

Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego
Śląskiego Uniwersytetu Medycznego w Katowicach
40-514 Katowice ul. Ceglana 35

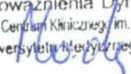
Znak sprawy : DZP.381.15A.2021

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA (SWZ)

na Dostawę systemu zabezpieczeń klasy UTM

Postępowanie o udzielenie zamówienia prowadzone jest w trybie **przetargu nieograniczonego powyżej 139 000 EURO** na podstawie ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.)

Zatwierdzam SWZ wraz z załącznikami

Z upoważnienia Dyrektora
Uniwersyteckiego Centrum Klinicznego im. prof. K. Gibińskiego
Śląskiego Uniwersytetu Medycznego w Katowicach

mgr Karina Madej
Kierownik Działu Zamówień Publicznych

Katowice, dn. 10.05.2021 r.

I. Zamawiający:

Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego

Śląskiego Uniwersytetu Medycznego w Katowicach

40-514 Katowice, ul. Ceglana 35

NIP: 954-22-74-017 Regon: 001325767

Tel. 32/3581200 lub 32/358-14-42

Adres strony www: <https://www.uck.katowice.pl>

e-mail: bzp@uck.katowice.pl lub ekamzela@uck.katowice.pl

II. TRYB UDZIELENIA ZAMÓWIENIA:

1. Postępowanie o udzielenie zamówienia prowadzone jest w trybie przetargu nieograniczonego na podstawie ustawy z dnia 11 września 2019 roku Prawo Zamówień Publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm. – dalej w treści Pzp).
2. **Zamawiający, zgodnie z art.139 ust.1 dokona najpierw badania i oceny ofert, a następnie dokona kwalifikacji podmiotowej wykonawcy, którego oferta zostanie najwyższej oceniona, w zakresie braku podstaw wykluczenia oraz spełniania warunków udziału w postępowaniu.**
3. Postępowanie prowadzone jest w języku polskim w formie elektronicznej a komunikacja między Zamawiającym a Wykonawcami odbywać się będzie za pośrednictwem Platformy SmartPZP dostępnej pod adresem <https://portal.smartpzp.pl/uck> oraz za pośrednictwem poczty elektronicznej bzp@uck.katowice.pl lub ekamzela@uck.katowice.pl w zależności od rodzaju dokumentów tj. przekazanie ofert następuje za pośrednictwem Platformy; w pozostałych przypadkach komunikacja może odbywać się za pośrednictwem w/w Platformy lub za pomocą poczty elektronicznej e-mail: bzp@uck.katowice.pl lub ekamzela@uck.katowice.pl.
4. Szczegółowa instrukcja użytkownika Wykonawcy SmartPZP dostępna jest na stronie Platformy <https://portal.smartpzp.pl/uck/elearning>. Szczegółowe informacje o sposobie pozyskania usługi kwalifikowanego podpisu elektronicznego oraz warunkach jej użycia można znaleźć na stronach internetowych kwalifikowanych dostawców usług zaufania, których lista znajduje się pod adresem internetowym: <http://www.nccert.pl/kontakt.htm>
5. Informacje dotyczące zmiany i wyjaśnienia treści specyfikacji warunków zamówienia oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem udostępniane będą na stronie prowadzonego postępowania pod adresem: <https://portal.smartpzp.pl/uck> oraz dodatkowo <https://www.uck.katowice.pl/>
6. Szczegółowo informacje dotyczące wymogów komunikacji elektronicznej (w tym dotyczące wymagań w zakresie użytkowania Platformy) zostały wskazane w Rozdziale VIII SWZ.

III. OPIS PRZEDMIOTU ZAMÓWIENIA

1. Przedmiotem zamówienia jest **Dostawa systemu zabezpieczeń klasy UTM**, którego wyszczególnienie ilościowe i asortymentowe określono w formularzu ofertowym stanowiącym załącznik nr 1 do specyfikacji warunków zamówienia (dalej w treści: SWZ). Szczegółowe parametry przedmiotu zamówienia określono w Opisie Przedmiotu Zamówienia stanowiącym załącznik nr 6 do SWZ. Wykonawca zobowiązany jest m. in. dostarczyć, zainstalować i uruchomić Sprzęt oraz przeprowadzić instruktaż wskazanych pracowników Zamawiającego.
3. Nazwa i kod według Wspólnego Słownika Zamówień (CPV):
32420000-3 Urządzenia sieciowe
72611000-6 Usługi w zakresie wsparcia technicznego

72700000-7 Usługi w zakresie sieci komputerowej

4. Zamawiający nie wymaga wniesienia wadium.
5. Zamawiający nie dopuszcza składania ofert częściowych (przedmiot zamówienia jest udzielany w częściach).
6. Przedmiot zamówienia jest dofinansowany w ramach projektu: „Śląska Cyfrowa Platforma Medyczna eCareMed - Telemedycyna i eksploracja danych medycznych (wraz z zadaniem pn. włączenie usług teleonkologii Uniwersyteckiego Centrum Klinicznego do Śląskiej Cyfrowej Platformy Medycznej eCareMed oraz z zadaniem pn. włączenie telekardiologii i teleneurologii Górnośląskiego Centrum Medycznego im. Prof. L. Gieca do Śląskiej Cyfrowej Platformy Medycznej eCareMed)” UDA-RPSL.02.01.00-24-0201/18-00

IV. INFORMACJA O PRZEDMIOTOWYCH ŚRODKACH DOWODOWYCH

1. **Na potwierdzenie, że oferowany przedmiot zamówienia spełnia określone przez zamawiającego wymagania wykonawca do oferty** zobowiązany jest dołączyć:
 - a) dokumentację techniczną oferowanego przedmiotu zamówienia lub inny dokument lub oświadczenie producenta lub oświadczenie autoryzowanego serwisu producenta - w języku polskim lub angielskim potwierdzające parametry techniczne opisane w tabeli 4 Opisu Przedmiotu Zamówienia (dalej w treści OPZ – załącznik nr 6 do SWZ) w zakresie wskazanym w tabeli nr 4 w OPZ
2. Jeżeli Wykonawca nie złoży przedmiotowych środków dowodowych lub złożone przedmiotowe środki dowodowe będą niekompletne, Zamawiający wezwie do ich złożenia lub uzupełnienia w wyznaczonym terminie. W/w postanowień nie stosuje się, jeżeli przedmiotowy środek dowodowy służy potwierdzaniu zgodności z cechami lub kryteriami określonymi w opisie kryteriów oceny ofert lub, pomimo złożenia przedmiotowego środka dowodowego, oferta podlega odrzuceniu albo zachodzą przesłanki unieważnienia postępowania.

V. TERMIN WYKONANIA ZAMÓWIENIA:

Realizacja zamówienia: do 60 dni kalendarzowych od dnia zawarcia umowy.

VI. WARUNKI UDZIAŁU W POSTĘPOWANIU ORAZ PODSTAWY WYKLUCZENIA

1. O udzielenie zamówienia mogą ubiegać się Wykonawcy, którzy:
 - 1) **spełniają warunki udziału w postępowaniu:**

Zamawiający nie stawia warunku w powyższym zakresie.
 - 2) **nie podlegają wykluczeniu;**

Zamawiający wykluczy z postępowania o udzielenie zamówienia publicznego Wykonawcę wobec którego zaistnieją przesłanki do wykluczenia, o których mowa w art.108 ust. 1 Pzp. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust.1 pkt 1,2 i 5 PZP jeżeli udowodni zamawiającemu, że spełnił łącznie przesłanki określone w art. 110 ust.2 PZP. Wykluczenie wykonawcy nastąpi zgodnie z art. 111 ustawy Pzp.
2. Zamawiający nie przewiduje wykluczenia wykonawcy z udziału w niniejszym postępowaniu w oparciu o przesłanki wynikające z art. 109 ust.1 Pzp.

VII. WYKAZ PODMIOTOWYCH ŚRODKÓW DOWODOWYCH

1. Wykonawca zobowiązany jest złożyć Oświadczenie o niepodleganiu wykluczeniu, spełnianiu warunków udziału w postępowaniu w zakresie wskazanym przez Zamawiającego w

załączniku nr 2 do SWZ. Zamawiający działając w trybie art. 139 ust 2 UPZP przewiduje możliwość żądania JEDZ wyłącznie od wykonawcy, którego oferta zostanie najwyżej oceniona.

2. Oświadczenie, o którym mowa w pkt.1, składa się na formularzu jednolitego europejskiego dokumentu zamówienia (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). Sposób przekazania oświadczenia wskazano w punkcie XI.5 SWZ.
3. W przypadku wspólnego ubiegania się o zamówienie przez wykonawców jednolity dokument JEDZ składa każdy z wykonawców wspólnie ubiegających się o zamówienie. Oświadczenia te mają potwierdzać brak podstaw wykluczenia oraz spełnianie warunków udziału w postępowaniu w zakresie, w jakim każdy z wykonawców wykazuje spełnianie warunków udziału w postępowaniu.
4. Zamawiający nie żąda od wykonawcy złożenia jednolitego dokumentu (JEDZ) dotyczącego podwykonawcy, któremu zamierza powierzyć wykonanie części zamówienia.
5. **Zamawiający przed wyborem najkorzystniejszej oferty wezwie Wykonawcę, którego oferta zostanie najwyżej oceniona, do złożenia w wyznaczonym terminie, nie krótszym niż 10 dni, aktualnych na dzień złożenia podmiotowych środków dowodowych.**
 - 1) Oświadczenie w formie jednolitego dokumentu (JEDZ) w zakresie wskazanym w załączniku nr 2 do SWZ - oświadczenie wykonawcy tymczasowo zastępujące wymagane przez zamawiającego podmiotowe środki dowodowe stanowiące dowód potwierdzający brak podstaw wykluczenia, spełniania warunków udziału w postępowaniu, odpowiednio na dzień składania ofert w formie jednolitego dokumentu (JEDZ) w zakresie wskazanym w załączniku nr 2 do SWZ
 - 2) Informacji z Krajowego Rejestru Karnego w zakresie określonym w art. 108 ust. 1 pkt 1,2 i 4 ustawy PZP, wystawiona nie wcześniej niż 6 miesięcy przed jej złożeniem.
 - 3) Oświadczenia wykonawcy w zakresie określonym w art. 108 ust.1 pkt 5 ustawy Pzp o braku przynależności do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 roku o ochronie konkurencji i konsumentów (Dz.U. z 2021r. poz. 275) z innym Wykonawcą, który złożył odrębną ofertę w postępowaniu, albo oświadczenie o przynależności do tej samej grupy kapitałowej wraz z dokumentami lub informacjami potwierdzającymi przygotowanie oferty niezależnie od innego Wykonawcy należącego do tej samej grupy kapitałowej. Oświadczenie Wykonawca może sporządzić zgodnie ze wzorem stanowiącym załącznik nr 3 do SWZ.
 - 4) Oświadczenia Wykonawcy o aktualności informacji zawartych w oświadczeniu JEDZ, w zakresie podstaw wykluczenia z postępowania na podstawie art. 108 ust.1 pkt. 3-6 ustawy Pzp). Oświadczenie Wykonawca może sporządzić zgodnie ze wzorem stanowiącym załącznik nr 4 do SWZ.
6. Jeżeli wykonawca ma siedzibę lub miejsce zamieszkania poza granicami Rzeczypospolitej Polskiej, zamiast dokumentów, o których mowa w punkcie VII.5.2) SWZ składa informację z odpowiedniego rejestru, takiego jak rejestr sądowy, albo, w przypadku braku takiego rejestru, inny równoważny dokument wydany przez właściwy organ sądowy lub administracyjny kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania - wystawiony nie wcześniej niż 6 miesięcy przed jego złożeniem.
7. Jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania, nie wydaje się dokumentów, o których mowa w pkt 6 lub gdy dokumenty te nie odnoszą się do wszystkich przypadków, o których mowa w art. 108 ust. 1 pkt 1, 2 i 4 Pzp, zastępuje się je odpowiednio

- w całości lub w części dokumentem zawierającym odpowiednio oświadczenie wykonawcy, ze wskazaniem osoby albo osób uprawnionych do jego reprezentacji, lub oświadczenie osoby, której dokument miał dotyczyć, złożone pod przysięgą, lub, jeżeli w kraju, w którym wykonawca ma siedzibę lub miejsce zamieszkania nie ma przepisów o oświadczeniu pod przysięgą, złożone przed organem sądowym lub administracyjnym, notariuszem, organem samorządu zawodowego lub gospodarczego, właściwym ze względu na siedzibę lub miejsce zamieszkania wykonawcy - wystawionym nie wcześniej niż 6 miesięcy przed jego złożeniem
8. Jeżeli wykonawca niełoży oświadczenia, o którym mowa w art.125.ust.1 Pzp, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu lub są one niekompletne lub zawierają błędy, zamawiający wezwie Wykonawcę odpowiednio do ich złożenia ,poprawienia lub uzupełnienia w terminie przez siebie wyznaczonych, chyba że mimo ich złożenia, uzupełnienia lub poprawienia oferta wykonawcy podlega odrzuceniu lub zachodzą przesłanki unieważnienia postępowania.
 9. Zamawiający nie wezwie do złożenia podmiotowych środków dowodowych, jeżeli: może je uzyskać za pomocą bezpłatnych i ogólnodostępnych baz danych, w szczególności rejestrów publicznych w rozumieniu ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, o ile wykonawca wskaże w jednolitym dokumencie dane umożliwiające dostęp do tych środków;
 10. Wykonawca nie jest zobowiązany do złożenia podmiotowych środków dowodowych, które zamawiający posiada, jeżeli wykonawca wskaże te środki oraz potwierdzi ich prawidłowość i aktualność.
 11. W zakresie nieuregulowanym SWZ, zastosowanie mają przepisy Rozporządzenia Ministra Rozwoju Pracy i Technologii z dnia 23 grudnia 2020 roku w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń jakich może żądać zamawiający od wykonawcy (Dz.U z 2020 poz 2415 z późn. zm.) oraz rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 roku w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 poz. 2452 z późn. zm.).

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

1. W postępowaniu komunikacja między zamawiającym a wykonawcami prowadzona jest w języku polskim w formie elektronicznej zgodnie z art. 61 ustawy Pzp.
 - a) przekazanie ofert, oświadczeń o których mowa w art. 125 ust.1 PZP w tym jednolitego europejskiego dokumentu zamówienia następuje za pośrednictwem Platformy SmartPZP dostępnej pod adresem <https://portal.smartpzp.pl/uick>. Za datę wpływu dokumentów na Platformę przyjmuje się datę zapisania na serwerach. Aktualna data i godzina, zsynchronizowane z Głównym Urzędem Miar, wyświetlane są w prawym górnym rogu otwartego okna aplikacji Platformy.
 - b) w pozostałych przypadkach wymiana informacji, przekazywanie dokumentów lub oświadczeń może odbywać się za pośrednictwem Platformy SmartPZP lub za pośrednictwem poczty elektronicznej e-mail: bzp@uick.katowice.pl lub ekamzela@uick.katowice.pl
 - c) Za datę i godzinę wpływu w przypadku poczty elektronicznej przyjmuje się datę wpływu na serwerze pocztowym Zamawiającego.

2. Szczegółowa instrukcja użytkownika Wykonawcy SmartPZP dostępna jest na stronie Platformy <https://portal.smartpzp.pl/uck/elearning>
3. Do pełnego i prawidłowego korzystania z Systemu przez Użytkowników Zewnętrznych konieczne jest posiadanie przez co najmniej jednego uprawnionego Użytkownika Zewnętrznego Wykonawcy elektronicznego podpisu kwalifikowanego służącego do autentykacji i podpisu.
4. Korzystanie z Systemu możliwe jest na 2 sposoby, pod warunkiem spełnienia następujących minimalnych wymagań technicznych:
 - a) Oprogramowanie zewnętrzne (dostawcy podpisu kwalifikowanego)
 - Mozilla Firefox ver. 65 i późniejsze, Google Chrome ver. 66 i późniejsze lub Opera ver. 58 i późniejsze, Microsoft Edge ver 18 i późniejsze, Internet Explorer 11
 - Lista zalecanych przeglądarek internetowych: Google Chrome, Mozilla Firefox, Opera. Zalecane jest używanie najnowszych wersji przeglądarek
 - system operacyjny Windows 7 i późniejsze
 - b) Oprogramowanie wbudowane w SmartPZP
 - zainstalowane środowisko Java w wersji min. 1.8 (jre)
 - w przypadku przeglądarek Opera, Chrome i Firefox należy doinstalować dodatek do przeglądarki Szafir SDK Web
 - oprogramowanie SzafirHost w systemie operacyjnym.
5. Użycie przez Wykonawcę do kontaktu z Zamawiającym środków komunikacji elektronicznej zapewnionych w Systemie jest uzależnione od uprzedniej akceptacji przez Wykonawcę Regulaminu korzystania z usług Systemu na witrynie internetowej przy zakładaniu profilu Wykonawcy.
6. Korzystanie z Systemu przez Wykonawców jest bezpłatne.
7. Użytkownikom Zewnętrznym Wykonawcy przysługuje prawo korzystania z asysty obejmującej wsparcie techniczne w kwestiach dotyczących korzystania z Systemu, polegające na doradztwie telefonicznym i e-mailowym na zasadach określonych w Regulaminie korzystania z usług Systemu
8. Maksymalny rozmiar pojedynczych plików przesyłanych za pośrednictwem Systemu wynosi 100 MB. Za pośrednictwem Systemu można przesłać wiele pojedynczych plików lub plik skompresowany do archiwum (ZIP) zawierający wiele pojedynczych plików.
9. Sposób sporządzenia podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń musi być zgodny z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie oraz w rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać zamawiający od wykonawcy. Zamawiający preferuje przysyłanie dokumentów w formacie pdf, ale dopuszcza w szczególności następujące formaty przesyłanych danych: .pdf, .doc, .docx, .rtf, .odt., .txt, .xls, .xlsx,
10. W zależności od formatu kwalifikowanego podpisu (np. PAdES, XAdES) i jego typu (zewnętrzny, wewnętrzny) Wykonawca dołącza do platformy SmartPZP uprzednio podpisane dokumenty wraz z wygenerowanym plikiem podpisu (typ zewnętrzny) lub dokument z wszytym podpisem (typ wewnętrzny):
11. Podpis elektroniczny musi być wystawiony przez dostawcę kwalifikowanej usługi zaufania, będącego podmiotem świadczącym usługi certyfikacyjne – podpis elektroniczny, spełniający wymogi bezpieczeństwa określone w ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.

12. Format przesyłanych danych winien być zgodny z Ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne oraz z Rozporządzeniem Rady Ministrów z dnia 12 kwietnia 2012r w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych
13. Jeżeli Zamawiający lub Wykonawca przekazują oświadczenia, wnioski, zawiadomienia oraz informacje za pośrednictwem środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną, każda ze stron na żądanie drugiej strony niezwłocznie potwierdza fakt ich otrzymania.
14. Wykonawca może zwrócić się do Zamawiającego z wnioskiem o wyjaśnienie treści SWZ. Zamawiający jest obowiązany udzielić wyjaśnień niezwłocznie, jednak nie później niż na 6 dni przed upływem terminu składania ofert, pod warunkiem, że wniosek o wyjaśnienie treści SWZ wpłynie do Zamawiającego nie później niż na 14 dni przed upływem terminu składania ofert.
15. Jeżeli Zamawiający nie udzieli wyjaśnień w terminie o którym mowa w pkt. 14, przedłuży termin składania ofert o czas niezbędny do zapoznania się wszystkich zainteresowanych wykonawców z wyjaśnieniami niezbędnymi do należytego przygotowania i złożenia oferty. Przedłużenie terminu składania ofert nie wpływa na bieg terminu składania wniosku o wyjaśnienie treści SWZ.
16. W przypadku gdy wniosek o wyjaśnienie treści SWZ nie wpłynie w terminie o którym mowa w pkt. 14, Zamawiający nie ma obowiązku udzielenia wyjaśnień SWZ oraz obowiązku przedłużenia terminu składania ofert.
17. W uzasadnionych przypadkach Zamawiający może przed upływem terminu składania ofert zmienić treść SWZ. Dokonaną zmianę treści SWZ Zamawiający udostępni na stronie internetowej prowadzonego postępowania.

IX. OSOBY UPRAWNIONE DO KOMUNIKOWANIA SIĘ WYKONAWCAMI

1. Osobą uprawnioną do porozumiewania się z wykonawcami jest Ewa Kamzela e-mail: bzp@uck.katowice.pl lub ekamzela@uck.katowice.pl tel. 32 358 14 45 w dni robocze (tj. od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy) w godzinach 7.00 – 14.35.

X. TERMIN ZWIĄZANIA OFERTĄ

1. Wykonawca jest związany ofertą do dnia **12.09.2021 r.**
Pierwszym dniem terminu związania ofertą jest dzień, w którym upływa termin składania ofert.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania ofertą, o którym mowa w pkt. 1 zamawiający przed upływem terminu związania ofertą, zwróci się jednokrotnie do wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 60 dni.
3. Przedłużenie terminu związania ofertą, o którym mowa w pkt. 2, wymaga złożenia przez wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

XI. OPIS SPOSOBU PRZYGOTOWYWANIA OFERTY

1. Ofertę oraz oświadczenie, o którym mowa w art. 125 ust.1 ustawy Pzp (JEDZ) składa się pod rygorem nieważności w formie elektronicznej.
2. Wykonawca ponosi wszelkie koszty przygotowania i złożenia oferty.
3. Każdy wykonawca może złożyć tylko jedną ofertę.

4. **Zamawiający wymaga, złożenia oferty zawierającej następujące dokumenty:**

- 1) formularz ofertowy według druku stanowiącego załącznik nr 1 do SWZ,
- 2) przedmiotowe środki dowodowe wskazane w punkcie IV.1 SWZ
- 3) w przypadku podpisania oferty przez osobę niewymienioną w dokumencie rejestracyjnym (ewidencyjnym) Wykonawcy, pełnomocnictwo w formie oryginału podpisanego przez osobę uprawnioną ze strony Wykonawcy kwalifikowanym podpisem elektronicznym lub kopii elektronicznej opatrzonej kwalifikowanym podpisem elektronicznym notariusza.

5. **Sposób przygotowania oświadczenia JEDZ:**

Wykonawca wypełnia JEDZ, tworząc dokument elektroniczny. Może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu elektronicznego. Zamawiający może skorzystać z podanej instrukcji :

a. Instrukcja wypełniania JEDZ:

- a) Ściągnąć ze strony Zamawiającego i zapisać na swoim komputerze plik „JEDZ w formacie xml”.
- b) Wejść na stronę <https://espd.uzp.gov.pl/> lub Urzędu Zamówień Publicznych (gdzie znajduje się instrukcja elektronicznego narzędzia do wypełniania JEDZ/ESPD /eESPD/:
<https://www.uzp.gov.pl/baza-wiedzy/prawo-zamowien-publicznych-regulacje/prawo-krajowe/jednolity-europejski-dokument-zamowienia>
Zaznaczyć opcje „jestem wykonawcą” i chcę „zaimportować ESPD”.
- c) Następnie wybrać ikonkę „przeglądaj” i zaimportować ściągnięty uprzednio plik „JEDZ w formacie xml”
- d) Zaznaczyć odpowiedź na pytanie „Gdzie znajduje się siedziba Państwa przedsiębiorstwa” - menu rozwijane
- e) Nacisnąć przycisk „DALEJ”
- f) Otworzy się edytowalna wersja JEDZ, którą należy wypełnić.
UWAGA: w części „Informacje na temat postępowania o udzielenie zamówienia” w polu „Rodzaj procedury” należy zaznaczyć „Procedura otwarta” - menu rozwijane.
- g) Wypełnić JEDZ z zastrzeżeniem, iż w części IV: Kryteria kwalifikacji – ogólne oświadczenie dotyczące wszystkich kryteriów kwalifikacji – wypełnić w wersji skróconej tj. jedynie część α tzn. Tak/Nie w sytuacji, gdy Zamawiający stawia wymogi dotyczące warunków udziału, o których mowa w punkcie VI.1.2) SWZ.
- h) Wykonawca wypełnia JEDZ, tworząc dokument elektroniczny. Może korzystać z narzędzia ESPD lub innych dostępnych narzędzi lub oprogramowania, które umożliwiają wypełnienie JEDZ i utworzenie dokumentu elektronicznego, w szczególności w jednym z ww. formatów.

5. Dla wykonawców występujących wspólnie ma w szczególności zastosowanie art. 58 Prawa zamówień publicznych. Wykonawcy wspólnie ubiegający się o udzielenie zamówienia zobowiązani są do ustanowienia pełnomocnika do reprezentowania ich w postępowaniu o udzielenie zamówienia albo reprezentowania ich w postępowaniu i zawarcia umowy w sprawie zamówienia publicznego. Pełnomocnictwo należy złożyć wraz z ofertą.

6. Zamawiający informuje, iż zgodnie z art. 18 w zw. z art. 74 ustawy PZP oferty wraz z załącznikami składane w postępowaniu o zamówienie publiczne są jawne i udostępnia się niezwłocznie po otwarciu ofert, z wyjątkiem informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów ustawy z dnia 16 kwietnia 1993 r. o zwalczaniu

nieuczciwej konkurencji, jeśli 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 Pzp.

7. Zamawiający nie ujawni informacji stanowiących tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, jeżeli Wykonawca, nie później niż w terminie składania ofert zastrzeże, że nie mogą być one udostępniane oraz wykaże, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa. Przez tajemnicę przedsiębiorstwa rozumie się informacje techniczne, technologiczne, organizacyjne przedsiębiorstwa lub inne informacje posiadające wartość gospodarczą, które jako całość lub w szczególnym zestawieniu i zbiorze ich elementów nie są powszechnie znane osobom zwykle zajmującym się tym rodzajem informacji albo nie są łatwo dostępne dla takich osób, o ile uprawniony do korzystania z informacji lub rozporządzania nimi podjął, przy zachowaniu należytej staranności, działania w celu utrzymania ich w poufności. Wykonawca w celu utrzymania w poufności tych informacji „przekazuje je w wydzielonym i odpowiednio oznaczonym pliku.
8. Oferty składane w formie elektronicznej - podczas załączania przez Wykonawcę plików, wymagane jest odpowiednie oznaczenia statusu takiego dokumentu w kolumnie oznaczonej „Jawny”. Ustawieniem domyślnym jest jawność załączonego pliku, aby oznaczyć plik jako zawierający tajemnicę przedsiębiorstwa należy oznaczyć checkbox ☐. W przypadku, gdy dany dokument tylko w części zawiera tajemnicę przedsiębiorstwa, Wykonawca powinien podzielić ten dokument na dwa pliki i dla każdego z nich odpowiednio oznaczyć status jawności (część jawna bez zaznaczonego checkboxa ☐ część zawierająca informacje stanowiące tajemnicę przedsiębiorstwa z zaznaczonym checkboxem ☒). W celu wykazania, iż zastrzeżone informacje stanowią tajemnicę przedsiębiorstwa należy załączyć do oferty w formie odrębnego pliku wyjaśnienia lub inne dokumenty potwierdzające iż dane informacje stanowią tajemnicę przedsiębiorstwa.
9. Zgodnie z Rozporządzeniem Ministra Rozwoju Pracy i Technologii z dnia 18 grudnia 2020 r. w sprawie protokołów postępowania oraz dokumentacji postępowania o udzielenie zamówienia publicznego (Dz.U. 2020 r. poz. 2434 z późn. zm.) Zamawiający udostępnia protokół lub załączniki do protokołu na wniosek. Udostępnianie protokołu postępowania lub załączników do protokołu postępowania następuje przy użyciu środków komunikacji elektronicznej.
10. Podmiotowe środki dowodowe oraz inne dokumenty lub oświadczenia, sporządzone w języku obcym przekazuje się wraz z tłumaczeniem na język polski. **Zamawiający dopuszcza złożenie przedmiotowych środków dowodowych wskazanych w punkcie IV.1 SWZ w języku angielskim.**
11. Dokumenty inne niż oświadczenia, składane w celu potwierdzenia spełniania warunków udziału w postępowaniu i braku podstaw wykluczenia określone w pkt. VII.5 powinny zostać złożone w następujący sposób:
 - a) w sytuacji gdy zostały wytworzone jako dokument elektroniczny - przekazuje się ten dokument;
 - b) w sytuacji gdy zostały wytworzone jako dokument w postaci papierowej, przekazuje się cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, poświadczające zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej. Z zastrzeżeniem treści § 6 Rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków

komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie,

- c) poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej dokonuje w przypadku:
- podmiotowych środków dowodowych – odpowiednio wykonawca, wykonawca wspólnie ubiegający się o udzielenie zamówienia, podwykonawca, w zakresie podmiotowych środków dowodowych, które każdego z nich dotyczą;
 - przedmiotowego środka dowodowego, dokumentu, o którym mowa w art. 94 ust. 2 ustawy, oświadczenia, o którym mowa w art. 117 ust. 4 ustawy PZP, lub zobowiązania podmiotu udostępniającego zasoby – odpowiednio wykonawca lub wykonawca wspólnie ubiegający się o udzielenie zamówienia;
 - pełnomocnictwa – mocodawca.

12. Poświadczenia zgodności cyfrowego odwzorowania z dokumentem w postaci papierowej, może dokonać również notariusz.

XII. SPOSÓB ORAZ TERMIN SKŁADANIA OFERT

1. Termin składania ofert upływa w dniu **15.06.2021** o godz.10.00.
2. Ofertę wraz ze wszystkimi wymaganymi oświadczeniami i dokumentami, należy przesłać za pośrednictwem Platformy elektronicznej dostępnej pod adresem: <https://portal.smartpzp.pl/uck>.
3. Wykonawca celem złożenia oferty rejestruje się na Platformie pod adresem: <https://portal.smartpzp.pl/uck> klikając przycisk „Załącz konto”. Do założenia konta wymagany jest certyfikat kwalifikowany.
4. Szczegółowe informacje dot. sposobu wykonania tych czynności znajdują się w „Instrukcja obsługi Portalu e-Usług SmartPZP”, dostępnej na stronie Platformy pod adresem <https://portal.smartpzp.pl/uck/elearning>
5. Wykonawca ma możliwość złożenia oferty korzystając z zakładki Oferty dostępnej na Platformie. Aby to zrobić należy kliknąć na przycisk „Złóż ofertę”, który znajduje się w prawym dolnym rogu strony aplikacji. Po kliknięciu „Złóż ofertę” Wykonawca zostanie przeniesiony na stronę składania oferty, na której widnieją zakładki:
 - Dane ogólne – zawiera dane Wykonawcy wprowadzone podczas rejestracji.
 - Wykonawcy – w tym miejscu istnieje możliwość wprowadzenia danych innego wykonawcy w przypadku występowania w danym postępowaniu więcej niż jednego wykonawcy. W tym celu należy zaznaczyć checkbox ☐ „Wykonawcy występujący wspólnie”, a następnie wypełnić dane podmiotu. Wykonawca może dodać załączniki do składanej oferty w miejscu „Załączniki”. Aby dodać załącznik, należy kliknąć przycisk „+ Dodaj plik”, który znajduje się w lewym dolnym rogu strony aplikacji. W tym momencie otworzy się okno dodawania pliku. Należy wówczas kliknąć przycisk „+ Wybierz”, wybrać plik z dysku komputera a następnie potwierdzić dodanie pliku przyciskiem „Dodaj do oferty”. W chwili dodawania pliku, Wykonawca ma możliwość zaznaczenia checkboxów ☐ dotyczących jawności oraz danych osobowych. Po dodaniu załączników ofertę można wysłać. Aby wysłać ofertę należy kliknąć przycisk „Wyślij ofertę”, który otworzy okno z podsumowaniem oraz przycisk „☐ Podpisz”. Po kliknięciu przycisku „☐ Podpisz”, powinna uruchomić się aplikacja do kwalifikowanego podpisu elektronicznego, która pozwoli nam podpisać kwalifikowanym podpisem czynność wysłania oferty analogicznie jak w przypadku podpisywania czynności rejestracji konta Wykonawcy.
6. Po prawidłowym złożeniu podpisu, pojawi się okno z raportem z podpisywania/szyfrowania dokumentów. W tym momencie oferta została prawidłowo złożona w danym postępowaniu.

7. Przed terminem składania ofert wykonawca ma możliwość wycofania bądź zmiany oferty (poprzez jej wycofanie oraz złożenie nowej oferty – z uwagi na zaszyfrowaną ofertę brak możliwości edycji złożonej oferty). Wykonawca loguje się na stronę <https://portal.smartpzp.pl/uck>, wyszukuje dane postępowanie a następnie po przejściu do zakładki „Oferta”, wycofuje ją przy pomocy przycisku „Wycofaj ofertę”. Szczegółowe informacje dot. Sposobu wykonania tych czynności znajdują się w „Instrukcji obsługi Portalu e-Usług SmartPZP”, dostępnej na stronie Platformy pod adresem <https://portal.smartpzp.pl/uck/elearning>
8. Zaleca się nazwanie poszczególnych plików dokumentów składanych na Platformie Smartpzp w sposób umożliwiający ich identyfikację: np. formularz ofertowy, formularz cenowy, JEDZ itp.

XIII. TERMIN OTWARCIA OFERT

1. Otwarcie ofert nastąpi w dniu **15.06.2021 r.** o godz. 10.30 poprzez ich odszyfrowanie na Platformie Smartpzp.
2. W przypadku awarii tego systemu, która powoduje brak możliwości otwarcia ofert w terminie określonym przez zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
3. Zamawiający poinformuje o zmianie terminu otwarcia ofert na stronie internetowej prowadzonego postępowania.
4. Zamawiający, najpóźniej przed otwarciem ofert, udostępni na stronie internetowej prowadzonego postępowania informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
5. Zamawiający, niezwłocznie po otwarciu ofert, udostępni 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.

XIV. OPIS SPOSOBU OBLICZENIA CENY

1. Wykonawca w przedstawionej ofercie winien zaoferować cenę ryczałtową, kompletną, jednoznaczną, która będzie ceną ostateczną.
2. Cena brutto oferty musi uwzględniać wszystkie wymagania niniejszej specyfikacji warunków zamówienia tj. obejmować wszelkie koszty, jakie poniesie Wykonawca z tytułu należytej oraz zgodnej z obowiązującymi przepisami realizacji przedmiotu zamówienia w tym: cena brutto oferty powinna zawierać wszystkie koszty związane z dostawą przedmiotu zamówienia do Zamawiającego w szczególności: transport, opakowanie, czynności związane z przygotowaniem dostawy, dostarczenie, instruktaż personelu, uruchomieniem, instalacje, montaż, gwarancję, przeglądy okresowe w okresie gwarancji itp. Wykonawca winien uwzględnić w cenie oferty również wszystkie inne koszty jakie poniesie w związku z realizacją przedmiotu przetargu, także nie wymienione w zdaniu poprzedzającym, a które mają wpływ na cenę oferty.
3. Cena ma być wyrażona w złotych polskich. Rozliczenia między Zamawiającym a Wykonawcą prowadzone będą w złotych polskich.
4. Ceny jednostkowe netto oraz wartości netto i brutto należy podać z dokładnością do dwóch miejsc po przecinku.
5. Stawka podatku VAT jest określana zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług.
6. Jeżeli Wykonawca stosuje w swojej praktyce kupieckiej upusty cenowe, to proponując je Zamawiającemu w ofercie, musi już uwzględnić je w ostatecznej cenie oferty.

7. Przyjęte przez Wykonawcę w ofercie ceny i stawki w złotych polskich nie będą podlegać waloryzacji w trakcie realizacji przedmiotu zamówienia z zastrzeżeniem przypadków, o których mowa w umowie i UPZP.
8. Wykonawca określa cenę realizacji zamówienia poprzez wypełnienie stosownej tabelki w formularzu ofertowym stanowiącym załącznik nr 1 do SWZ.
9. W formularzu ofertowym w pozycji VAT (%) dopuszcza się wpisanie zamiennie liczbowej lub procentowej wartości stawki podatku VAT.
10. Zamawiający dopuszcza, aby Wykonawca w formularzu ofertowym rozbił tabelkę na poszczególne pozycje np. w celu wskazania odrębnej stawki VAT itp.
11. Jeżeli w postępowaniu złożona będzie oferta, której wybór prowadziłby do powstania u zamawiającego obowiązku podatkowego zgodnie z ustawą z dnia 11 marca 2004 r. o podatku od towarów i usług, dla celów zastosowania kryterium ceny zamawiający doliczy do przedstawionej w tej ofercie ceny kwotę podatku od towarów i usług, którą miałyby obowiązek rozliczyć. W takim przypadku Wykonawca ma obowiązek wraz ze złożoną ofertą :
 - a) poinformowania zamawiającego, że wybór jego oferty będzie prowadził do powstania u zamawiającego obowiązku podatkowego;
 - b) wskazania nazwy (rodzaju) towaru lub usługi, których dostawa lub świadczenie będą prowadziły do powstania obowiązku podatkowego;
 - c) wskazania wartości towaru lub usługi objętego obowiązkiem podatkowym zamawiającego, bez kwoty podatku;
 - d) wskazania stawki podatku od towarów i usług, która zgodnie z wiedzą wykonawcy, będzie miała zastosowanie.

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

15.1. Przy wyborze oferty Zamawiający będzie się kierował następującymi kryteriami oceny ofert:

- | | |
|---|--------|
| 1) Cena | – 60 % |
| 2) Okres wsparcia gwarancyjnego | – 10 % |
| 3) Czas usunięcia awarii w okresie wsparcia gwarancyjnego | – 10 % |
| 4) Dodatkowe wsparcie techniczne producenta w okresie wsparcia gwarancyjnego | – 10 % |
| 5) Czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego | – 10 % |

Sposób obliczania punktów dla poszczególnych kryteriów:

Ad. 1 kryterium Cena (C) – waga 60%

W ramach kryterium „Cena” ocena ofert zostanie dokonana przy zastosowaniu wzoru:

$$C = \frac{C_n}{C_o} \times 100 \times 60 \%$$

gdzie:

C – liczba punktów w ramach kryterium „Cena”,

C_n - najniższa cena spośród ofert ocenianych

C_o - cena oferty ocenianej

Ocenie w ramach kryterium „Cena” podlegać będzie cena łączna brutto za wykonanie całego przedmiotu zamówienia podana w formularzu ofertowym.

W tym kryterium wykonawca może uzyskać maksymalnie 60 punktów.

Ad.2 kryterium okres wsparcia gwarancyjnego (G) – waga 10 %

<u>okres wsparcia gwarancyjnego</u>	Liczba punktów
36 miesięcy i więcej	10
24 miesiące	0

Sposób obliczenia punktów dla w/w kryterium:

- Kryterium okres wsparcia gwarancyjnego będzie rozpatrywane na podstawie okresu zadeklarowanego w formularzu ofertowym.
- Minimalny okres wsparcia gwarancji to 24 miesiące.
- Maksymalna liczba punktów jaką można uzyskać w tym kryterium to 10 punktów.

W przypadku nie wypełnienia w formularzu ofertowym stosownej rubryki zamawiający uzna, że wykonawca deklaruje 24 miesięczny okres wsparcia gwarancyjnego. Wykonawca może zaoferować okres dłuższy niż 36 miesięcy.

Ad. 3 kryterium czas usunięcia awarii w okresie wsparcia gwarancyjnego (CA) – waga 10%

<u>czas usunięcia awarii</u>	Liczba punktów
do 4 godzin roboczych	10
Powyżej 4 godzin roboczych do 6 godzin roboczych	5
Powyżej 6 godzin roboczych do 8 godzin roboczych	0

Sposób obliczenia punktów dla w/w kryterium:

- Kryterium czas usunięcia awarii w okresie wsparcia gwarancyjnego będzie rozpatrywane na podstawie okresu zadeklarowanego w formularzu ofertowym.
- Maksymalny czas to 8 godzin roboczych. (tj. liczonych od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy w godzinach 08:00 do 16:00) od momentu zgłoszenia przez Zamawiającego. Jeżeli wykonawca wpisze czas dłuższy niż maksymalny to przygotuje ofertę niezgodną z SWZ co skutkować będzie odrzuceniem oferty.
- Maksymalna liczba punktów jaką można uzyskać w tym kryterium to 10 punktów.
- W przypadku nie wypełnienia w formularzu ofertowym stosownej rubryki zamawiający uzna, że wykonawca deklaruje czas usunięcia awarii powyżej 6 godzin roboczych do 8 godzin roboczych.

Ad.4 kryterium dodatkowe wsparcie techniczne producenta w okresie wsparcia gwarancyjnego (WG) – waga 10 %

<u>dodatkowe wsparcie techniczne producenta w okresie wsparcia gwarancyjnego</u>	Liczba punktów
W trybie 24 godziny przez 7 dni w tygodniu	10
Co najmniej w godzinach od 8.00 do 16.00 od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy	0

Sposób obliczenia punktów dla w/w kryterium:

- Kryterium dodatkowe wsparcie techniczne producenta w okresie wsparcia gwarancyjnego będzie rozpatrywane na podstawie okresu zadeklarowanego w formularzu ofertowym.
- Minimalny czas to zaoferowanie wsparcia co najmniej w godzinach od 8.00 do 16.00 od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy
- Maksymalna liczba punktów jaką można uzyskać w tym kryterium to 10 punktów.
- W przypadku nie wypełnienia w formularzu ofertowym stosownej rubryki zamawiający uzna, że wykonawca deklaruje wsparcie w godzinach od 8.00 do 16.00 od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy

Ad.5 kryterium czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego (WU) – waga 10 %

<u>czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego</u>	Liczba punktów
do 4 dni roboczych	10
5 – 6 dni roboczych	5
7 dni roboczych	0

Sposób obliczenia punktów dla w/w kryterium:

- Kryterium czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego będzie rozpatrywane na podstawie czasu zadeklarowanego w formularzu ofertowym.
- Maksymalny czas to 7 dni roboczych. (tj. od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy) liczonych od dnia otrzymania przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego.. Jeżeli wykonawca wpisze czas dłuższy niż maksymalny to przygotuje ofertę niezgodną z SWZ co skutkować będzie odrzuceniem oferty.
- W przypadku nie wypełnienia w formularzu ofertowym stosownej rubryki zamawiający uzna, że wykonawca deklaruje maksymalny czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego tj. 7 dni roboczych liczony od dnia otrzymania przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego.
- Maksymalna liczba punktów jaką można uzyskać w tym kryterium to 10 punktów.

13.2. Za najkorzystniejszą ofertę zostanie uznana oferta, która uzyskała łącznie najwyższą liczbę punktów obliczoną wg następującego wzoru:

$$P = C + G + CA + WG + WU$$

gdzie:

- P - łączna liczba punktów jaką uzyskała oceniana oferta
C - liczba punktów przyznanych ocenianej ofercie w ramach kryterium cena
G - liczba punktów przyznanych ocenianej ofercie w ramach kryterium okres wsparcia gwarancyjnego
CA - liczba punktów przyznanych ocenianej ofercie w ramach kryterium czas usunięcia awarii w okresie wsparcia gwarancyjnego
WG - liczba punktów przyznanych ocenianej ofercie w ramach kryterium dodatkowe wsparcie techniczne producenta w okresie wsparcia gwarancyjnego
WU - liczba punktów przyznanych ocenianej ofercie w ramach kryterium czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego

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

1. Jeżeli wybrana oferta została złożona przez wykonawców o których mowa w art. 58 Prawa zamówień publicznych Zamawiający może żądać przed zawarciem umowy w sprawie zamówienia publicznego kopii umowy regulującej współpracę tych wykonawców.
2. Zamawiający zawrze umowę w sprawie zamówienia publicznego w formie pisemnej w postaci papierowej, z zastrzeżeniem art. 264 ust.1 ustawy Pzp, z wybranym wykonawcą w terminie nie krótszym niż 10 dni od dnia przesłania zawiadomienia o wyborze najkorzystniejszej oferty przy użyciu środków komunikacji elektronicznej, na warunkach będących istotnymi postanowieniami, a stanowiącymi wzór umowy – **załącznik nr 5** do niniejszej specyfikacji.
3. Zamawiający może zawrzeć umowę w sprawie zamówienia publicznego przed upływem terminu określonego w pkt. 2 jeżeli w postępowaniu na dany pakiet zostanie złożona tylko jedna oferta.
4. Miejsce i termin podpisania umowy zamawiający wskaże wybranemu w wyniku niniejszego postępowania wykonawcy lub przekaże umowę do podpisu listownie.

XVII. WYMAGANIA DOTYCZĄCE ZABEZPIECZENIA NALEŻYTEGO WYKONANIA UMOWY

Zamawiający przed podpisaniem umowy nie będzie wymagał wniesienia zabezpieczenia należytego wykonania umowy.

XVIII. PROJEKTOWANE POSTANOWIENIA UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO, KTÓRE ZOSTANĄ WPROWADZONE DO UMOWY W SPRAWIE ZAMÓWIENIA PUBLICZNEGO – WZÓR UMOWY

Projektowane postanowienia umowy, które zostaną wprowadzone do treści zawieranej umowy w sprawie zamówienia publicznego stanowią Wzór umowy - **załącznik nr 5** do SWZ.

XIX. POUCZENIE O ŚRODKACH OCHRONY PRAWNEJ PRZYSŁUGUJĄCYCH WYKONAWCY

1. Środki ochrony prawnej przysługują Wykonawcom oraz innemu podmiotowi, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy.

2. Środki ochrony prawnej wobec ogłoszenia wszczynającego postępowanie o udzielenie zamówienia oraz dokumentów zamówienia przysługują również organizacjom wpisanym na listę, o której mowa w art. 469 pkt 15 Pzp, oraz Rzecznikowi Małych i Średnich Przedsiębiorców.
3. Odwołanie przysługuje na:
 - a) niezgodną z przepisami ustawy czynność Zamawiającego, podjętą w postępowaniu o udzielenie zamówienia, w tym na projektowane postanowienie umowy;
 - b) zaniechanie czynności w postępowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy.
4. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej albo w postaci elektronicznej opatrzone podpisem zaufanym.
5. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 PZP, stronom oraz uczestnikom postępowania odwoławczego przysługuje skarga do sądu. Skargę wnosi się do Sądu Okręgowego w Warszawie za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
6. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej” PZP.

XX. POZOSTAŁE REGUŁY POSTĘPOWANIA

1. Zamawiający nie przewiduje udzielenia zamówień o których mowa w art. 214 ust. 1 pkt 8 Prawa zamówień publicznych.
2. Zamawiający nie dopuszcza możliwości składania ofert wariantowych.
3. Zamawiający nie przewiduje przeprowadzenia aukcji elektronicznej, nie ustanawia dynamicznego systemu zakupów oraz nie zamierza zawrzeć umowy ramowej.
4. Do spraw nieuregulowanych w niniejszej specyfikacji warunków zamówienia mają zastosowanie przepisy ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.) oraz Kodeksu cywilnego.
5. 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:
 - a) administratorem uzyskanych w niniejszym postępowaniu danych osobowych jest Uniwersyteckie Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach, 40-514 Katowice, ul. Ceglana 35, Tel. 32 3581200 fax. 32 251-84-37 lub 32/358-14-32, adres strony [www: https://www.uck.katowice.pl](https://www.uck.katowice.pl)
 - b) inspektorem ochrony danych w Uniwersyteckim Centrum Kliniczne im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach jest Pan Patryk Rozumek tel. 32 3581 524, iod@uck.katowice.pl
 - c) uzyskane w niniejszym postępowaniu dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego na **Dostawę systemu zabezpieczeń klasy UTM – DZP.381.15A.2021**
 - d) odbiorcami uzyskanych w niniejszym postępowaniu danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 17 ustawy PZP;
 - e) Uzyskane w niniejszym postępowaniu dane osobowe będą przechowywane, zgodnie z art. 78 ust. 4 ustawy PZP, przez cały okres obowiązywania umowy w sprawie zamówienia publicznego. Okres ten może ulec wydłużeniu o czas niezbędny dla ewentualnego ustalenia, dochodzenia lub obrony przed roszczeniami;

- f) obowiązek podania danych osobowych bezpośrednio dotyczących danej osoby 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;
 - g) w odniesieniu do uzyskanych w postępowaniu danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
 - h) osoba, której dane osobowe dotyczą posiada:
 - na podstawie art. 15 RODO prawo dostępu do danych osobowych jej dotyczących;
 - na podstawie art. 16 RODO prawo do sprostowania danych osobowych jej dotyczących (*Wyjaśnienie: skorzystanie przez osobę, której dane dotyczą, z uprawnienia do sprostowania lub uzupełnienia, o którym mowa w art. 16 rozporządzenia 2016/679, nie może naruszać integralności protokołu oraz jego załączników*);
 - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych z zastrzeżeniem przypadków, o których mowa w art. 18 ust. 2 RODO (*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*);
 - prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy osoba, której dane osobowe dotyczą uzna, że przetwarzanie jej danych osobowych narusza przepisy RODO;
 - i) nie przysługuje osobie, której dane osobowe dotyczą:
 - 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 tych danych osobowych jest art. 6 ust. 1 lit. c RODO.
 - j) w przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1-3 RODO, wymagałoby niewspółmiernie dużego wysiłku, zamawiający może żądać od osoby, której dane dotyczą, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty postępowania o udzielenie zamówienia publicznego
 - k) Wystąpienie z żądaniem, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego.
6. Jeżeli w SWZ, umowie lub załącznikach jest mowa o “produkcie, materiale czy systemie typu lub np. ...” należy przez to rozumieć produkt, materiał czy system taki, jak zaproponowany lub inny o standardzie i parametrach technicznych nie gorszych niż zaproponowany. Wszystkie użyte w SWZ, umowie lub załącznikach znaki handlowe, towarowe, przywołania patentów, nazwy modeli, numery katalogowe służą jedynie do określenia cech technicznych i jakościowych materiałów, a nie są wskazaniem na producenta. Użyte wszelkie nazwy handlowe w opisie przedmiotu zamówienia Zamawiający traktuje, jako informację uściślającą, która została użyta wyłącznie w celu przybliżenia potrzeb Zamawiającego. Dopuszcza się użycie do realizacji zamówienia produktów równoważnych, w stosunku do ich jakości, docelowego przeznaczenia, spełnianych funkcji i walorów użytkowych. Przez jakość należy rozumieć zapewnienie minimalnych parametrów produktu wskazanego w SWZ, umowie i załącznikach. Wykonawca, który do wyceny przyjmie rozwiązanie równoważne jest zobowiązany udowodnić równoważność przyjętego wyposażenia, materiałów. W celu potwierdzenia, że oferowane rozwiązanie równoważne spełnia wymagania określone w SWZ, wykonawca złoży Szczegółowy opis oferowanego przedmiotu zamówienia równoważnego, w którym dla każdego produktu określi nazwę producenta, typ/model oraz inne cechy produktu pozwalające na

jednoznaczną identyfikację zaoferowanego produktu i potwierdzenie zgodności z opisem przedmiotu zamówienia. Niezłożenie takiego wykazu będzie równoznaczne z przyjęciem rozwiązań wskazanych w SWZ. Zamawiający dopuszcza rozwiązania równoważne opisywane w SWZ oraz załącznikach za pomocą norm, europejskich ocen technicznych, aprobat, specyfikacji technicznych i systemów referencji technicznych w tym dokumenty równoważne. Wykonawca, który powołuje się na rozwiązania równoważne opisane przez Zamawiającego, jest obowiązany wykazać, że oferowany przez niego przedmiot zamówienia spełnia wymagania określone przez Zamawiającego. Niezłożenie takiego wykazu będzie równoznaczne z przyjęciem rozwiązań wskazanych w SWZ oraz załącznikach.

Załączniki:

- | | |
|---|---------|
| 1. Wzór formularza ofertowego | - zał 1 |
| 2. Formularz oświadczeń wykonawcy – JEDZ | - zał 2 |
| 3. Formularz oświadczenia o przynależności/braku przynależności do tej samej grupy kapitałowej składany na wezwanie Zamawiającego | - zał 3 |
| 4. Formularz oświadczeń wykonawcy składany na wezwanie Zamawiającego | - zał 4 |
| 5. Wzór umowy | - zał 5 |
| 6. Opis przedmiotu zamówienia | - zał 6 |

DZP.381.15A.2021

Załącznik nr 1

**FORMULARZ OFERTOWY DLA UNIWERSYTECKIEGO CENTRUM
KLINICZNEGO IM. PROF. K. GIBIŃSKIEGO SUM W KATOWICACH**

Nazwa wykonawcy

Siedziba:

Adres zamieszkania*

**) dotyczy osób fizycznych prowadzących działalność gospodarczą oraz wspólników w spółce cywilnej*

REGON NIP

Tel. fax

e-mail

Adres strony www (jeśli istnieje)

numer konta (w celu
wpisania do umowy - w przypadku nie podania numeru konta Wykonawca zobowiązany jest
wpisać numer konta w umowie)

1. Ubiegając się o zamówienie publiczne na **Dostawę systemu zabezpieczeń klasy UTM** oferujemy realizację przedmiotowego zamówienia na warunkach określonych w specyfikacji warunków zamówienia (dalej w treści: SWZ) za łączną kwotę:

L.p.	Przedmiot zamówienia	Ilość	Cena jedn. netto	Wartość netto (ilość x cena jedn. netto)	VAT (%)	Wartość brutto (wartość netto + VAT)
1.	System zabezpieczeń klasy UTM opisany w załączniku nr 6 (Opis Przedmiotu zamówienia)	1				
RAZEM					X	

Zamawiający dopuszcza, aby Wykonawca rozbił powyższą tabelkę cenową na poszczególne pozycje np. w celu wskazania odrębnej stawki VAT dla poszczególnych elementów itp.

Oświadczamy, iż oferujemy następujący System zabezpieczeń klasy UTM

- Nazwa systemu (podać)
- Producent: (podać)
- Model: (podać)

2. **Oświadczamy, iż oferujemy następujący okres wsparcia gwarancyjnego:**

- a) 24 miesiące*
- b) 36 miesięcy lub więcej tj.(podać liczbę miesięcy tylko w przypadku, gdy Wykonawca oferuje większą liczbę miesięcy niż 36) *

* niepotrzebny podpunkt (a lub b) skreślić lub właściwy zaznaczyć

(W przypadku nie skreślenia lub nie zaznaczenia żadnego podpunktu Zamawiający przyjmuje, iż Wykonawca oferuje 24 miesięczny okres wsparcia gwarancyjnego). Niedopuszczalne jest zaoferowanie niepełnych miesięcy np. 36,5 - w takim wypadku Zamawiający przy ocenie oferty zaokrągla podany termin w „dół” do pełnych miesięcy.)

3. **Oświadczamy, iż oferujemy następujący czas usunięcia awarii w okresie wsparcia gwarancyjnego:**

- a) do 4 godzin roboczych*
- b) powyżej 4 godzin roboczych do 6 godzin roboczych*
- c) powyżej 6 godzin roboczych do 8 godzin roboczych *

* niepotrzebny podpunkt (a lub b lub c) skreślić lub właściwy zaznaczyć

(W przypadku nie skreślenia lub nie zaznaczenia żadnego podpunktu Zamawiający przyjmuje, iż Wykonawca oferuje termin powyżej 6 godzin roboczych do 8 godzin roboczych (tj. liczonych od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy w godzinach 08:00 do 16:00) od momentu zgłoszenia przez Zamawiającego.)

4. **Oświadczamy, iż oferujemy następujący tryb dodatkowego wsparcia technicznego producenta w okresie wsparcia gwarancyjnego:**

- a) W trybie 24 godziny przez 7 dni w tygodniu*
- b) Co najmniej w godzinach od 8.00 do 16.00 od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy *

* niepotrzebny podpunkt (a lub b) skreślić lub właściwy zaznaczyć

(W przypadku nie skreślenia lub nie zaznaczenia żadnego podpunktu Zamawiający przyjmuje, iż Wykonawca oferuje tryb wskazany w ppkt b) tj. Wykonawca deklaruje wsparcie co najmniej w godzinach od 8.00 do 16.00 od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy)

5. **Oświadczamy, iż oferujemy następujący czas wymiany lub części urządzenia na sprawne w okresie wsparcia gwarancyjnego:** dni roboczych *(maksymalny termin to 7 dni roboczych liczonych od dnia otrzymania przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego). W przypadku nie uzupełnienia Zamawiający przyjmuje, iż Wykonawca oferuje termin 7 dni roboczych liczonych od dnia otrzymania przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego. Niedopuszczalne jest zaoferowanie okresu częściowego np. 5,5 dnia - w takim wypadku Zamawiający przy ocenie oferty zaokrągla podany termin w „górę” do pełnych dni.)*

- 6. Oświadczamy, iż w cenie naszej oferty zostały uwzględnione wszystkie koszty wykonania zamówienia.
- 7. Oświadczamy, że wybór naszej oferty nie będzie prowadzić do powstania u Zamawiającego obowiązku podatkowego, w sytuacji, gdy nie dołączyliśmy do oferty informacji wykonawcy o powstaniu obowiązku podatkowego.

8. Zapoznaliśmy się ze Specyfikacją Warunków Zamówienia, nie wnosimy do niej zastrzeżeń oraz zdobyliśmy konieczne informacje do przygotowania oferty i zobowiązujemy się spełnić wszystkie wymienione w Specyfikacji wymagania Zamawiającego
9. Jesteśmy związani niniejszą ofertą przez czas wskazany w Specyfikacji Warunków Zamówienia.
10. Zawarta w Specyfikacji Warunków Zamówienia treść wzoru umowy została przez nas zaakceptowana i zobowiązujemy się w przypadku wyboru naszej oferty do zawarcia umowy na wyżej wymienionych warunkach w miejscu i terminie wyznaczonym przez Zamawiającego
11. W przypadku dołączenia do oferty dokumentów o których mowa w pkt. VII.5 SWZ oświadczamy, że pomimo tego, że nie było to wymagane na tym etapie postępowania dokumenty te są aktualne oraz zgodne ze stanem faktycznym na dzień złożenia i wyrażamy zgodę na zbadanie przez Zamawiającego załączonych dokumentów.
12. Oświadczam, że wypełniłem obowiązki informacyjne przewidziane w art. 13 lub art. 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016) (dalej w treści RODO) wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskałem w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu.*
*(*W przypadku gdy wykonawca nie przekazuje danych osobowych innych niż bezpośrednio jego dotyczących lub zachodzi wyłączenie stosowania obowiązku informacyjnego, stosownie do art. 13 ust. 4 lub art. 14 ust. 5 RODO, może wykreślić treść niniejszego oświadczenia)*
13. Rodzaj Wykonawcy:
 - a) Mikroprzedsiębiorstwo*
 - b) Małe przedsiębiorstwo*
 - c) Średnie przedsiębiorstwo*
 - d) Jednoosobowa działalnością gospodarczą
 - e) Osoba fizyczna nieprowadząca działalności gospodarczej
 - f) Inny rodzaj*

(*Niewłaściwe skreślić lub właściwe zaznaczyć – punkt nieobowiązkowy)

DZP.381.15A.2021

Załącznik nr 3

.....
(nazwa wykonawcy)

**Oświadczenie
o przynależności lub braku przynależności*
do tej samej grupy kapitałowej, o której mowa w art. 108 ust. 1 pkt 5
Prawa zamówień publicznych**

Dotyczy postępowania o udzielenie zamówienia publicznego na
Dostawę systemu zabezpieczeń klasy UTM

dla Uniwersyteckiego Centrum Klinicznego im. prof. K. Gibińskiego Śląskiego Uniwersytetu
Medycznego w Katowicach

- ☐ Oświadczam, że **nie należę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), z innym Wykonawcą, który złożył odrębną ofertę, ofertę częściową w niniejszym postępowaniu.

lub

- ☐ Oświadczam, że **należę** do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (Dz. U. z 2021 r. poz. 275), co następujący Wykonawca, który złożył odrębną ofertę w niniejszym postępowaniu:

.....
(nazwa Wykonawcy)

W przypadku przynależności do tej samej grupy kapitałowej wykonawca składa dokumenty lub informacje potwierdzające przygotowanie oferty, oferty częściowej w postępowaniu niezależnie od innego wykonawcy należącego do tej samej grupy kapitałowej

Uwaga w przypadku Wykonawców ubiegających się wspólnie o udzielenie zamówienia na podstawie art. 23 ustawy PZP dokument składa każdy z Wykonawców oddzielnie.

- ☐ Właściwe zaznaczyć *X*
lub niewłaściwe skreślić

DZP.381.15A.2021

Załącznik nr 4

.....
(nazwa wykonawcy)**OŚWIADCZENIE****O AKTUALNOŚCI INFORMACJI ZAWARTYCH W OŚWIADCZENIU , O KTÓRYM
MOWA W ART.125.UST.1 USTAWY PZP**

Dotyczy postępowania o udzielenie zamówienia publicznego na **Systemu zabezpieczeń klasy UTM** dla Uniwersyteckiego Centrum Klinicznego im. prof. K. Gibińskiego Śląskiego Uniwersytetu Medycznego w Katowicach

Oświadczam, że informacje zawarte w Jednolitym Europejskim Dokumencie Zamówienia (JEDZ), o którym mowa w art. 125 ust. 1 ustawy, w zakresie podstaw wykluczenia z postępowania o których mowa w:

- 1) art. 108 ust. 1 pkt 3 ustawy, dotyczących wydania prawomocnego wyroku sądu lub ostatecznej decyzji administracyjnej o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne,
- 2) art. 108 ust. 1 pkt 4 ustawy, dotyczących prawomocnego orzeczenia zakazu ubiegania się o zamówienie publiczne,
- 3) art. 108 ust. 1 pkt 5 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenie konkurencji,
- 4) art. 108 ust. 1 pkt 6 ustawy, dotyczących zawarcia z innymi wykonawcami porozumienia mającego na celu zakłócenia konkurencji, wynikającego z wcześniejszego zaangażowania Wykonawcy lub podmiotu który należy z Wykonawcą do tej samej grupy kapitałowej w przygotowanie postępowania o udzielenie zamówienia,

są nadal aktualne.

DZP.381.15A.2021

Załącznik nr 5

wzór

UMOWA nr

Zawarta w dniu w Katowicach pomiędzy:

Uniwersyteckim Centrum Klinicznym im. prof. K. Gibińskiego
Śląskiego Uniwersytetu Medycznego w Katowicach

z siedzibą: 40 – 514 Katowice, ul. Ceglana 35

wpisanym do KRS pod nr 0000049660

NIP 954-22-74-017

REGON 001325767

zwanym w treści umowy Zamawiającym,
reprezentowanym przez:

.....

a

.....

z siedzibą:

wpisanym do

NIP

REGON

zwanym w treści umowy Wykonawcą
reprezentowanym przez:

.....

W wyniku przeprowadzenia przez Zamawiającego postępowania o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego – zgodnie z ustawą z dnia 19 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 2019 z późn. zm.) (dalej zwanej: „Pzp”) została zawarta umowa następującej treści:

§ 1.

PRZEDMIOT UMOWY

W wyniku przeprowadzonego postępowania w trybie przetargu nieograniczonego na **Dostawę systemu zabezpieczeń klasy UTM** Zamawiający zamawia a Wykonawca zobowiązuje się sprzedać i dostarczyć do siedziby Zamawiającego w lokalizacji przy ul. Ceglanej 35 w Katowicach system wskazany w opisie przedmiotu zamówienia stanowiącym załącznik nr 2 oraz zainstalować, wdrożyć, skonfigurować oraz uruchomić dostarczony system (zwany dalej: systemem) wraz z instruktażem personelu Zamawiającego w zakresie jego obsługi i konfiguracji w zakresie wskazanym w załącznik nr 2 zgodnie z formularzem ofertowym będącym integralną częścią niniejszej umowy stanowiącym załącznik nr 1.

§ 2.

WARUNKI REALIZACJI UMOWY

1. Wykonawca zobowiązuje się realizować umowę zgodnie z:
 - a) obowiązującymi przepisami prawa
 - b) warunkami wynikającymi z treści Specyfikacji Warunków Zamówienia.
2. Wykonawca oświadcza i gwarantuje, że:
 - a) dostarczony system jest fabrycznie nowy
 - b) przedmiot umowy jest wolny od wad
 - c) oferowany system posiada wszystkie wymagane prawem certyfikaty lub dokumenty równoważne,
 - d) system nie jest obciążony prawami osób trzecich, oraz należnościami na rzecz Skarbu Państwa z tytułu sprowadzenia go na polski obszar celny,
3. Dostawa systemu do Zamawiającego do lokalizacji przy ul. Ceglanej 35 w Katowicach.
4. Wykonawca zobowiązuje się w terminie do **60 dni kalendarzowych** od dnia zawarcia umowy dostarczyć, wdrożyć, skonfigurować i uruchomić system oraz przeprowadzić instruktaż wskazanych pracowników Zamawiającego, co zostanie potwierdzone protokołem odbioru podpisanym przez obie strony.
5. Najpóźniej na 3 dni robocze (tj. od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy) przed dostawą winno nastąpić zawiadomienie Działu Informatyki (tel. 32 358 13 52 e-mail informatyka@uck.katowice.pl) o terminie dostarczenia systemu.
6. Wykonawca ponosi koszty transportu, rozładunku, ubezpieczenia systemu do miejsca jego odbioru wskazanego w § 2 ust. 3.
7. Wykonawca dostarczy Zamawiającemu wraz z systemem:
 - a) komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
 - b) wszystkie niezbędne licencje oprogramowania pozwalające na poprawne funkcjonowanie systemu oraz opisanych funkcjonalności
 - c) wykaz podmiotów upoważnionych do wykonywania czynności serwisowych
 - d) instrukcję obsługi w wersji elektronicznej (pendrive itp)
8. Instruktaż pracowników Zamawiającego, o których mowa w § 1 musi być przeprowadzony przez osoby posiadające stosowną wiedzę i doświadczenie, a także spełniające obowiązujące u Zamawiającego warunki pozwalające takim osobom na przebywanie w pomieszczeniach Zamawiającego.

§3.

WYNAGRODZENIE I WARUNKI PŁATNOŚCI

1. Wynagrodzenie Wykonawcy za należyte zrealizowanie przedmiotu umowy określonego w §1 wynosi:
netto:zł
należny podatek VAT:zł
brutto:zł
(słownie:.....)
2. Zapłata za dostarczony zgodnie z umową system nastąpi przelewem na następujący rachunek bankowy Wykonawcy w ciągu 30 dni od dnia otrzymania przez Zamawiającego prawidłowo wypełnionej faktury VAT w formie papierowej na adres Zamawiającego lub w formie elektronicznej poprzez

zastosowanie adresu PEF (rodzaj adresu PEF: NIP, numer adresu PEF: 9542274017). W przypadku gdyby Wykonawca zamieścił na fakturze inny termin płatności niż określony w niniejszej umowie obowiązuje termin płatności określony w umowie. Podstawą wystawienia faktury jest protokół odbioru o którym mowa w § 2 ust. 4.

3. Za datę dokonania zapłaty przyjmuje się datę obciążenia rachunku bankowego Zamawiającego.
4. Na podstawie art. 12 ust. 4i i 4j oraz art. 15d ustawy o podatku dochodowym od osób prawnych (tekst jednolity: Dz.U. 2020 poz. 1406 z późn.zm.):
 - a. Wykonawca ma obowiązek wskazania w umowie rachunku bankowego, który jest zgodny z rachunkiem bankowym przypisanym mu w wykazie podmiotów zarejestrowanych jako podatnicy VAT, w tym podmiotów których rejestracja jako podatników VAT została przywrócona, prowadzonym przez Szefa Krajowej Administracji Skarbowej zgodnie z art. 96b ustawy o podatku od towarów i usług.
 - b. W przypadku zmiany rachunku bankowego lub wykreślenia wskazanego w pkt. a rachunku bankowego Wykonawcy z wykazu jest on zobowiązany do poinformowania o tym fakcie Zamawiającego w terminie 1 dnia od momentu zaistnienia zmiany. Informacja winna zawierać nowy numer rachunku bankowego umieszczony w wykazie na który mają zostać dokonane płatności, i być podpisana przez osoby upoważnione do reprezentowania Wykonawcy oraz w pierwszej kolejności przekazana Zamawiającemu drogą elektroniczną (na adres poczty elektronicznej: ksiegowosc@uck.katowice.pl), a następnie w oryginale do siedziby Zamawiającego. Informacja o której mowa powyżej stanowi podstawę do sporządzenia przez Zamawiającego aneksu do umowy w zakresie zmiany rachunku bankowego. W przypadku poinformowania Zamawiającego o zmianie rachunku bankowego, jego wykreślenia lub stwierdzenia przez Zamawiającego wykreślenia wskazanego w pkt. a rachunku bankowego Wykonawcy z wykazu, płatność wymagalna zostaje zawieszona do dnia wskazania przez Wykonawcę innego rachunku, który znajduje się w wykazie, o którym mowa w pkt a.
 - c. W przypadku zawieszenia terminu płatności faktury zgodnie z pkt b, który został określony zgodnie z niniejszą umową, Wykonawcy nie będzie przysługiwało prawo do naliczania dodatkowych opłat, kar, rekompensat, ani nie będzie naliczał odsetek za powstałe opóźnienie w zapłacie faktury.
 - d. W przypadku, jeżeli Zamawiający dokona wpłaty na rachunek bankowy Wykonawcy wskazany w umowie, a rachunek ten na dzień zlecenia przelewu nie będzie ujęty w wykazie, o którym mowa w pkt a Wykonawca zobowiązany będzie do zapłaty na rzecz Zamawiającego kary umownej w wysokości równowartości sankcji jaka zostanie nałożona przez Urząd Skarbowy wobec Zamawiającego wraz z należnymi odsetkami lub równowartości podatku dochodowego od osób prawnych jaki Zamawiający zapłaci do Urzędu skarbowego z tytułu okoliczności wynikających z powyższych punktów, albo szkody jaką Zamawiający poniesie z tego tytułu. Kara umowna będzie płatna na podstawie noty księgowej wystawionej przez Zamawiającego w terminie 7 dni od daty jej wystawienia.

§ 4.

GWARANCJA, REALIZACJA UPRAWNIENÍ GWARANCYJNYCH

1. Wykonawca udziela miesięcznego okresu wsparcia gwarancyjnego (tj. gwarancji), który rozpoczyna się od dnia podpisania przez Zamawiającego bez zastrzeżeń protokołu z odbioru systemu. Szczegółowo warunki gwarancji zostały opisane w załączniku nr 2 do umowy.

2. Wykonawca udziela również dodatkowego wsparcia technicznego producenta w okresie wsparcia gwarancyjnego w trybie Szczegółowo warunki wsparcia zostały opisane w załączniku nr 2 do umowy.
3. Wykonawca gwarantuje, iż czas usunięcia awarii w okresie gwarancji będzie nie dłuższy niż godzin roboczych (tj. godzin liczonych od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy w godzinach 08.00 do 16.00) od momentu zgłoszenia przez Zamawiającego.
4. Wykonawca gwarantuje, iż czas rozwiązania błędu/konsultacji w okresie wsparcia gwarancyjnego będzie nie dłuższy niż 2 dni robocze od chwili zgłoszenia przez Zamawiającego. Zamawiający dokonuje zgłoszenia błędu na adres e-mail lub telefonicznie na numer
5. Zgłoszenia awarii dokonywane będą pisemnie (za pośrednictwem poczty elektronicznej na adres e-mail: lub za pośrednictwem faxu na numer.....)
6. Gdy liczba napraw gwarancyjnych tego samego systemu (urządzenia) lub części sytemu (urządzenia) przekroczy 3 (trzy) (z wyjątkiem uszkodzeń z winy Zamawiającego) Wykonawca zobowiązuje się do wymiany urządzenia lub części urządzenia na swój koszt. Czas wymiany urządzenia lub części urządzenia na sprawne nie może przekroczyć dni roboczych liczonych od dnia otrzymania przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego.
7. Usunięcie awarii objętych gwarancją, w tym także ewentualne koszty transportu systemu lub jego elementów składowych do miejsca naprawy i z miejsca na koszt własny Wykonawcy.
8. Okres gwarancji udzielonej przez Wykonawcę ulega przedłużeniu o pełen okres niesprawności dostarczonego systemu.

§ 5.

KARY UMOWNE

1. Wykonawca zapłaci Zamawiającemu następujące kary umowne:
 - a) w wysokości 0,5% kwoty wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy za każdy dzień zwłoki w realizacji obowiązków określonych w § 2 ust. 4 umowy;
 - b) w wysokości 50,00 zł (słownie: pięćdziesięciu złotych 00/100), za każdą godzinę zwłoki w realizacji względem terminu, o którym mowa w § 4 ust. 2, 3 umowy.
 - c) w wysokości 0,1 % kwoty wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy za każdy dzień zwłoki w realizacji obowiązków określonych w § 4 ust. 4 umowy;
 - d) w wysokości 0,1 % kwoty wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy za każdy dzień zwłoki w realizacji obowiązków określonych w § 4 ust. 6 umowy;
 - e) w wysokości 10% kwoty wynagrodzenia brutto określonego w §3 ust. 1 niniejszej umowy – w przypadku gdy z przyczyn, za które odpowiada Wykonawca nastąpi odstąpienie od umowy lub wypowiedzenie lub rozwiązanie umowy ze skutkiem natychmiastowym.
2. Łączna wartość kar umownych naliczonych na podstawie zapisów umowy nie przekroczy 50% wartości brutto wynagrodzenia określonego w § 3 ust. 1 umowy.
3. Należność z tytułu kary umownej będzie płatna w terminie 7 dni od daty wystawienia przez Zamawiającego noty obciążeniowej.
4. W przypadku, gdy wysokość wyrządzonej szkody przewyższa naliczoną karę umowną Zamawiający ma prawo żądać odszkodowania uzupełniającego na zasadach ogólnych.

§ 6.

ROZWIĄZANIE I ODSTĄPIENIE OD UMOWY

1. W razie zaistnienia istotnej zmiany okoliczności powodującej, że wykonanie umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia umowy, lub dalsze wykonywanie umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu Zamawiający może odstąpić od umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu wykonania części umowy.
2. Zamawiający może rozwiązać umowę ze skutkiem natychmiastowym w przypadku gdy zwłoka Wykonawcy w realizacji obowiązków określonych w § 2 ust. 4 przekroczy 10 dni kalendarzowych.
3. Dla skuteczności oświadczenia o rozwiązaniu umowy, wystarczające jest jego przesłanie na adres Wykonawcy wskazany w umowie.
4. Rozwiązanie umowy na podstawie ust. 2 niniejszego paragrafu nie zwalnia Wykonawcy od obowiązku zapłaty kar umownych i odszkodowań.

§ 7.

POSTANOWIENIA KOŃCOWE

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie odpowiednie przepisy ustawy – Prawo zamówień publicznych i Kodeksu Cywilnego.
2. W przypadku niejasności w zapisach niniejszej umowy Strony mogą odwołać się do zapisów w Specyfikacji Warunków Zamówienia.
3. Strony ustalają, że wszelkie zmiany postanowień niniejszej umowy mogą być wprowadzane wyłącznie zgodnie z obowiązującymi przepisami prawa oraz przy zachowaniu zasad wynikających z niniejszej umowy.
4. Zmiana numeru rachunku bankowego Wykonawcy wymaga formy pisemnego aneksu pod rygorem nieważności.
5. Strony dopuszczają zmiany w umowie w zakresie:
 - a) zmiany danych stron (np. zmiana siedziby, adresu, nazwy),
 - b) zmniejszenie ceny określonej w umowie przy zachowaniu pozostałych warunków bez zmian.
 - c) zmiany systemu na nowszy lub aktualizacji rozwiązań technicznych zastosowanych w systemie ze względu na postęp techniczny lub technologiczny (np. wycofanie z obrotu/niedostępność zaoferowanego w ofercie systemu, zmiana wersji oprogramowania. Zmiana taka nie może spowodować: podwyższenia ceny, wzrostu wartości umowy, ani obniżenia parametrów technicznych, jakościowych i innych wynikających z oferty na podstawie której był dokonany wybór Wykonawcy;
5. Zmiany określone w ust. 5 pkt a) wymagają dla swej skuteczności pisemnego powiadomienia drugiej strony. Zmiany określone w ust. 4, ust. 5 pkt b) i c) wymagają formy pisemnego aneksu pod rygorem nieważności.
6. Wykonawca nie może bez uzyskania wcześniejszej pisemnej zgody Zamawiającego, przelać jakichkolwiek praw lub obowiązków wynikających z niniejszej umowy na osoby trzecie. Czynność prawna mająca na celu zmianę wierzyciela może nastąpić wyłącznie po wyrażeniu zgody przez podmiot tworzący Zamawiającego.
7. Wszelkie spory wynikłe na tle realizacji umowy będzie rozstrzygał sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
8. Umowę sporządzono w trzech jednobrzmiących egzemplarzach, dwa egzemplarze dla

Zamawiającego, jeden egzemplarz dla Wykonawcy.

Załączniki do umowy:

1. Formularz ofertowy
2. Opis przedmiotu zamówienia

Wykonawca

Zamawiający

OPIS PRZEDMIOTU ZAMÓWENIA

SYSTEM ZABEZPIECZEŃ KLASY UTM

1. Wymagania dotyczące realizacji przedmiotu Zamówienia

1.1. Wymagania ogólne dotyczące dostawy i instalacji elementów zamówienia

1. Dostarczony sprzęt musi być fabrycznie nowy (zapakowany w opakowanie przeznaczone dla przedmiotu zamówienia), wyprodukowany nie wcześniej niż 2021 r. Nie dopuszcza się urządzeń noszących jakiegokolwiek widoczne ślady użycia, odnawianych, demonstracyjnych lub powystawowych oraz wykorzystanych przynajmniej raz w innym projekcie.
2. Nie dopuszcza się, aby licencje przypisane do obecnie posiadanych przez Zamawiającego zostały przeniesione na urządzenia dostarczane w ramach bieżącego zamówienia.
3. Urządzenia muszą być oznakowane w taki sposób, aby była możliwa identyfikacja zarówno produktu, jak i producenta. Do każdego urządzenia musi być dostarczony komplet standardowej dokumentacji dla użytkownika w języku polskim lub angielskim w formie papierowej lub elektronicznej.
4. Wraz ze sprzętem muszą zostać dostarczone wszystkie niezbędne licencje oprogramowania pozwalające na poprawne funkcjonowanie sprzętu oraz opisanych funkcjonalności.
5. Wraz z sprzętem Wykonawca ma obowiązek dostarczyć wszystkie elementy i okablowanie niezbędne do poprawnej pracy oraz montażu sprzętu w posiadanej przez Zamawiającego szafie Rack.
6. Wykonawca zobowiązany jest zorganizować prace tak, aby w maksymalnym stopniu nie zakłócać ciągłości funkcjonowania Zamawiającego, a w szczególności wszystkich usług, które dotychczas są realizowane przez obecnie posiadane urządzenia UTM.

1.2. Wymagania dotyczące dokumentacji

W ramach przedmiotu zamówienia Wykonawca zobowiązany jest dostarczyć na etapie realizacji następującą dokumentację dotyczącą systemu bezpieczeństwa:

1. Harmonogram realizacji umowy uzgodniony z Zamawiającym zgodnie z tabelą wskazaną w punkcie 1.3. poniżej.
2. Propozycję konfiguracji systemu uzgodnioną z Zamawiającym – do zatwierdzenia przez Zamawiającego.
3. Instrukcję postępowania w przypadku awarii systemu – procedurę przywracania kopii zapasowych konfiguracji systemu.
4. Dokument zawierający dane do logowania dla administratora do poszczególnych elementów systemu.
5. Kompletną dokumentację techniczną elementów systemu bezpieczeństwa w języku polskim obejmującą:
 - opis konfiguracji całego systemu,
 - instrukcje aktualizacji,

- instrukcje administrowania dostarczonym systemem bezpieczeństwa.

1.3. Harmonogram realizacji umowy

Realizacja umowy obejmującej dostarczenie systemu bezpieczeństwa będzie przebiegać etapowo, zgodnie z poniższym harmonogramem:

ETAP	Zakres prac	Termin Realizacji
ETAP I	Uzgodnienia z Zamawiającym, przygotowanie szczegółowego harmonogramu realizacji umowy, przygotowanie koncepcji konfiguracji dostarczonego systemu.	15 dni kalendarzowych od daty podpisania umowy
ETAP II	Dostawa przedmiotu zamówienia obejmująca sprzęt oraz oprogramowanie.	15 dni kalendarzowych od daty zakończenia etapu I
ETAP III	Konfiguracja, parametryzacja systemu zgodnie z zaakceptowaną przez Zamawiającego koncepcją i uruchomienie systemu w środowisku produkcyjnym Zamawiającego.	15 dni kalendarzowych od daty zakończenia etapu II
ETAP IV	Instruktaż dla personelu Zamawiającego.	8 dni kalendarzowych od zakończenia Etapu III
ETAP V	Zakończenie realizacji umowy – dostarczenie niezbędnych dokumentów.	7 dni kalendarzowych od daty zakończenia Etapu IV

Wykonawca zrealizuje co najmniej następujące zadania w ramach poniższych etapów:

ETAP I

- 1 Uzgodnienie z Zamawiającym warunków instalacji systemu bezpieczeństwa w infrastrukturze sieciowej Zamawiającego.
- 2 Zapoznanie (wykonanie audytu) się z istniejącą topologią sieci oraz używanych przez Zamawiającego mechanizmów sieciowych w obu lokalizacjach pod kątem wyboru optymalnej topologii docelowej.
- 3 Wykonanie kompleksowego audytu konfiguracji i funkcjonowania obecnie posiadanych przez Zamawiającego systemów firewall FortiGate firmy Fortinet, których konfiguracja ma stanowić punkt wyjścia do opracowania koncepcji wdrożenia nowego systemu bezpieczeństwa.
- 4 Wykonanie analizy użycia używanych obecnie łącz oraz przepływu danych w sieci pod kątem aktywnego wykorzystania przez poszczególne usługi biznesowe Zamawiającego.

- 5 Przygotowanie konfiguracji dla nowego systemu bezpieczeństwa zgodnie z wytycznymi Zamawiającego, pod kątem zgodności z wdrożonym Systemem Zarządzania Bezpieczeństwem Informacji w oparciu o normę ISO 27001:2017 lub równoważną.
- 6 Przygotowanie konfiguracji dla nowego systemu bezpieczeństwa z uwzględnieniem dobrych praktyk (Best Practices) producenta oferowanego systemu.
- 7 Przygotowanie koncepcji wdrożenia systemu bezpieczeństwa, w skład którego wejdą posiadane przez Zamawiającego obecnie urządzenia FortiGate 600E firmy Fortinet (w jednej z lokalizacji Zamawiającego) oraz urządzenia dostarczone w ramach tego zamówienia dla drugiej lokalizacji, które zastąpią obecnie posiadane urządzenia FortiGate 600C firmy Fortinet.
- 8 Uwzględnienie w koncepcji wdrożenia integracji z pozostałymi posiadanymi przez Zamawiającego urządzeniami bezpieczeństwa tj. m.in. FortiWeb 400C, FortiAP223E, przełącznikami szkieletowymi HP serii ProCurve 54xx, usługami RADIUS, Active Directory.
- 9 W oparciu o powyższe przedstawienie właściwej topologii dla obu lokalizacji.
- 10 W oparciu o przeprowadzone audyty przygotowanie koncepcji wdrożenia podstawowych elementów (m.in. reguł filtracji, translacji) oraz szczegółowej koncepcji wszystkich obsługiwanych przez firewall funkcji bezpieczeństwa, tuneli VPN (typu IPSec oraz SSL), identyfikacji użytkowników z wykorzystaniem kont w Active Directory oraz inteligentnego obciążenia łącz do Internetu.
- 11 Przygotowanie koncepcji integracji dostarczanego systemu bezpieczeństwa z dostarczonym centralnym systemem logowania, raportowania i korelacji, który ma zastąpić posiadany przez Zamawiającego systemem logowania i raportowania FortiAnalyzer 200D firmy Fortinet Przygotowanie procedury awaryjnej „rollback” na wypadek niepowodzenia wdrożenia nowego systemu bezpieczeństwa.

ETAP II – dostawa przedmiotu umowy**ETAP III**

- 1 Kompletne uruchomienie całego systemu bezpieczeństwa zgodnie z zatwierdzoną przez Zamawiającego koncepcją weryfikacja poprawności funkcjonowania uruchomionego systemu, testy powdrożeniowe.
- 2 Przedstawienie w formie dokumentacji pisemnej analizy/wyników uruchomienia systemu.
- 3 Przetestowanie procedury awaryjnej.

ETAP IV – przeprowadzenie instruktażu**Etap V**

- 1 Przekazanie i odbiór dokumentacji użytkownika, administratora oraz technicznej.
- 2 Odbiór końcowy systemu na środowisku produkcyjnym Zamawiającego.

2. Wymagania dotyczące sposobu realizacji przedmiotu Zamówienia

Poniżej przedstawione zostały szczegółowe wymagania dotyczące sposobu realizacji umowy.

2.1. Zarządzanie realizacją Umowy

Za bieżące zarządzanie wdrożeniem odpowiadają odpowiednio osoba nadzorująca wdrożenie po stronie Wykonawcy oraz kierownik Działu Informatyki i jego zastępca po stronie Zamawiającego.

2.2. Wymagania dotyczące instruktaży dla administratorów

Zamawiający określa ilość osób do odbycia instruktażu dla administratorów na **maksymalnie 2 osoby** spośród swoich pracowników. Instruktaże odbędą się w ramach realizacji Etapu IV oraz w terminie przewidzianym na jego realizację. Instruktaż dla administratorów ma na celu umożliwienie Zamawiającemu samodzielne użytkowanie oraz administrowanie zakupionym i wdrożonym systemem bezpieczeństwa.

Wykonawca przeprowadzi dwa rodzaje instruktażu:

- instruktaż z obsługi i konfiguracji systemu bezpieczeństwa UTM – **UWAGA** tylko w przypadku gdy dostarczony „system bezpieczeństwa UTM będzie innego producenta niż obecnie stosowany
- instruktaż z administracji „systemu centralnego zarządzania”.

Instruktaż dla administratorów należy przeprowadzić w siedzibie Zamawiającego, w uzgodnionych terminach, tak by nie zakłócił on bieżącej pracy. Dopuszczalne jest przeprowadzenie instruktażu poza siedzibą Zamawiającego, za jego uprzednią zgodą. W takim przypadku Wykonawca ponosi koszty organizacji i zakwaterowania uczestników. Instruktaż musi obejmować zakres wiedzy niezbędnej do samodzielnego realizowania funkcji administratora. Wykonawca jest zobowiązany zapewnić sprzęt niezbędny do realizacji instruktażu. Zamawiający udostępni Wykonawcy salę na okres trwania instruktażu.

Wykonawca musi zapewnić szczegółowe materiały do instruktażu w języku polskim pozwalające na samodzielne przeprowadzenie konfiguracji opcji dostępnych w oferowanym urządzeniu dla wszystkich uczestników instruktażu, zagwarantować przeprowadzenie go przez osoby posiadające certyfikacje techniczne na poziomie zaawansowanym potwierdzające umiejętności, zdolności do wdrażania, administrowania i rozwiązywania problemów związanych z rozwiązaniami bezpieczeństwa będącymi przedmiotem zamówienia, potwierdzone właściwymi certyfikatami wystawionymi przez podmiot uprawniony.

Czas trwania instruktażu z „systemu UTM” określa się na minimum 3 dni robocze oraz z „systemu centralnego zarządzania” na minimum 1 dzień roboczy. Systemy te są składowymi dostarczanego systemu bezpieczeństwa.

Lista osób do odbycia instruktażu dla administratorów będzie ustalona przez strony oraz potwierdzona przez Zamawiającego w trakcie Etapu II.

2.3. Odbiory

2.3.1. Odbiory systemu bezpieczeństwa (ilościowe, jakościowe)

Formalny odbiór elementów systemu bezpieczeństwa następuje poprzez podpisanie przez Strony Protokołu Końcowego Odbioru.

W ramach odbioru Wykonawca dostarczy następujące dokumenty:

- wykaz zawierający nazwę, model, numer seryjny, datę produkcji dla poszczególnych dostarczanych elementów systemu bezpieczeństwa,
- wykaz licencji zawierający nazwę i wersję oprogramowania,
- raport z weryfikacji poprawności działania wdrożonego systemu (poprawność utworzonych polityk, komunikacja z pozostałymi elementami systemu bezpieczeństwa posiadanymi już przez Zamawiającego, poprawność konfiguracji).

2.4. Dodatkowe zobowiązania wykonawcy

Wykonanie Przedmiotu Zamówienia z efektywnością oraz zgodnie z praktyką i wiedzą zawodową.

Wykonanie w całości Przedmiotu Zamówienia w zakresie określonym w Umowie.

Dokonanie z Zamawiającym wszelkich koniecznych ustaleń mogących wpływać na zakres i sposób realizacji Przedmiotu Zamówienia oraz ciągła współpraca z Zamawiającymi na każdym etapie realizacji.

Stosowanie się do wytycznych i polityk bezpieczeństwa informacji obowiązujących u Zamawiającego.

Udzielanie na każde żądanie Zamawiającego pełnej informacji na temat stanu realizacji Przedmiotu Zamówienia.

Współdziałanie z osobami wskazanymi przez Zamawiającego.

Lista załączników:

Załącznik nr 1. Opis Przedmiotu Zamówienia zawierający specyfikacje elementów systemu bezpieczeństwa, specyficzne warunki instalacji, dostaw i gwarancji.

3. Załącznik nr 1. Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest dostawa systemu zabezpieczeń klasy UTM dla lokalizacji Ceglana

Tabela 1. Elementy systemu bezpieczeństwa

Nazwa	Liczba zamawianego sprzętu
System UTM w konfiguracji wysokiej dostępności (HA)	1 komplet tj. 2 sztuki urządzeń
System logowania, raportowania i korelacji	1

Tabela 2. Wymagania wspólne dla systemu bezpieczeństwa

Wymagania wspólne		
1.	Ogólne	Dopuszcza się, aby poszczególne elementy wchodzące w skład systemu bezpieczeństwa były zrealizowane w postaci osobnych, komercyjnych platform sprzętowych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej systemu UTM dostawca musi zapewnić niezbędne platformy sprzętowe wraz z odpowiednio zabezpieczonym systemem operacyjnym (nie dotyczy systemu centralnego logowania, raportowania i korelacji).
2.	Licencje	- w ramach postępowania Wykonawca dostarczy minimum następujące licencje: • licencje umożliwiające korzystanie z aktualizacji baz funkcji ochronnych producenta i serwisów przez cały okres gwarancji. Muszą one obejmować co najmniej: kontrolę aplikacji, IPS, antywirus'a (z uwzględnieniem sygnatur do ochrony urządzeń mobilnych – co najmniej dla systemu operacyjnego Android), • licencje umożliwiające analizę typu antyspam, web filtering, bazy reputacyjne adresów IP/domen Wszystkie licencje na okres zgodny z zaoferowanym okresem wsparcia gwarancyjnego
3.	Gwarancja	KRYTERIUM PUNKTOWANE: <u>Okres wsparcia gwarancyjnego</u> zgodny z zaoferowanym w formularzu ofertowym okresem wsparcia, liczony od daty podpisania protokołu końcowego bez uwag na cały system bezpieczeństwa, (nie krótszy niż 24 miesiące), obejmujący minimum: naprawę lub wymianę urządzenia w przypadku jego wadliwości. Dostęp do aktualizacji dostarczonego w ramach systemu

		oprogramowania, usuwanie awarii całego systemu obejmujące zarówno awarie sprzętu jak i dostarczonego oprogramowania <u>Dodatkowe wsparcie techniczne producenta (kryterium punktowane)</u> • Zgodnie z zaoferowanym w formularzu ofertowym trybem, jednak co najmniej w godzinach od 8.00 do 16.00 od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy • możliwość konsultacji telefonicznych lub poprzez witrynę internetową w zakresie realizacji przedmiotu niniejszej umowy szczególnie informacje dotyczące używanych produktów w tym pomoc przy rozwiązywaniu problemów występujących w oprogramowaniu <u>Czas usunięcia awarii (kryterium punktowane)</u> • Zgodnie z zaoferowanym w formularzu ofertowym terminem – jednak nie dłużej niż 8 godzin roboczych (liczonych od poniedziałku do piątku za wyjątkiem dni ustawowo wolnych od pracy w godzinach 08:00 do 16:00) od momentu zgłoszenia na wskazany adres e-mail. W razie braku możliwości naprawy urządzenia Wykonawca przygotowuje raport z awarii celem zgłoszenia wymiany urządzenia. Przez „awarię” rozumie się problem, który uniemożliwia użytkowanie dostarczonego systemu bezpieczeństwa (w zakresie jego podstawowej funkcjonalności wskazanej w dokumentacji użytkownika (zgodnie z dostarczonymi licencjami na ich użytkowanie) i prowadzący do zatrzymania jego eksploatacji, utrata możliwości prowadzenia działalności wykonywanej przez Zamawiającego do której wymagany jest w/w system bezpieczeństwa, zgłoszony przez Zamawiającego przeznaczonym do tego celu kanałem komunikacyjnym <u>Czas wymiany urządzenia lub części urządzenia na sprawne (kryterium punktowane)</u> • Zgodnie z zaoferowanym w formularzu ofertowym czasem na wymianę jednak nie później niż w ciągu maksymalnie 7 dni roboczych, liczonych od dnia otrzymania od Zamawiającego przesyłki przez wskazany przez Wykonawcę serwis do dnia otrzymania sprawnego urządzenia przez Zamawiającego POZOSTAŁE WYMAGANIA: • Zamawiający ma mieć możliwość dokonania zgłoszenia błędu poprzez pocztę elektroniczną oraz telefonicznie a czas rozwiązania błędu/konsultacji będzie nie dłuższy niż 2 dni robocze od chwili zgłoszenia przez Zamawiającego.
--	--	---

		W przypadku, gdy zgłoszenie zostanie przyjęte przez Wykonawcę: - w godzinach pomiędzy 16.00 a 24.00 dnia roboczego – traktowane jest jak przyjęte o godz. 8.00 następnego dnia roboczego, - w godzinach pomiędzy 0.00 a 8.00 dnia roboczego – traktowane jest jak przyjęty o godz. 8.00 danego dnia roboczego, - w dniu ustawowo lub dodatkowo wolnym od pracy – traktowane jest jak przyjęte o godz. 8.00 najbliższego dnia roboczego. • serwisowany sprzęt oraz jego części, w razie awarii, muszą zostać wymienione na części fabrycznie nowe, o parametrach nie gorszych niż parametry sprzętów podlegających wymianie, • Zamawiający ma mieć dostęp do centrów kompetencyjnych Producenta oraz dokumentacji produktowej, • Zamawiający ma mieć możliwość sprawdzenia statusu gwarancji poprzez stronę internetową- podając unikatowy numer urządzenia.
4.	Serwis	Usługa serwisowa może być świadczona przez Wykonawcę, który przez okres trwania wsparcia gwarancyjnego będzie posiadał minimum jednego pracownika posiadającego kwalifikacje techniczne na poziomie zaawansowanym w zakresie wdrażania, administrowania i rozwiązywania problemów z rozwiązaniami bezpieczeństwa będącymi przedmiotem tego zamówienia, potwierdzone certyfikatem podmiotu odpowiedzialnego dla oferowanego systemu bezpieczeństwa dla celów realizacji wysokiej jakości wsparcia technicznego w okresie powdrożeniowym, Zamawiający może w każdym momencie trwania umowy poprosić o przedstawienie certyfikatu osoby o wymaganych kwalifikacjach.

Tabela 3. Szczegółowe parametry techniczne systemu bezpieczeństwa

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
System UTM w konfiguracji wysokiej dostępności (HA) Zamawiający wymaga dostarczenia jednego klastra wysokiej dostępności (HA) dla lokalizacji Ceglana. Na klaster składać się będą dwa urządzenia fizyczne lub dwa pre-instalowane systemy wirtualne tzw. Virtual Appliance wraz ze sprzętem i systemem operacyjnym na którym będą mogły być uruchomione, z którym będą kompatybilne i na którym ich wydajność nie będzie mniejsza od równorzędnego systemu na urządzeniach fizycznych. Zamawiający oświadcza, iż posiada wdrożony i działający system bezpieczeństwa w oparciu o urządzenia FortiGate 600C pracujące w klastrze HA oraz personel przeszkolony z jego obsługi. Używany obecnie klaster urządzeń FortiGate 600C nie będzie nadal wykorzystywany w strukturze sieciowej Zamawiającego, jednocześnie Zamawiający zgadza się na program wymiany posiadanych urządzeń FortiGate 600C na nowe zgodne z poniższymi wymaganiami (zwrot starych urządzeń zostanie potwierdzony stosownym protokołem)		
1.	Redundancja, monitoring i wykrywanie awarii	- system musi pełnić funkcje: Firewall'a, IPSec, Kontroli Aplikacji oraz IPS - system musi posiadać możliwość łączenia w klaster Active-Active lub Active-Passive, a w obu tych trybach musi istnieć funkcja synchronizacji sesji firewall - system musi posiadać funkcje monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych - system musi posiadać monitoring stanu realizowanych połączeń VPN - system musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP, jednocześnie musi istnieć możliwość tworzenia interfejsów redundantnych
2.	Interfejsy, zasilanie	- każde z urządzeń w klastrze HA składające się na system realizujący funkcję Firewall musi dysponować: minimum 10 portami Gigabit Ethernet RJ-45 - minimum 8 gniazdami SFP 1 Gbps - minimum 2 gniazdami SFP+ 10 Gbps - każde z urządzeń w klastrze HA składające się na system musi zostać wyposażone w dwa moduły SFP+ 10Gbps LRM i kablami światłowodowymi MM OM3/125 o długości 2m~5m do połączenia z przełącznikiem szkieletowym Zamawiającego - każde z urządzeń w klastrze HA składające się na system Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB - w ramach systemu Firewall powinna być możliwość zdefiniowania co najmniej 200 interfejsów wirtualnych – definiowanych jako VLAN'y w oparciu o standard

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		802.1Q - system musi być wyposażony w zasilanie AC 220/230V - każde z urządzeń w klastrze HA składające się na system bezpieczeństwa musi być wyposażony w dodatkowy redundantny zasilacz, zasilacz ten musi być kompatybilny z oferowanym rozwiązaniem. - w przypadku zaoferowania rozwiązania opartego o tzw. Virtual Appliance Zamawiający wymaga aby sprzęt na którym będzie to rozwiązanie pracować zapewniało redundantne zasilanie w oparciu o minimum dwa zasilacze
3.	Wydajność systemu bezpieczeństwa	- w zakresie Firewall'a obsługa nie mniej niż 8 milionów jednoczesnych połączeń oraz nie mniej niż 390 tysięcy nowych połączeń na sekundę - przepustowość Stateful Firewall nie mniej niż 36 Gbps - przepustowość Firewall'a z włączoną funkcją Kontroli Aplikacji nie mniej niż 15 Bps - wydajność szyfrowania IPSec VPN nie mniej niż 20 Gbps - wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix minimum 10 Gbps - wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, Application Control, Antywirus minimum 7 Gbps - wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http minimum 8 Gbps
4.	Funkcje systemu UTM	W ramach dostarczonego systemu ochrony muszą być realizowane wszystkie poniższe funkcje. Mogą one być zrealizowane w postaci komercyjnych platform sprzętowych lub programowych: - kontrola dostępu – zaporą ogniową klasy Statefull Inspection - kontrola aplikacji - poufność transmisji danych - połączenia szyfrowane IPSec VPN oraz SSL VPN - ochrona przed Malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS - ochrona przed atakami - Intrusion Prevention System - kontrola stron WWW - kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP - zarządzanie pasmem (QoS, Traffic Shaping) - mechanizmy ochrony przed wyciekami poufnej informacji (DLP) - dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych - w ramach postępowania muszą zostać dostarczone co najmniej 2 tokeny sprzętowe lub programowe, które będą zastosowane do dwuskładnikowego

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		uwierzytelnienia administratorów lub w ramach połączeń VPN typu Client-to-Site - analiza ruchu szyfrowanego protokołem SSL - analiza ruchu szyfrowanego protokołem SSH
4a.	Polityki Firewall	- polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń - system musi zapewniać translację adresów NAT źródłowego i docelowego, translację PAT oraz translację jeden do jeden, translację jeden do wielu, dedykowany ALG (Application Level Gateway) dla protokołu SIP - w ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
4b.	Połączenia VPN	- system musi umożliwiać konfigurację połączeń typu IPsec VPN i zapewniać wsparcie dla IKE v1 oraz v2, obsługę szyfrowania protokołem AES z kluczem 128 i 256 bitów w trybie pracy Galois/Counter Mode(GCM), obsługę protokołu Diffie-Hellman grup 19 i 20, wsparcie dla pracy w topologii Hub and Spoke oraz Mesh, w tym wsparcie dla dynamicznego zestawiania tuneli pomiędzy SPOKE w topologii HUB and SPOKE, tworzenie połączeń typu Site-to-Site oraz Client-to-Site, monitorowanie stanu tuneli VPN i stałego utrzymywania ich aktywności, możliwość wyboru tunelu przez protokoły dynamicznego routingu (np. OSPF) oraz routingu statycznego, obsługę mechanizmów IPsec NAT Traversal, DPD, Xauth, mechanizm „Split tunneling” dla połączeń Client-to-Site - system musi umożliwiać konfigurację połączeń typu SSL VPN i zapewniać pracę w trybie Portal – gdzie dostęp do chronionych zasobów realizowany jest za pośrednictwem przeglądarki (w tym zakresie system musi zapewniać stronę komunikacyjną działającą w oparciu o HTML 5.0), pracę w trybie Tunnel z możliwością włączenia funkcji „Split tunneling” przy zastosowaniu dedykowanego klienta
4c.	Routing i obsługa łączy WAN	- w zakresie routingu rozwiązanie powinno zapewniać obsługę routingu statycznego, polityk ruchu bazujących na routingu, protokołów dynamicznego routingu w oparciu o protokoły RIPv2, OSPF, BGP oraz PIM - system musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN
4d.	Zarządzanie pasmem	- system Firewall musi umożliwiać zarządzanie pasmem poprzez określenie: maksymalnej, gwarantowanej ilości pasma, oznaczanie DSCP oraz wskazanie priorytetu ruchu - musi istnieć możliwość określania pasma dla poszczególnych aplikacji

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- system musi zapewniać możliwość zarządzania pasmem dla wybranych kategorii URL
4e.	Kontrola antywirusowa	- silnik antywirusowy musi umożliwiać skanowanie ruchu w obu kierunkach komunikacji dla protokołów działających na niestandardowych portach (np. FTP na porcie 2021) - system musi umożliwiać skanowanie archiwów, w tym co najmniej: ZIP, RAR - system musi dysponować sygnaturami do ochrony urządzeń mobilnych (co najmniej dla systemu operacyjnego Android) - system musi współpracować z dedykowaną platformą typu Sandbox lub usługą typu Sandbox realizowaną w chmurze.
4f.	Ochrona przed atakami (IPS)	- ochrona IPS powinna opierać się co najmniej na analizie sygnaturowej oraz na analizie anomalii w protokołach sieciowych - system powinien chronić przed atakami na aplikacje pracujące na niestandardowych portach - baza sygnatur ataków powinna zawierać minimum 6500 wpisów i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora - administrator systemu musi mieć możliwość definiowania własnych wyjątków oraz własnych sygnatur - system musi zapewniać wykrywanie anomalii protokołów i ruchu sieciowego, realizując tym samym podstawową ochronę przed atakami typu DoS oraz DDoS - mechanizmy ochrony dla aplikacji Web'owych na poziomie sygnaturowym (co najmniej ochrona przed: CSS, SQL Injecton, Trojany, Exploity, Roboty) oraz możliwość kontrolowania długości nagłówka, ilości parametrów URL, Cookies - wykrywanie i blokowanie komunikacji C&C do sieci Botnet
4g.	Kontrola aplikacji	- funkcja Kontroli Aplikacji powinna umożliwiać kontrolę ruchu na podstawie głębokiej analizy pakietów, nie bazując jedynie na wartościach portów TCP/UDP - baza Kontroli Aplikacji powinna zawierać minimum 2250 sygnatur i być aktualizowana automatycznie, zgodnie z harmonogramem definiowanym przez administratora - aplikacje chmurowe (co najmniej: Facebook, Google Docs, Dropbox) powinny być kontrolowane pod względem wykonywanych czynności, np.: pobieranie, wysyłanie plików - baza powinna zawierać kategorie aplikacji szczególnie istotne z punktu widzenia bezpieczeństwa: proxy, P2P - administrator systemu musi mieć możliwość definiowania wyjątków oraz własnych sygnatur

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
4h.	Kontrola stron internetowych (WWW)	- moduł kontroli WWW musi korzystać z bazy adresów URL pogrupowanych w kategorie tematyczne - filtr WWW musi dostarczać kategorii stron zabronionych prawem: Hazard - administrator musi mieć możliwość nadpisywania kategorii oraz tworzenia wyjątków – białe/czarne listy dla adresów URL - administrator musi mieć możliwość definiowania komunikatów zwracanych użytkownikowi dla różnych akcji podejmowanych przez moduł filtrowania
4i.	Uwierzytelnianie użytkowników w ramach sesji	- system Firewall musi umożliwiać weryfikację tożsamości użytkowników za pomocą haseł statycznych i definicji użytkowników przechowywanych w lokalnej bazie systemu, haseł statycznych i definicji użytkowników przechowywanych w bazach zgodnych z LDAP, haseł dynamicznych (RADIUS, RSA SecurID) w oparciu o zewnętrzne bazy danych - musi istnieć możliwość zastosowania w tym procesie uwierzytelniania dwuskładnikowego - rozwiązanie powinno umożliwiać budowę architektury uwierzytelniania typu Single Sign On przy integracji ze środowiskiem Active Directory oraz zastosowanie innych mechanizmów np. RADIUS lub API
4j.	Zarządzanie systemem	- elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania - komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów - powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego - system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow - system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację - element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall
4k.	Logowanie zdarzeń	- elementy systemu bezpieczeństwa muszą realizować logowanie do aplikacji (logowania i raportowania) udostępnianej w chmurze, lub w ramach postępowania musi zostać dostarczony komercyjny system logowania i

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		raportowania w postaci odpowiednio zabezpieczonej, komercyjnej platformy sprzętowej lub programowej - w ramach logowania system pełniący funkcję Firewall musi zapewniać przekazywanie danych o zaakceptowanym ruchu, ruchu blokowanym, aktywności administratorów, zużyciu zasobów oraz stanie pracy systemu. Musi być zapewniona możliwość jednoczesnego wysyłania logów do wielu serwerów logowania - logowanie musi obejmować zdarzenia dotyczące wszystkich modułów sieciowych i bezpieczeństwa oferowanego systemu - musi istnieć możliwość logowania do serwera SYSLOG
5.	Certyfikaty	System musi posiadać deklarację zgodności Poszczególne elementy oferowanego systemu bezpieczeństwa muszą posiadać następujące certyfikacje: - certyfikacja ICSA lub EAL4 dla oferowanego urządzenia, - certyfikat ICSA lub rekomendacja respektowana przez NATO i Unię Europejską NATO Restricted i UE Restricted dla funkcji IPS, IPSec VPN, SSL VPN
6.	Pozostałe	- system UTM realizujący funkcje Firewall musi dawać możliwość pracy w jednym z trzech trybów tj.: routera z funkcją NAT, transparentnym oraz w trybie monitorowania na porcie SPAN, - musi być zapewniona możliwość budowy minimum dwóch oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewall'a, IPSec VPN, antywirusa, IPS, kontroli aplikacji, - musi istnieć możliwość dedykowania co najmniej 10 administratorów do poszczególnych instancji systemu UTM, - musi wspierać Ipv4 oraz Ipv6 w zakresie: firewall'a, ochrony w warstwie aplikacji, protokołów routingu dynamicznego.
System logowania, raportowania i korelacji Zamawiający wymaga dostarczenia jednego systemu, który: - zastąpi pracę posiadanego systemu analizy logów i raportowania FortiAnalyzer 200D, - będzie umożliwiał centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej DOSTARCZANEJ w ramach niniejszego postępowania infrastruktury zabezpieczeń Klasy UTM jak również posiadanego już przez Zamawiającego systemu zabezpieczeń klasy UTM zbudowanego na urządzeniach fizycznych FortiGate 600E (klaster HA) oraz, oraz systemu ochrony aplikacji webowych FortiWeb 400C, poprzez ich integrację w zakresie opisanym poniżej.		
7.	Kompatybilność	

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy lub komercyjnych platform działających w środowisku wirtualnym lub w postaci komercyjnej platformy działających na bazie systemu linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: Vmware ESX/ESXi 5.5,6.0,6.5,6.7, Microsoft Hyper-V 2008 R2,2012, R2,2016, Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).
8.	Interfejsy, dyski	System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 6 TB.
9.	Wydajność	Rozwiązanie musi umożliwiać kolekcjonowanie logów z wszystkich wskazanych systemów posiadanych przez Zamawiającego, tj. FortiGate 600E, FortiWeb400C, oraz dostarczanych w ramach niniejszego postępowania. Rozwiązanie musi umożliwiać kolekcjonowanie logów z minimum 1000 systemów. System musi być w stanie przyjmować minimum 11 GB logów na dzień.
10.	Funkcje systemu	W ramach centralnego systemu zarządzania muszą być realizowane co najmniej poniższe funkcje dla wszystkich podłączonych do systemu urządzeń: W zakresie logowania: - podgląd logowanych zdarzeń w czasie rzeczywistym, - możliwość przeglądania logów historycznych z funkcją filtrowania, - dostępne predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa obejmujące co najmniej: • listę najczęściej wykrywanych ataków, • listę najbardziej aktywnych użytkowników, • listę najczęściej wykorzystywanych aplikacji, • listę najczęściej odwiedzanych stron www,

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		- listę krajów, do których nawiązywane są połączenia - listę najczęściej wykorzystywanych polityk firewall - informacje o realizowanych połączeniach IPSec W zakresie raportowania: - możliwość generowania raportów co najmniej w formatach: PDF, CSV, - dostępne predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników, - możliwość definiowania własnych raportów, - możliwość spolszczenia raportów, - możliwość generowania raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesyłania wyników na określony adres lub adresy email. W zakresie korelacji logów: - umożliwiać określenie urządzeń, dla których proces korelacji ma być realizowany, - umożliwiać konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa, - umożliwiać wybór kategorii zdarzeń dla których tworzone będą reguły korelacyjne, - umożliwiać korelację zdarzeń co najmniej z następujących kategorii zdarzeń: malware, aplikacje sieciowe, email, IPS, traffic, systemowe (utracone połączenia vpn, utracone połączenia sieciowe).
11.	Komunikacja/eksport danych	Rozwiązanie musi posiadać możliwość przesyłanie kopii logów do innych systemów logowania i przetwarzania danych. W tym zakresie musi zapewniać mechanizmy filtrowania dla wysyłanych logów. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.

Lp.	Funkcjonalność	Wymagane minimalne parametry techniczne
		System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.
12.	Zarządzenie	System musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów HTTPS oraz SSH lub producent rozwiązania musi dostarczyć dedykowana konsolę zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów. Proces uwierzytelniania administratorów musi być realizowany w oparciu o lokalną bazę, Radius, LDAP, PKI. System musi umożliwiać zdefiniowanie co najmniej 3 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.
13.	Licencje	System musi być dostarczony w modelu „na własność” tj. niewykupienie odnowienia licencji wsparcia technicznego dla rozwiązania nie spowoduje zablokowania funkcjonowania systemu, a jedynie pozbawi możliwości pobierania aktualizacji oprogramowania.

Tabela 4. Wymagania Zamawiającego dotyczące potwierdzenia oferowanych parametrów technicznych (odnośnik do punktu IV1 a) SWZ

I.	Dla Systemu UTM w konfiguracji wysokiej dostępności (HA)
1.	Redundancja, monitoring i wykrywanie awarii: - system musi pełnić funkcje: Firewall'a, IPSec, Kontroli Aplikacji oraz IPS - system musi posiadać możliwość łączenia w klaster Active-Active lub Active-Passive, - system musi posiadać funkcje monitoringu i wykrywania uszkodzenia elementów sprzętowych i programowych systemów zabezpieczeń oraz łącz sieciowych - system musi posiadać monitoring stanu realizowanych połączeń VPN - system musi umożliwiać agregację linków statyczną oraz w oparciu o protokół LACP, jednocześnie musi istnieć możliwość tworzenia interfejsów redundantnych

2.	Interfejsy, zasilanie: - każde z urządzeń w klastrze HA składające się na system realizujący funkcję Firewall musi dysponować: minimum 10 portami Gigabit Ethernet RJ-45, minimum 8 gniazdami SFP 1 Gbps, minimum 2 gniazdami SFP+ 10 Gbps - każde z urządzeń w klastrze HA składające się na system Firewall musi posiadać wbudowany port konsoli szeregowej oraz gniazdo USB umożliwiające podłączenie modemu 3G/4G oraz instalacji oprogramowania z klucza USB
3.	Wydajność systemu bezpieczeństwa: - w zakresie Firewall'a obsługa nie mniej niż 8 milionów jednoczesnych połączeń oraz nie mniej niż 390 tysięcy nowych połączeń na sekundę - przepustowość Stateful Firewall nie mniej niż 36 Gbps - przepustowość Firewall'a z włączoną funkcją Kontroli Aplikacji nie mniej niż 15 Bps - wydajność szyfrowania IPsec VPN nie mniej niż 20 Gbps - wydajność skanowania ruchu w celu ochrony przed atakami (zarówno client side jak i server side w ramach modułu IPS) dla ruchu Enterprise Traffic Mix minimum 10 Gbps - wydajność skanowania ruchu typu Enterprise Mix z włączonymi funkcjami IPS, Application Control, Antywirus minimum 7 Gbps - wydajność systemu w zakresie inspekcji komunikacji szyfrowanej SSL dla ruchu http minimum 8 Gbps
4.	Funkcje systemu UTM: - kontrola dostępu - zaporą ogniową klasy Statefull Inspection - kontrola aplikacji - poufność transmisji danych - połączenia szyfrowane IPsec VPN oraz SSL VPN - ochrona przed Malware – co najmniej dla protokołów SMTP, POP3, IMAP, HTTP, FTP, HTTPS - ochrona przed atakami - Intrusion Prevention System - kontrola stron WWW - kontrola zawartości poczty – Antyspam dla protokołów SMTP, POP3, IMAP - zarządzanie pasmem (QoS, Traffic Shaping) - mechanizmy ochrony przed wyciekiem poufnej informacji (DLP) - dwuskładnikowe uwierzytelnianie z wykorzystaniem tokenów sprzętowych lub programowych
5.	Polityki Firewall: - polityka Firewall musi uwzględniać adresy IP, użytkowników, protokoły, usługi sieciowe, aplikacje lub zbiory aplikacji, reakcje zabezpieczeń, rejestrowanie zdarzeń - system musi zapewniać translację adresów NAT źródłowego i docelowego, translację PAT oraz translację jeden do jeden, translację jeden do wielu, dedykowany ALG (Application Level Gateway) dla protokołu SIP - w ramach systemu musi istnieć możliwość tworzenia wydzielonych stref bezpieczeństwa np. DMZ, LAN, WAN
6.	Routing i obsługa łączy WAN: - w zakresie routingu rozwiązanie powinno zapewniać obsługę routingu statycznego, polityk ruchu bazujących na routingu, protokołów dynamicznego routingu w oparciu o protokoły RIPv2, OSPF, BGP oraz PIM - system musi umożliwiać obsługę kilku (co najmniej dwóch) łączy WAN z mechanizmami statycznego lub dynamicznego podziału obciążenia oraz monitorowaniem stanu połączeń WAN
7.	Zarządzanie systemem:

	- elementy systemu bezpieczeństwa muszą mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów HTTPS oraz SSH, jak i powinny mieć możliwość współpracy z dedykowanymi platformami centralnego zarządzania i monitorowania - komunikacja systemów zabezpieczeń z platformami centralnego zarządzania musi być realizowana z wykorzystaniem szyfrowanych protokołów - powinna istnieć możliwość włączenia mechanizmów uwierzytelniania dwuskładnikowego dla dostępu administracyjnego - system musi współpracować z rozwiązaniami monitorowania poprzez protokoły SNMP w wersjach 2c, 3 oraz umożliwiać przekazywanie statystyk ruchu za pomocą protokołów netflow lub sflow - system musi mieć możliwość zarządzania przez systemy firm trzecich poprzez API, do którego producent udostępnia dokumentację - element systemu pełniący funkcję Firewall musi posiadać wbudowane narzędzia diagnostyczne, przynajmniej: ping, traceroute, podglądu pakietów, monitorowanie procesowania sesji oraz stanu sesji firewall
8.	Pozostałe: - system UTM realizujący funkcje Firewall musi dawać możliwość pracy w jednym z trzech trybów tj.: routera z funkcją NAT, transparentnym oraz w trybie monitorowania na porcie SPAN, - musi być zapewniona możliwość budowy minimum dwóch oddzielnych (fizycznych lub logicznych) instancji systemów w zakresie: routingu, firewall'a, IPSec VPN, antywirusa, IPS, kontroli aplikacji,
II.	Dla Systemu centralnego logowania, raportowania i korelacji
1.	Kompatybilność: - możliwość uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi 6.0,6.5,6.7,7.0 Microsoft Hyper-V 2012 R2, 2016, Microsoft Azure, Google Cloud (GCP)
2.	Interfejsy, dyski: - system musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności minimum 6 GB oraz pozwalać na dalsze rozszerzenie pojemności dyskowej
3.	Wydajność: System musi umożliwiać zarządzanie co najmniej 10 systemami bezpieczeństwa/UTM.