

1. zakres i okres mojego udziału przy wykonywaniu zamówienia:

……………………………………………………………………………………………

***ZAŁĄCZNIK NR 15***

**Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych wynikających z RODO**

Wykonawca ubiegając się o udzielenie zamówienia publicznego jest zobowiązany do wypełnienia wszystkich obowiązków formalno-prawnych związanych z udziałem w postępowaniu. Do obowiązków tych należą m.in. obowiązki wynikające z RODO[[4]](#footnote-4)), w szczególności obowiązek informacyjny przewidziany w **art. 13 RODO** względem osób fizycznych, których dane osobowe dotyczą i od których dane te wykonawca bezpośrednio pozyskał. Jednakże obowiązek informacyjny wynikający z art. 13 RODO nie będzie miał zastosowania, gdy i w zakresie, w jakim osoba fizyczna, której dane dotyczą, dysponuje już tymi informacjami (vide: art. 13 ust. 4).

Wykonawca musi wypełnić obowiązek informacyjny wynikający z **art. 14 RODO** względem osób fizycznych, których dane przekazuje zamawiającemu i których dane pośrednio pozyskał, chyba że ma zastosowanie co najmniej jedno z włączeń, o których mowa w art. 14 ust. 5 RODO.

W celu zapewnienia, że wykonawca wypełnił ww. obowiązki informacyjne oraz ochrony prawnie uzasadnionych interesów osoby trzeciej, której dane zostały przekazane w związku z udziałem wykonawcy w postępowaniu, wykonawca składa w postępowaniu o udzielenie zamówienia publicznego oświadczenie o wypełnieniu przez niego obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO.

Oświadczenie wykonawca składa razem z ofertą.

*Oświadczenie wymagane od wykonawcy w zakresie wypełnienia obowiązków informacyjnych przewidzianych w art. 13 lub art. 14 RODO*

Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 RODO1) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.\*

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

1. Rozporządzenie Prezesa Rady Ministrów z dnia 27 czerwca 2017 r. w sprawie użycia środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego oraz udostępniania i przechowywania dokumentów elektronicznych. [↑](#footnote-ref-1)
2. \* niniejsze oświadczenie składa każdy z Wykonawców wspólnie ubiegających się o udzielenie zamówienia [↑](#footnote-ref-2)
3. \*\* niepotrzebne skreślić [↑](#footnote-ref-3)
4. ) 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). [↑](#footnote-ref-4)